Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit

Zur Erlangung des akademischen Grades eines Doktors der Ingenieurwissenschaften von der Fakultät für Informatik der Universität Karlsruhe

vorgelegte

Dissertation

von

Hadmut Danisch

aus

Mannheim

Tag der mündlichen Prüfung:
Erster Gutachter:
Zweiter Gutachter:

Inhaltlicher Stand: Frühjahr 1998
Layout und Korrekturen: 29. August 1999

– Vorbemerkung usw. –
(Wird zum gegebenen Zeitpunkt mit dem passenden Inhalt gefüllt werden.)

Inhaltsverzeichnis

Verzeichnis der Definitionen, Beispiele, Bemerkungen etc. **VII**

Abbildungsverzeichnis **XI**

Tabellenverzeichnis **XIII**

1 Einführung **1**
1.1 Motivation und Überblick 1
1.2 Was ist Sicherheit? 2
1.3 Was ist Kryptographie? 6
1.4 Bestehende Kriterien- und Maßnahmenkataloge 10
1.4.1 Überblick über wichtige Werke 10
1.4.2 Kritik 12
1.5 Zertifizierungen und Evaluierungen 14
1.5.1 Zertifizierungen des BSI 14
1.5.2 Konkrete Betrachtung einer Zertifizierung 16
1.5.3 Bewertung 22
1.6 Formale Sicherheitsmodelle 23
1.6.1 Grundprobleme Formaler Modelle 24
1.6.2 Das Bell-LaPadula-Modell 26
1.6.3 Das „Chinese Wall“ Modell 26

2 Die System- und Bedrohungsanalyse **29**
2.1 Überblick 29
2.2 Die befugten Parteien 31
2.2.1 Der Begriff der Partei 31
2.2.2 Eigenschaften der Parteien 32
2.2.3 Parteispezifische Rahmenbedingungen 35
2.2.4 Akausale Kommunikation 37
2.2.5 Die unabhängige dritte Partei 37
2.3 Die Eigenschaften des Übertragungsmediums 37
2.3.1 Übertragung in Raum oder Zeit 37
2.3.2 Kommunikationswege 41

2.3.3 Aufbau im Schichtenmodell 42
2.3.4 Grad der Interaktion 43
2.3.5 Nebenwirkungen und Risiken der Absicherung 44
2.4 Der Angreifer 44
2.4.1 Das Feindbild 44
2.4.2 Angriffszweck 52
2.4.3 Aufwand und Kosten des Angriffs 53
2.5 Das Schutzobjekt 54
2.5.1 Sicherungszweck 54
2.5.2 Weitere Sicherungsziele 57
2.5.3 Komponenten 63
2.5.4 Zeitliche und räumliche Beschränkungen 67
2.5.5 Schadenserwartung 68
2.5.6 Schutzobjekt Sicherungsmaßnahme 68

3 Sicherungsmethoden 69
3.1 Überblick 69
3.2 Bewertungen und dynamische Auswahlverfahren 70
3.3 Spezifikationstreue und Korrektheit 71
3.4 Veränderungen des Kosten/Nutzen-Verhältnisses 72
3.4.1 Anhebung der Angriffskosten 73
3.4.2 Senkung der Leistungsfähigkeit des Angreifers 73
3.4.3 Senkung des Angriffsnutzens 74
3.5 Erschwerung der Angriffsvorbereitung 74
3.6 Organisatorische Maßnahmen 76
3.6.1 Ausgewählte Beispiele für organisatorische Sicherungsmaßnahmen 78
3.6.2 Sicherung der Sekundärinformationen 79
3.7 Seiteneffektdämpfende Maßnahmen 82
3.8 Kryptographische Maßnahmen 83
3.9 Verschleiernde Maßnahmen 85
3.9.1 Beispiele 86
3.10 Schadensbegrenzung 87
3.10.1 Entkopplung der Schutzobjekte 88
3.10.2 Entkopplung der Mechanismen 88
3.11 Angriffserkennung und -nachweis 89
3.11.1 Implizite Erkennung 89
3.11.2 Explizite Erkennung 90
3.12 Reaktionen während und nach dem Angriff 91
3.12.1 Objektdestruktive Maßnahmen 91
3.12.2 Offensive Maßnahmen 93

4 Bewertung von Sicherheitsmechanismen 95
4.1 Positionierung im Schichtenmodell 95
4.1.1 Reichweite 98
4.1.2 Schutz der Primär- und Sekundärinformationen 101
4.1.3 Resistenz gegen Umgehung 103
4.2 Effektivität und Kosten 112
4.2.1 Erfolg und Erfolgsdetektion 112
4.2.2 Theoretische Schranken 112
4.2.3 Angriffskosten 113
4.2.4 Alterung 113
4.3 Nebenwirkungen und Anforderungen 114
4.3.1 Abhängigkeit von Systemeigenschaften 114
4.3.2 Eingriffstiefe und Nebenwirkungen 114
4.3.3 Übersicherung 115
4.3.4 Problemverlagerungen 116
4.3.5 Abbildung auf technische Merkmale 116
4.4 Nichttechnische Eigenschaften 117
4.4.1 Verbot und Gebot von Mechanismen 117
4.4.2 Rechtstreue als Schutzobjekt 118
4.4.3 Verbote und Gebote als Angriff 118
4.4.4 Wirksamkeit 118

5 Besondere Probleme staatlicher Kommunikationsüberwachung 119
5.1 Überblick 120
5.2 Informationstheoretische Grundlagen 122
5.2.1 Allgemeine Informationstheorie 122
5.2.2 Informationstheorie und Kryptographie 126
5.3 Verbot chiffrierter Übertragungen 130
5.3.1 Position im Schichtenmodell 130
5.3.2 Probleme der Detektion 131
5.3.3 Entfernung kompromittierender Redundanz 136
5.3.4 Täuschung des Zensors durch falsche Redundanz 137
5.4 Beschränkungen der Schlüssellänge 139
5.4.1 Informationstheoretische Betrachtungen 140
5.4.2 Schlüssellose Chiffren 144
5.4.3 Verkürzung der Schlüssellänge ohne Kenntnis des Senders . . 153
5.5 Protokolle mit Schlüsseloffenlegung 154
5.5.1 Offenlegung des Schlüssels mit Kenntnis des Senders 154
5.5.2 Offenlegung des Schlüssels ohne Kenntnis des Senders 156
5.5.3 Triviale Umgehungen der Offenlegung 161
5.5.4 „Legale“ Umgehungen der Offenlegung 162
5.6 Nachträgliche Verpflichtung zur Offenlegung 164
5.6.1 Schutzobjekt eigene Identität 164

5.6.2 Eigenpartitionierung 165
5.6.3 Verteidiger *vor* Angreifer – Unwiederholbarkeit 166
5.6.4 Verteidiger *nach* Angreifer – Zeitfenster 170
5.7 Konflikte mit der Signatursicherheit 171
5.7.1 Impliziter Schlüsseltausch durch DLP-Signaturen 172
5.7.2 Expliziter Schlüsseltausch durch Eigenzertifizierung 174
5.7.3 Signaturen als Nachrichtenkanäle 175

6 Zusammenfassung und Einordnung 177

Literaturverzeichnis 179

Lebenslauf 189

Verzeichnis der Definitionen, Beispiele, Bemerkungen etc.

Bem.	1.1	Konflikt zwischen Safety und Security	3
Def.	1.2	„Bedrohung“ und „Angriff“	4
Def.	1.3	„Sicherheit“	4
Bem.	1.4	„Triviale Sicherheit“	5
Bem.	1.5	Abgrenzung zur „Safety“	5
Def.	1.6	„Information“, „Daten“, „Nachricht“	5
Bem.	1.7	Beschränkung auf digitale Daten	5
Def.	1.8	„Steganographie“ und „Kryptographie“ die I.	8
Def.	1.9	„Geheimnis“	8
Def.	1.10	„Steganographie“ und „Kryptographie“ die II.	9
Zit.	1.11	Aus den Zertifikaten des BSI	15
Zit.	1.12	§ 4 Abs. 3 Nr. 2 BSIG	15
Zit.	1.13	§ 3 BSIZertV	16
Bsp.	1.14	Sicherheitstechnische Anforderungen an eine Banküberweisung	20
Bsp.	1.15	Betriebssystem mit chinesischer Mauer	27
Def.	2.1	„Partei“	31
Bem.	2.2	Die drei Grundparteien	31
Def.	2.3	„Partition“	33
Def.	2.4	„Adresse“	33
Def.	2.5	„passend“	33
Def.	2.6	„Position“	34
Bsp.	2.7	Parteienunterscheidung durch Paßwort	34
Bsp.	2.8	Parteiflexibilität im Schichtenmodell	35
Bsp.	2.9	Sicherungsaufwand	36
Bsp.	2.10	Zeitliche und räumliche Übertragung	38
Bem.	2.11	Zur Wahl des Schichtenmodells	42
Bsp.	2.12	Sicherungsfähigkeit der Schichten	43
Bsp.	2.13	Betrachtung der Interaktion im Schichtenmodell	43
Def.	2.14	„Feindbild“	45
Bsp.	2.15	Festlegung des Feindbildes	45
Bsp.	2.16	Festlegung des Feindbildes	46

Bsp.	2.17	Angriff nach Übertragung	49
Bsp.	2.18	Angriff gegen Chiffre	52
Zit.	2.19	§ 267 I StGB	56
Def.	2.20	Integrität, Authentizität, Vollständigkeit, Eindeutigkeit, Echtheit	56
Bsp.	2.21	Parteienspezifische Beweiskraft	57
Bsp.	2.22	Denial of Service	58
Bsp.	2.23	Denial of Service durch Angreiferposition	59
Bsp.	2.24	Kombination billiger und starker Verfahren	59
Bsp.	2.25	Beweislast beim „Telebanking“	60
Bsp.	2.26	Angriff gegen „Anonymous Remailer“	67
Bem.	3.1	Methoden nach Angriffserfolg	69
Bsp.	3.2	Systemschutz durch die JAVA Virtual Machine	72
Bem.	3.3	Angriffsvorbereitung	75
Bem.	3.4	Schwerer Fehler: „Security by Obscurity“	75
Bem.	3.5	Nichttechnische Bereiche: Social Engineering	76
Def.	3.6	„organisatorisch“	76
Bem.	3.7	Organisatorische Maßnahmen und Partitionen	77
Bem.	3.8	Position im Angreifermodell	77
Bsp.	3.9	Paketfilter	77
Bsp.	3.10	Zusammenbruch einer organisatorischen Sicherung	78
Bsp.	3.11	Verlagerung der Sekundärinformationen in höhere Schichten	80
Bsp.	3.12	Sender/Empfänger-Entkopplung	81
Bsp.	3.13	Bindung an andere Schichten	81
Bsp.	3.14	Bindung an physikalische Adressen	82
Bsp.	3.15	Kompromittierende Abstrahlung	82
Bsp.	3.16	Software mit Seiteneffekten	83
Bem.	3.17	Verhältnis zur Spezifikationstreue und Eingrenzung	83
Def.	3.18	„kryptographisch“	84
Bem.	3.19	Schutzobjekt Geheimnis	84
Bem.	3.20	Verhältnis zu organisatorischen Maßnahmen	84
Def.	3.21	„verschleiernd“	85
Bem.	3.22	Schutz gegen absichtslose Angriffe	87
Bsp.	3.23	Ungenügende Mechanismenentkopplung	88
Bem.	3.24	Plausibilitätsprüfung	89
Bsp.	3.25	Erkennung von „Spamming“	89
Bsp.	3.26	Angriffserkennung auf Schicht 1	90
Bsp.	3.27	Angriffserkennung auf Schicht 4	90
Bsp.	3.28	Angriffserkennung am Geldautomat	91
Bsp.	3.29	Transportbehälter für Spionagematerial	91
Bsp.	3.30	Quantenkommunikation	91
Bsp.	3.31	Angriff auf RAID-Systeme	92

Bsp. 4.1 Doppelsicherung bei E-Mail . . . 102
Bem. 4.2 Verlagerung der Schutzobjekte in andere Schichten . . . 105
Bsp. 4.3 Unterlaufen der Schicht im Bell-LaPadula Modell . . . 106
Bsp. 4.4 Schwächen der Intel 80x86 Prozessoren . . . 107
Bem. 4.5 Trennung von Betriebssystem und Anwendung . . . 108
Bsp. 4.6 Horizontale Umgehung . . . 110
Bem. 4.7 Relevanz des Angriffszeitraumes . . . 113
Bem. 4.8 Größen für Angriffskosten . . . 113
Bsp. 4.9 Übersicherung durch PIN . . . 115
Bem. 4.10 Schutzobjekt Adresse . . . 117

Def. 5.1 Stichprobe und Wahrscheinlichkeitsverteilung . . . 122
Def. 5.2 Bedingte Wahrscheinlichkeit . . . 123
Def. 5.3 Quelle . . . 123
Def. 5.4 Kanal . . . 123
Def. 5.5 Informationsgehalt . . . 124
Def. 5.6 Entropie . . . 124
Stz. 5.7 Satz über die Verbundentropie . . . 124
Stz. 5.8 Satz über die Verbundentropie und Irrelevanz . . . 125
Stz. 5.9 Satz über die Verbundentropie und Äquivokation . . . 125
Bem. 5.10 Verbundentropie . . . 125
Def. 5.11 Transinformationsgehalt . . . 125
Def. 5.12 Kanalkapazität . . . 126
Def. 5.13 Kryptosystem . . . 126
Bem. 5.14 Berechnung von $p_{\mathcal{P}}(x|y)$ . . . 127
Bem. 5.15 Berechnung von $p_{\mathcal{P}}(k|y)$ . . . 127
Bem. 5.16 $H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{P}|\mathcal{C}) + H_a(\mathcal{K}|(\mathcal{C}\mathcal{P}))$ . . . 129
The. 5.17 Unzensierbarkeit des voll genutzten Kanals . . . 132
Bew. 5.18 Unzensierbarkeit des voll genutzten Kanals . . . 132
Bem. 5.19 Randbedingungen . . . 135
Bem. 5.20 Identität von Chiffraten und Klartexten . . . 135
Bem. 5.21 Anforderung an das Kompressionsverfahren . . . 137
Bsp. 5.22 Tarnung durch falsche Redundanz . . . 137
Bem. 5.23 Gefahr falscher Verdächtigung . . . 138
Bem. 5.24 $H_a(\mathcal{C}|(\mathcal{K}\mathcal{P})) \neq 0$ . . . 144
Def. 5.25 „Schlüssellose Chiffre“ . . . 147
Bsp. 5.26 Eine schlüssellose Chiffre . . . 147
Bem. 5.27 Wirkung „schlüsselloser Chiffren“ . . . 148
Bem. 5.28 Qualitative Unterscheidung vom längeren Schlüssel . . . 148
Bem. 5.29 Abgrenzung zum Shared Secret-Schema . . . 149
Bem. 5.30 Hash-Verfahren als Chiffre . . . 150
Bsp. 5.31 CBC mit vollständiger Durchmischung . . . 150
Bem. 5.32 Aufwandsbetrachtung zu Schlüssellosen Chiffren . . . 151

Bsp. 5.33 Telefonverschlüsselung 160
Bsp. 5.34 Zeitliche Beschränkung des Zensors 163
Def. 5.35 „kryptographisch interaktiv“ 168
Bem. 5.36 Unvernichtbarkeit der Signierinformation 168
Bsp. 5.37 Pseudointeraktiver Schlüsseltausch 169
Bsp. 5.38 Signaturen mit Schlüsselabwurf 170
Bsp. 5.39 Der Zeit-Notar 171
Bsp. 5.40 Waschmaschine und Käsekuchen 173
Bem. 5.41 Signaturen und Chiffrierschlüssel 175
Bem. 5.42 Kombination beider Verfahren 176

Abbildungsverzeichnis

2.1 Kommunikationsgrundschema 31
2.2 Asymmetrie zwischen Raum- und Zeitübertragungsschlüsseln 40
2.3 Positionen des Angreifers im Kommunikationsschema 48
2.4 Schema für die Angreiferposition 49
2.5 Zerlegung einer normalen Datenübertragung 50
2.6 Wissensformen 53
2.7 Nutzlast und Hilfslast im Schichtenmodell 64

4.1 Datentransport im Internet 99
4.2 Mehrfache Absicherung 102
4.3 Überspringen von Sicherungsmaßnahmen 105
4.4 Unterlaufen von Sicherungsmaßnahmen 107
4.5 Horizontale Umgehung von Sicherungsmaßnahmen 110
4.6 Vertikale Umgehung von Sicherungsmaßnahmen 111

5.1 Einfaches Kanalmodell zur Kommunikationsüberwachung 122
5.2 Der Legalitätsdetektor 133
5.3 Phantomredundanz gegen vollständige Schlüsselsuche 143
5.4 Betriebsarten für Blockchiffren 145
5.5 Eine „Schlüssellose Chiffre“ 148
5.6 CBC-Variation mit breiter Durchmischung 151
5.7 Schlüssellose Chiffre mit $O(n \log n)$ 153
5.8 Der „Clipper Chip“ 156
5.9 Einbettung eines Subliminal Channels 158
5.10 Eine „Black Box“ mit verdecktem Kanal für Schlüsselentropie 159

Tabellenverzeichnis

1.1 Altgriechische Vokabeln 7
1.2 TCSEC-Klassen 11

3.1 Methoden und ihre Wirkung in zeitlicher Ordnung 70

4.1 Belegungen im Schichtenmodell 97
4.2 Funktionale Charakterisierung der Schichten 100

5.1 Rechenzeiten für die vollständige Suche 140

1 Einführung

1.1 Motivation und Überblick

Die Vernetzung von Rechnersystemen und die Nutzung von Rechnernetzwerken, besonders des Internet, haben in den letzten Jahren explosionsartig zugenommen. Der Anschluß an ein firmen- oder sogar weltweit reichendes Netzwerk gehört inzwischen zur normalen Ausstattung im privaten, öffentlichen und kommerziellen Bereich. Damit einher geht aber auch eine völlig neue Art der Verletzlichkeit, weil zunehmend sensible Daten über Netzwerke transportiert werden und mit der steigenden Zahl vernetzter Rechner auch die Zahl der potentiellen Angriffsziele zunimmt.

Die Folge ist ein erheblich erhöhter Bedarf an Sicherheit. Hinzu kommt eine neue Vielfalt von Sicherheitsanforderungen. Durch neue Anwendungen, die die Telekommunikation funktional integrieren, entstehen neue Sicherheitsinteressen, die über althergebrachte Systemsicherheit, die sich auf den Zugang zu Rechenanlagen und Resourcen bezieht, weit hinausgeht. Gleichzeitig wird der Entwurf von Sicherheitssystemen immer schwieriger, weil die Komplexität und Vielfalt der Protokolle und Anwendungen immer schneller ansteigt.

Demgegenüber ist aber kein adäquater Fortschritt beim Entwurf, der Analyse und der Beschreibung von Sicherheitssystemen zu bemerken. Es gibt zwar verschiedene (Teil-) Disziplinen der Informatik, die sich mit dem Thema Sicherheit befassen, etwa die Bereiche Kryptographie, Systemsicherheit und Netzwerksicherheit, die aber nicht auf die eigentliche, neu entstandene Problematik eingehen. Darin ist die Ursache zu sehen, daß es eine Vielzahl von Sicherheitssystemen gibt, die nicht die benötigte Sicherheit gewährleisten, weil sie – vollgestopft mit „bewährten“ Verfahren – eine ganz andere Form von Sicherheit herstellen, als eigentlich benötigt wird.

So ist zu beobachten, daß der Begriff „Bedrohungsanalyse“ gern verwendet wird, weil er eine wissenschaftliche Untersuchung suggeriert und den Eindruck hervorruft, kein System „von der Stange“, sondern eine maßgeschneiderte Problemlösung hervorzubringen. In der Realität fallen die Bedrohungsanalysen aber fast immer gleich – und gleich banal – aus: *Man braucht Vertraulichkeit und Integrität. Deshalb müssen Verschlüsselungen und Signaturen her.* Gelegentlich werden auf Grundlage dieser „individuellen“ Bedrohungsanalyse mit formalen Methoden oder gewissen Modellen Anforderungen und Lösungen erarbeitet, die dann eine Problemlösung sein sollen, obwohl

das spezifisch individuelle Problem weder analysiert noch beschrieben und schon gar nicht im Entwurf verarbeitet wurde.

Die vorliegende Arbeit setzt an dieser Stelle an und stellt die Analyse, die Beschreibung und den Entwurf von Sicherheitssystemen im Bereich der Kommunikation dar:

- Kapitel 2 stellt Kriterien vor, anhand derer die *Analyse* und die *Beschreibung* des zu sichernden Systems und der Bedrohung erstellt werden können.
- Kapitel 3 nimmt eine grundsätzliche Klassifizierung von Sicherungsmethoden anhand ihrer Wirkung gegen einen Angriff vor.
- In Kapitel 4 werden Kriterien aufgezeigt, anhand derer Sicherheitsmechanismen, also konkrete technische Realisierungen der Methoden, bewertet werden können.
- Schließlich wird in Kapitel 5 eine ganz besondere Klasse von Problemen kritisch betrachtet, die einerseits die zur Verfügung stehenden Sicherungsmethoden und -mechanismen einschränkt, andererseits aber auch neue Bedrohungen mit sich bringt, nämlich die staatliche Kommunikationsüberwachung.

1.2 Was ist Sicherheit?

„Sicherheit“ ist der zentrale Begriff der vorliegenden Arbeit. Als Grundlage und zur Einleitung wird daher zunächst erkundet, was eigentlich unter diesem Begriff zu verstehen ist.

Der Begriff „Sicherheit“ ist kein Fachbegriff der Informatik bzw. Computertechnik, sondern ein der Umgangssprache entnommener Begriff. Die umgangssprachliche Bedeutung des Begriffes ist an seiner etymologischen Herkunft zu erkennen [49]:

> **sicher:** Das *westgerm.* Adjektiv *mhd.* sicher, *ahd.* sichur, *niederl.* zeker, *aengl.* sicor ist schon früh aus *lat.* sēcūrus „sorglos, unbekümmert, sicher“ entlehnt worden, einer Bildung zu *lat.* cūra „Sorge; Pflege“ (vgl. *Kur*; *lat.* sē[d] bedeutet „ohne; beseite, weg“). [. . .] Abl.: Sicherheit *w* (*mhd.* sicherheit, *ahd.* sichurheit);

Sicherheit zu haben bedeutet also, sich keine Sorgen machen zu müssen und unbekümmert sein zu können bzw. irgendetwas unbekümmert tun zu können; tatsächlich sind „sorglos“ und „unbekümmert“ wortwörtliche Übersetzungen von „sicher“ (se*cure* = *care*less). Sicherheit hat folglich mit der Abwehr dessen zu tun, weswegen man sich sorgen müßte.

Unglücklicherweise wird im Deutschen der Begriff „Sicherheit“ im Zusammenhang mit elektronischer Datenverarbeitung gleich in zwei verschiedenen Bedeutungen verwendet, was gelegentlich zu Mißverständnissen führt, insbesondere wenn dabei nicht ausreichend zwischen den Bedeutungen differenziert wird. Im Englischen werden hingegen zwei verschiedene Begriffe verwendet:

„Security“ ist die eigentlich zutreffende Übersetzung von „Sicherheit“ und wird verwendet, wenn es im weitesten Sinne um die Abwehr von Angriffen Böswilliger geht.

„Safety“ [1] wird verwendet, wenn es um den Schutz vor ungewollten Ereignissen wie Unfällen, technischem Versagen usw. geht. Schaden droht hier nicht durch bösen Willen, sondern durch Zufälle, technische Unzulänglichkeiten, Defekte usw.

In der vorliegenden Arbeit geht es dabei fast ausschließlich nur um Sicherheit im Sinne von „Security“.

Bemerkung 1.1:
Konflikt zwischen Safety und Security
Zu bemerken ist allerdings, daß „Safety“ und „Security“ nicht immer konfliktfrei nebeneinander stehen.

In Beispiel 3.31 wird gezeigt, wie eine Fehlerkorrektur ein neues Sicherheitsproblem erzeugt.

In Beweis 5.18 und Abschnitt 5.4.1.4 wird gezeigt, daß die Redundanzfreiheit des Klartextes eine wichtige Sicherheitsanforderung sein kann und damit die Anhebung des Signal-Rauschabstandes durch fehlerkorrigierende Codes etc. ausschließt.

Diese sehr allgemein gehaltene sprachliche Beschreibung ist nicht ausreichend, um die Bedeutung des Begriffes im Bereich der Informations- und Datenverarbeitung zu beschreiben. Eine genaue Definition ist allerdings nicht trivial; es werden zunächst einige mehr oder weniger gelungende Definitionen aus der Literatur zusammengestellt:

Aus [75] stammt folgende Definition:

> „Unter *Sicherheit* ist . . . das Ziel zu verstehen, informationsverarbeitende Systeme so zu entwerfen, herzustellen und einzusetzen, daß ein Maximum an Schutz gegenüber Bedienungsfehlern, technischem Versagen, katastrophenbedingten Ausfällen und absichtlichen Manipulationsversuchen gegeben ist.“

Hierbei werden offensichtlich „Safety“ und „Security“ nicht ausreichend differenziert. Eine bessere Definition findet sich in [55]:

> „Unter Sicherheit von IT-Systemen versteht man eine Eigenschaft eines IT-Systems, bei der Maßnahmen gegen die im jeweiligen Einsatzumfeld als bedeutsam angesehenen Bedrohungen in dem Maße wirksam sind, daß die verbleibenden Risiken tragbar sind.“

[1] von *engl.* safe „unversehrt; sicher“, *afrz.* sauf, *lat.* salvus „gesund, heil“ (vgl. *Salve*).

Gegen diese Definition läßt sich nicht viel sagen; sie ist nämlich so weit und allgemein gefaßt, daß sie nicht über die schon dem umgangssprachlichen Begriff „Sicherheit“ anhaftende Bedeutung hinausgeht und eigentlich keinen Bezug zur Informatik hat. Die offengehaltene Hintertür der „verbleibenden tragbaren Risiken“ ist so ungenau, daß die gesamte Definition inhaltsleer wird.

Eine etwas andere Definition ist in [58] zu finden:

> „Datensicherheit ist das Ziel einer Summe von Maßnahmen und Mitteln zur Erfüllung einer anwendungsbezogenen Aufgabenstellung, erreichbar über Maßnahmen und Mittel des Schutzes bzw. der Sicherung bestimmter Objekte (Daten, Rechentechnik, Räume, Gebäude usw.) vor bestimmten Einwirkungen von Aktionen (Lesen, Verändern, Löschen, Hinzufügen, Zerstören, Blockieren, Benutzen usw.), wobei das verbleibende Restrisiko bekannt ist.“

Auch hier wird Sicherheit nicht *be-* sondern *um*schrieben: Sicherheit ist das, was man mit Maßnahmen der Sicherung erreichen kann. An gleicher Stelle findet man Zitate weiterer Definitionen, die alle in ungefähr dieselbe Richtung laufen.

Definitionen dieser Art sind plakativ, helfen aber im Grunde nicht weiter. Sicherheit und der Bedarf an derselben sind zu vielschichtig, um eine absolute und universelle Definition zu geben, die einerseits weitreichend genug ist, um alle Aspekte abzudecken, andererseits genügend Inhalt hat, um den Begriff festzulegen.

Daher soll hier ein anderer Weg zur Definition von Sicherheit beschritten werden.

Definition 1.2:
„Bedrohung“ und „Angriff“

Eine *Bedrohung* ist die Möglichkeit des Eintretens eines Zustandes oder eines Vorganges, der den Interessen eines *Interessenträgers* zuwiderläuft, von diesem als Schaden angesehen wird und der als Folge böswilliger (aktiver oder passiver) Handlungen eintreten kann.

Ein *Angriff* ist also ein böswilliger (und damit zielgerichteter) erfolgreicher oder -loser Versuch des *Angreifers*, den der Bedrohung zugrundeliegenden Zustand oder Vorgang herbeizuführen.

Definition 1.3:
„Sicherheit“

Die Sicherheit *eines Systems* gegen eine *bestimmte Bedrohung* ist die Fähigkeit des Systems, der böswilligen Herbeiführung der dieser Bedrohung zugrundeliegenden Zustände zu widerstehen oder gegen die daraus potentiell folgenden Schäden resistent zu sein.

Bemerkung 1.4:
„Triviale Sicherheit“
Triviale Sicherheit liegt vor, wenn der Interessenträger keinen Zustand oder Vorgang als Schaden ansieht und es deshalb auch keine Bedrohung und keinen Angriff geben kann.

Bemerkung 1.5:
Abgrenzung zur „Safety“
Das Verhalten des Angreifers ist böswillig und zielgerichtet, damit also keine aleatorische Größe. Deshalb sind die im Bereich „Safety“ üblichen Methoden der Abschätzung der Wahrscheinlichkeit einzelner und verknüpft auftretender Fehler hier nicht anwendbar.

Konsequenterweise wäre aber in Betracht zu ziehen, den Fall des zufälligen Findens eines kryptographischen Schlüssels ohne systematische Suche nicht als Angriff, sondern als „Panne“ dem Bereich „Safety“ zuzuordnen.

Damit wird Sicherheit *relativ* zum System und zur Bedrohung definiert. Eine von der Bedrohung abstrahierte, allgemeine Sicherheit gibt es hiernach nicht.

Der Vollständigkeit halber werden hier noch drei in der vorliegenden Arbeit mehrfach verwendete Begriffe definiert:

Definition 1.6:
„Information“, „Daten“, „Nachricht“
Eine *Information* besteht aus dem Eintreten eines für einen bestimmten Beobachter (=Empfänger) nicht zuverlässig vorhersagbaren Ereignisses *und* einer wie auch immer gearteten Interpretation des Eintretens durch den Beobachter. Sie ist damit von der Existenz und der Aufmerksamkeit eines Beobachters abhängig und unterscheidet sich fundamental von der *Formation*, in der Ereignisse exakt vorhersagbar sind[2].

Daten sind technisch verwertbare Darstellungen von Informationen, die nach einem vorgegebenen Schema gebildet werden und die aus einer endliche Folge von Zeichen aus einem endlichen Zeichenvorrat bestehen.

Nachrichten sind Daten, die semantisch und syntaktisch einem bestimmten Protokoll entsprechen und eine abgeschlossene Einheit dieses Protokolls bilden.

Bemerkung 1.7:
Beschränkung auf digitale Daten
Die vorliegende Arbeit beschränkt sich ausschließlich auf *digitale* Daten. Daher ist die Einschränkung auf endliche Folgen von Zeichen aus endlichen Zeichenvorräten zulässig.

[2] . . . und daher keine mehr sind.

1.3 Was ist Kryptographie?

Immer wenn es darum geht, Nachrichten so zu übermitteln, daß der Gegner sie nicht lesen kann, liegt der Gedanke an Geheimschriften und Verschlüsselungen – also klassische kryptographische Methoden – nahe. Was genau ist aber Kryptographie und wie ist sie in das dieser Arbeit zugrundegelegte Konzept einzuordnen? Im Fremdwörterbuch [50] findet sich folgende Definition:

> **Kryptographie** *die*; -, ...ien: 1. absichtslos entstandene Kritzelzeichnung bei Erwachsenen (Psychol.). 2. (veraltet) Geheimschrift.

Diese Definition hilft hier nicht weiter.[3] Schneier gibt in [108] die wenig tiefschürfende und ziemlich inhaltsleere Erklärung:

> „The art and science of keeping messages secure ist **cryptography**, and it is practiced by **cryptographers**."

Diese Definition grenzt die Kryptographie nicht von anderen Sicherungsmethoden ab. Eine Nachricht (bzw. deren Medium) zu verbrennen oder alle Angreifer zu erschießen wäre nach dieser Definition ein Akt der Kryptographie. Dieser Ansatz hätte durchaus seine Vorteile und fände zweifellos viele Freunde, soll hier aber nicht weiter verfolgt werden. Außerdem steht der Begriff „secure" hier isoliert und ohne Kontext, ist also unklar (vgl. 1.2).

Viele Werke gehen sogar ganz über eine Definition hinweg. In [107] wird die Kryptographie immerhin als die „Wissenschaft der Prinzipien und Methoden definiert, mit denen Information mit Hilfe von Schlüsseln chiffriert und von berechtigten Empfängern wieder dechiffriert werden kann." Diese Definition enthält bereits den Hinweis auf den Schlüssel und den Berechtigten, faßt aber die Kryptographie zu eng, indem sie nur auf die Verschlüsselung beschränkt wird.

Auch andere Definitionen legen „Kryptographie" sehr eng aus und verstehen darunter nur die Verschlüsselung. Andere Bereiche wie Steganographie, Signaturen, Kryptoanalyse usw. werden dann zusammen mit der Kryptographie dem Oberbegriff „Kryptologie" untergeordnet.

Den unterschiedlichen Definitionen des Begriffs „Kryptographie" ist jedoch eines gemeinsam: Sie beruhen auf einem Übersetzungsfehler und sind somit eigentlich falsch. Da alle Begriffe dem Altgriechischen entnommen wurden, sollen in Tabelle 1.1 daher zunächst die wortwörtlichen Übersetzungen einiger relevanter Begriffe betrachtet werden [57, 84, 85].

[3] Es sei aber bemerkt, daß ein Abgeordneter des Deutschen Bundestages im Rahmen einer Diskussion über das Für und Wider eines Kryptographieverbotes die erste der beiden Definitionen verwendet hat [100].

ἡ ἀνάλυσις	1. Auflösung, Ende, Tod. 2. Erlösung von. 3. Aufbruch.
ἄδηλος	1. verborgen, unsichtbar, dunkel, geheim; 2. unbekannt, unsicher, ungewiß, unbestimmt
ἀδήλως *(adv.)*	verborgen, im geheimen
γράφω	1. (act) in Wachs einritzen, in Stein einhauen, eingraben, malen, schreiben; 2. (med.) für sich aufschreiben
κρυπτός	verborgen, geheim, heimlich, versteckt
κρύπτω	1. verbergen, verstecken, verhüllen; bergen, begraben; a) verhehlen, verheimlichen, verschweigen, b) schützen, decken; 2. *(intr.)* verborgen sein, sich verstecken.
λόγος	1. Mitteilung, Wort, Rede, Erzählung, Sage, Nachricht, Gerücht. 2. Ausspruch Gottes, Befehl, Weissagung, Lehre. 3. Satz, Behauptung, Lehrsatz, Definition
στεγανός	1. bedeckt. 2. bedeckend, schützend, festschließend, dicht.
στεγανῶς *(adv.)*	durch eine geschlossene Röhre
στέγω	1. decken, bedecken: a) umschließen, bergen; verbergen. b) entschuldigen. – 2. a) schützen, abhalten, widerstehen. b) verschweigen, nicht verraten. c) ertragen, aushalten, dulden.
ἡ τέχνη	1. Kunst, Wissenschaft, Handwerk, Gewerbe. 2. Kunstfertigkeit, Kunstverständnis, wissenschaftliche Tüchtigkeit; Einsicht, Verständnis, Geschicklichkeit, Schlauheit. 3. Kunstwerk

Tabelle 1.1: Altgriechische Vokabeln

Wie man leicht sieht, hat die Wissenschaft die Begriffe *Kryptographie* und *Steganographie* gegenüber ihrer wortwörtlichen Bedeutung gerade vertauscht.

Eigentlicht müßte das heimliche, versteckte, nicht erkennbare Übertragen von Nachrichten nicht als *steganographisch*, sondern als *kryptographisch* bezeichnet werden[4].

Demgegenüber drängt sich der Begriff στεγανός mit seiner Bedeutung von *schützend, festschließend, dicht* geradezu auf, um eine Chiffre zu charakterisieren. Die Übersetzung des Adverbs mit *„durch eine geschlossene Röhre“* ist eine überaus treffende Beschreibung für den *sicheren Kanal*.

Der Begriff ἄδηλος trifft mit seiner Doppelbedeutung sehr gut beide Bereiche und könnte als Oberbegriff dienen.

[4]Eine „Krypta“ ist auch kein gut verschlossenes, sondern ein unterirdisch verborgenes und schwer zu entdeckendes Gewölbe.

Definition 1.8:
„Steganographie“ und „Kryptographie“ die I.
Eine sprachlich korrekte(re) Definition wäre es,

Kryptographie als das verborgene Schreiben zu definieren, darunter also Schreibtechniken zu verstehen, die die *Zeichen* unsichtbar machen bzw. verstecken (z. B. Schreiben mit Chemikalien oder Verstecken von Informationen in Bildern), also vornehmlich die *Syntax* schützen,

Steganographie als das unlesbare Schreiben zu definieren, darunter also Schreibtechniken zu verstehen, die die Nachricht *unverständlich* machen (z. B. verschlüsseln), also vornehmlich die *Semantik* schützen und

Adälographie als Oberbegriff für alle Geheimschreibtechniken zu verwenden.

Diese Definition ist allerdings nicht durchsetzbar, weil sich die Begriffe *Kryptographie* und *Steganographie* schon in der vertauschten Bedeutung festgesetzt haben. Die innere Befriedigung einer sprachlich genaueren Definition kann den Aufwand und die Probleme einer Umdefinierung nicht aufwiegen. Aufgrund der Gegebenheiten muß diese Vertauschung also leider beibehalten werden.

Aus Gründen der Abdeckung auch neuerer Techniken und unter Berücksichtigung der wortwörtlichen Übersetzung von „Kryptographie“ ist es sinnvoll, das Geheimnis (κρυπτός) nicht mehr zwingend auf das Geschriebene zu beziehen, sondern alle Schreib- und Lesetechniken, die (befugtermaßen) Geheimnisse verwenden, zuzulassen. Damit fallen auch Signaturen, Challenge-Response-Verfahren usw. unter den Begriff „Kryptographie“. Die „Analyse“ ist das Gegenstück, nämlich ohne Geheimnis – und damit unbefugt – das zu tun, wozu das Geheimnis notwendig sein sollte.

Eine gewisse Modernisierung und Anpassung an die Computertechnik ist beim Begriff „Graphie“ Übersetzung zeigt (s.o.), ist der Begriff nicht nur mit dem rein handschriftlichen Schreiben zu übersetzen (das es in der heutigen Form bei Entstehung dieses Begriffes ohnehin noch nicht gab), sondern mit *dem zeitlichen oder räumlichen Übertragen von Information.* Mit Hinblick auf den Verwendungszweck soll darunter nur das *befugte* Übertragen zu verstehen sein. Weil Schreiben ohne Lesen wenig Sinn macht, soll hierunter auch das *befugte Lesen* mitverstanden werden[5].

Daher werden hier folgende Definitionen verwendet:

Definition 1.9:
„Geheimnis“
Ein *Geheimnis* ist eine Nachricht (vgl. Definition 1.6) mit folgenden Eigenschaften:

[5] Analog zu der Tatsache, daß die für sich schon beachtliche Erfindung des Telefons erst durch die Erfindung des zweiten Telefons aufgewertet und voll zur Geltung gebracht wurde.

- Es gibt mindestens einen, der sie kennt bzw. verwenden kann[6].
- Es gibt mindestens einen, der sie *nicht* kennt.
- Es gibt einen Interessenträger, der eine Vorstellung davon hat, wer die Nachricht kennt oder verwenden kann und wer nicht, und der einen davon abweichenden Zustand als Schaden ansieht. (Womit die Verletzung und ggf. der Verlust des Geheimnisses zur Bedrohung werden.)

Definition 1.10:
„Steganographie“ und „Kryptographie“ die II.

Krypto*logie* ist der Oberbegriff für die Wissenschaft und Lehre von der systematischen Verwendung von Geheimnissen.

Krypto*graphie* ist die Kunst und Wissenschaft von der *inhaltlich* geschützten (zeitlichen oder räumlichen) Übertragung von Informationen *unter systematischer Verwendung* von Geheimnissen.

Im Kontext der vorliegenden Arbeit wird darunter speziell die Wissenschaft der Verfahren zur Sicherung von Datenübertragungen verstanden, die auf einer Verlagerung auf Kenntnis und Nichtkenntnis eines Geheimnisses beruhen, bei denen sich also die befugte Partei von der unbefugten durch Kenntnis eines Geheimnisses unterscheidet.

Krypto*analyse* ist die Kunst und Wissenschaft des *Aufbrechens* oder *Auflösens* von Geheimnissen, d. h. deren Aufdeckung oder Umgehung.

Steganographie ist die Kunst und Wissenschaft vom Verstecken der Zeichen und der Syntax eines Übertragungsverfahrens (vgl. Abschnitt 5.3.4).

Chiffre ist die Bezeichnung für ein Verschlüsselungsverfahren[7].

Chiffrat ist eine Nachricht in verschlüsselter Form.

Damit umfaßt Kryptographie nicht mehr nur die Kunst des Geheimschreibens, sondern verallgemeinert die Kunst des Schreibens unter Verwendung von Geheimnissen. Wie man leicht sieht, hat obige Definition durch den Aspekt der Verlagerung etwas „Rekursives“ an sich, denn die Sicherheit der Informationsübertragung hängt von der Sicherheit der Übertragung der Geheimnisinformation ab. Das ist jedoch kein Widerspruch, sondern eine (manchmal vertrackte) Eigenschaft der Kryptographie. Diese Überlegung zeigt aber, daß kryptographische Methoden nie für sich alleine eingesetzt werden können, sondern am Ende der Sicherungskette immer eine andere Methode stehen muß.

[6] Hierunter soll auch zu verstehen sein, daß mehrere zusammen das Geheimnis verwenden können.
[7] vgl. „Ziffer“ und „entziffern“ (aus dem Arabischen)

Kryptographische Methoden können aber Probleme soweit verkleinern und verlagern, bis eine andere Methode praktikabel durchführbar ist. Das ist Sinn und Zweck der Kryptographie.

1.4 Bestehende Kriterien- und Maßnahmenkataloge

1.4.1 Überblick über wichtige Werke

Es gibt eine Vielzahl von unterschiedlichen Kriterien- und Maßnahmenkatalogen zu Themen wie der Systemsicherheit und der Zertifizierung von Systemen. Eine vollständige Darstellung würde hier aber zu weit führen und wäre außerdem redundant, denn viele der Kataloge sind voneinander abgeleitet oder einander sehr ähnlich. Deshalb werden nur die wichtigsten und meistverwendeten Werke kurz beschrieben. Eine Bewertung der Kataloge erfolgt in Abschnitt 1.4.2.

1.4.1.1 DoD Trusted Computer System Evaluation Criteria (TCSEC, „Orange Book“)

Der Department of Defense Standard, DoD 5200.28-STD[98] vom Dezember 1985, „Trusted Computer System Evaluation Criteria (TCSEC)“, bekannter unter dem Namen „Orange Book“, ist der bekannteste Kriterienkatalog zur Beurteilung von automatisierten Datenverarbeitungssystemen. Die Einteilung erfolgt nach sieben Klassen (D, C1, C2, B1, B2, B3, B4), die in vier Gruppen zusammengefaßt sind (D, C, B und A). Diese werden in Tabelle 1.2 kurz zusammengefaßt. Details werden in [98] beschrieben.

1.4.1.2 An Introduction to Computer Security: The NIST Handbook

Das National Institut of Standards and Technology, U. S. Department of Commerce gibt das sog. „NIST Handbook“ [94] heraus. Zweck und Zielgruppe dieses Buches sind klar definiert:

> *„The purpose of this Handbook ist to assist managers in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. . . . The Handbook targets federal employees who have computer security responsibilities, but need assistance understanding computer security concepts and techniques.“*

D	Niedrigste Stufe. Das System wurde geprüft, konnte aber keine höhere Stufe erringen.
C1	Das System unterscheidet zwischen verschiedenen Benutzern und verschiedenen Datenobjekten. Für Datenobjekte lassen sich Zugriffsrechte für Benutzer und Benutzergruppen festlegen.
C2	Zusätzlich zu C1 müssen sich Benutzer durch eine Login-Prozedur identifizieren. Sicherheitsrelevante Vorgänge werden protokolliert. Die Zugriffsrechte sind feiner und können für einzelne Benutzer und Objekte definiert werden. Speicherbereiche werden initialisiert.
B1	Zusätzlich zu C2 muß es eine obligatorische Zugriffskontrolle für Datenobjekte, Benutzer, Prozesse, Geräte usw. geben. Datentypen müssen unterschieden und bezeichnet werden können. Es gibt eine nicht-formale Beschreibung der Sicherheitsregeln.
B2	Es gibt ein klar definiertes und dokumentiertes Sicherheitsmodell, das auf alle Objekte, Benutzer, Prozesse, Geräte usw. angewandt wird. Verdeckte Kanäle werden vermieden. Die Schutzmechanismen sind wohldefiniert, geprüft und getestet.
B3	Alle Zugriffe von Benutzern auf Objekte werden kontrolliert. Das System ist so klein, daß es systematisch analysiert und getestet werden kann. Das System enthält nur sicherheitsrelevante Funktionseinheiten und keine überflüssigen oder anderen Zwecken dienende Teile.
A1	Entspricht B3, jedoch anhand der formalen Spezifikation geprüft und verifiziert.

Tabelle 1.2: TCSEC-Klassen

Das NIST Handbook ist eine sehr gute Einführung und vermittelt einen Überblick über die Prinzipien und Methoden der Systemsicherheit. Seinem Zweck und seiner Zielgruppe entsprechend ist es aber nur für „Entscheidungsträger“ gedacht und behandelt nicht den eigentlichen Entwurf von Systemen.

1.4.1.3 Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)

Eine Kommission der Europäischen Gemeinschaften hat „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)“ erarbeitet[8] [68]. Die darin aufgelisteten Kriterienklassen sind von den TCSEC-Klassen abgeleitet, aber

[8] ITSEC und ITSEM (s.u.) liegen in mehreren Sprachen vor. Wesentlich beteiligt waren Frankreich, Deutschland, die Niederlande und Großbritannien.

nicht mit ihnen deckungsgleich. Sie wurden im Rahmen einer Harmonisierung von mehreren europäischen IT-Sicherheitskriterienkatalogen entwickelt und stellen somit auch einen Konsens dar.

Die ITSEC beschreiben u. a. eine Klassifikation der Sicherheitsvorgaben und verschiedene Zertifizierungsstufen.

1.4.1.4 Information Technology Security Evaluation Manual (ITSEM)

Aufbauend auf ITSEC wurde ein Evaluierungshandbuch entwickelt [53]. Darin wird der Ablauf der Evaluierung nach den ITSEC-Kriterien beschrieben. Das ITSEM ist daher eine Ergänzung der ITSEC.

1.4.1.5 IT-Grundschutzhandbuch

Das BSI gibt eine Sammlung von Sicherheitsempfehlungen, das „IT-Grundschutzhandbuch – Maßnahmenempfehlungen für den mittleren Schutzbedarf“ heraus [29, 30]. Dieses Handbuch ist eine für seine Zielgruppe durchaus sehr nützlicher und empfehlenswerter Maßnahmenkatalog. Er richtet sich jedoch nicht an den Informatiker, der ein System entwirft oder beurteilt, sondern an den weniger sachkundigen Anwender, der Computersysteme aufstellen und betreiben will. So sind darin auch Ratschläge für die räumliche und personelle Situation enthalten. Zu bemerken ist jedoch, daß „Safety“ und „Security“ darin nicht differenziert und gelegentlich vermischt werden.

1.4.1.6 IT-Sicherheitshandbuch

Ebenfalls vom BSI herausgegeben wird das „IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik“ [27]. Es richtet sich an Anwender der Informationstechnik, vornehmlich an Behörden, nicht jedoch an den Informatiker. Es enthält Anleitungen und Kriterien zur Aufstellung von Bedrohungsanalysen und Erstellung von Sicherheitskonzepten; es behandelt jedoch nicht den Entwurf und die Bewertung der inneren Funktionen sicherheitsrelevanter Systeme, sondern behandelt deren Anwendung und Einsatz.

1.4.2 Kritik

Die bestehenden und in der Praxis verwendeten Kriterien- und Maßnahmenkataloge erscheinen vom hier vertretenen Standpunkt der technischen Sicherheit aus betrachtet als unzureichend für den Entwurf und die Analyse von Kommunikationssystemen.

Die Eigenschaften der Kataloge, gegen die sich die Kritik dabei richtet, sind nicht auf einzelne Kataloge beschränkt, sondern jeweils in mehreren – oder allen hier erwähnten – Katalogen anzufinden. Aus diesem Grund und weil nicht die Kataloge selbst

angegriffen, sondern die als mangelhaft angesehenen Eigenschaften kritisiert werden sollen, erfolgt eine gesammelte Betrachtung.

Der Kern der Kritik richtet sich dabei gegen die folgenden Eigenschaften:

- Die Kataloge sind *veraltet*. Gegenstand der Betrachtung ist überwiegend die Systemsicherheit, also der Schutz von Rechenanlagen und die Rechtevergabe auf diesen. Diese Sichtweise rührt von den früher üblichen Zentralrechnern her, auf denen eine Vielzahl von Benutzern zugange ist. Eine Vernetzung wird jedoch nicht gesondert betrachtet. Als Feindbild wird implizit das klassische, aber nicht mehr zeitgemäße Feindbild des Spions angesehen, der körperlich in das Gebäude eindringt („Putzfrau“) und sich direkt an Terminals usw. zu schaffen macht.

  Die inzwischen stark erhöhte Bedeutung der Telekommunikation und der nichtphysischen Angriffe wird nicht ausreichend berücksichtigt.

- In der Folge dessen steht auch nicht der *Zweck*, sondern das *System* im Mittelpunkt. Es werden überwiegend absolute Eigenschaften des Systems beschrieben und evaluiert, nicht dessen Eignung für bestimmte Zwecke. Dies deutet auf die militärische Herkunft der Kataloge hin.

- Der Einsatzzweck des Systems wird vernachlässigt. Eine Beschreibung der Sicherheitsanforderungen der geplanten Anwendung erfolgt praktisch nicht.

  Zertifizierungen beziehen sich darauf, ob ein vom Antragsteller behauptetes Sicherheitsziel erfüllt ist, nicht ob das Produkt für eine bestimmte Anwendung geeignet ist.

- Die Sicherheitsbetrachtungen erfolgen nicht aus wissenschaftlicher, sondern aus behördlicher Sichtweise. Sie enthalten Verhaltensmaßregeln, aber keine Entwurfskriterien.

- Es erfolgt praktisch keine Differenzierung zwischen „Safety“ und „Security“. Beide werden durcheinandergeworfen, obwohl etwa bezüglich der Bedrohung erhebliche Unterschiede bestehen.

- Es erfolgt praktisch keine Differenzierung zwischen „Sicherheit“ und „Korrektheit“ (vgl. Abschnitt 1.6.1). Beide werden oft miteinander verwechselt.

- Daraus resultiert eine Fehl- und Überbewertung semiformaler und formaler Beschreibungsmethoden (vgl. auch Abschnitt 1.6).

Systeme, deren Spezifikation in semiformaler oder gar formaler Darstellungsform beschrieben wird, werden höher eingestuft als andere Systeme. Es ist jedoch nicht ersichtlich, warum hierdurch mehr Sicherheit oder eine bessere Eignung vorliegen soll. Auch werden an die semiformale oder formale Darstellung keine qualitativen Anforderungen gestellt, die diese Besserbehandlung rechtfertigen könnten.

Als semiformale Darstellung werden etwa graphische Darstellungen und Darstellungen akzeptiert, die auf einer eingeschränkten Nutzung der Umgangssprache aufgebaut sind, z. B. eingeschränkte Satzstruktur und Schlüsselworte mit spezieller Bedeutung (siehe ITSEC 2.73 [68]). Es ist nicht nachvollziehbar, wie es die Sicherheit eines Systems verbessern soll, wenn es statt mit normaler nur mit beschränkter Sprache und eingeschränkter Satzstruktur beschrieben wird.

Tatsächlich vereinfacht, verbessert und ermöglicht eine (semi-)formale Spezifikation die Verifizierung und Evaluierung. Erst diese würden es aber rechtfertigen, formal spezifizierten Systemen das Erreichen einer bestimmten Stufe gegenüber anderen Systemen zu erleichtern. Eine höhere Sicherheitsstufe allein aufgrund der formalen Spezifikation zu vergeben ist irreführend.

Es handelt sich daher nur um Abstufungen der Prüfung auf Korrektheit, nicht der Sicherheit (vgl. Abschnitt 1.6.1).

- Letztlich beschreiben daher insbesondere die auf Zertifizierung ausgelegten Kataloge nicht, wie man ein System *sicher* macht, sondern wie man es *zertifiziert* bzw. die Zertifizierung erreicht. Die Zertifizierung belegt schon formal nicht die Sicherheit, sondern die Überprüfung einer willkürlichen Behauptung des Antragstellers.

1.5 Zertifizierungen und Evaluierungen

1.5.1 Zertifizierungen des BSI

Die derzeit in Deutschland übliche Art der Sicherheitszertifizierung ist die Erstellung eines Sicherheitszertifikates durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), die hier kurz beleuchtet werden soll.

Hersteller und Vertreiber können ein Zertifikat für informationstechnische Systeme oder Komponenten beim BSI nach § 4 BSIG [24] beantragen. Nach § 4 Abs. 2 BSI-ZertV [25] muß das Sicherheitszertifikat folgende Angaben enthalten:

1. Bezeichnung, Beschreibung und Hersteller des geprüften Produkts,

2. Liste der zum geprüften Produkt gehörenden Anwenderdokumentation,
3. Prüfgrundlagen, soweit sie bekannt gemacht sind,
4. Prüfstelle, deren Prüfung und Bewertung der Zertifizierung zugrunde gelegt wurde,
5. Beschreibung der Sicherheitsfunktionen,
6. erreichte Bewertungsstufe,
7. etwaige Auflagen und Beschränkungen des Gültigkeitsumfangs und
8. Ausstellungsort und -datum der Zertifizierung.

Dabei werden jedoch nicht einmal alle Komponenten des Produkts geprüft. In Zertifikaten des BSI (z. B. [140]) findet sich folgende Feststellung:

> **Zitat 1.11: Aus den Zertifikaten des BSI:**
> *„Die Sicherheit der für die Ver- und Entschlüsselung geeigneten Kryptoalgorithmen wurde nicht geprüft, da der Zertifizierung solcher Kryptoalgorithmen nach Feststellung des Bundesministeriums des Innern generell überwiegende öffentliche Interessen im Sinne des § 4 Abs. 3 Nr. 2 BSIG entgegenstehen.“*

Die für die Sicherheit wichtigsten Komponenten des Produkts werden also im Rahmen der „Sicherheitszertifizierung“ gar nicht geprüft. Die Formulierung erweckt den Eindruck, daß die Prüfung von Kryptoalgorithmen unmittelbar einem gesetzlichen – und damit demokratisch zustandegekommenen, veröffentlichten und nachvollziehbaren – Verbot zuwiderlaufen. Die entsprechende Stelle im *Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz – BSIG)* vom 17.12.1990 [24] enthält jedoch nur eine Ermächtigung des Bundesministers des Innern:

> **Zitat 1.12: § 4 Abs. 3 Nr. 2 BSIG:**
> *Das Sicherheitszertifikat wird erteilt, wenn . . . der Bundesminister des Innern festgestellt hat, daß überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland der Erteilung nicht entgegenstehen.*

Die Prüfung von Kryptoalgorithmen ist offensichtlich unerwünscht. Es nicht Gegenstand der vorliegenden Arbeit, dies politisch oder moralisch zu bewerten. Aber auch aus technisch-wissenschaftlicher Sicht ist es höchst fragwürdig, Sicherheitszertifikate auszustellen, die Sicherheitsalgorithmen dabei aber nicht prüfen zu wollen.

Auch bei den Produktkomponenten, die tatsächlich geprüft werden, ist nicht sichergestellt, daß die Prüfkriterien ersichtlich sind [25]:

Zitat 1.13: § 3 BSIZertV:
Der Bundesminister des Innern macht die vom Bundesamt festgelegten Sicherheitskriterien im Bundesanzeiger öffentlich bekannt, es sei denn, daß dadurch die Sicherheit bestimmter Produktkategorien beeinträchtigt wird oder die Sicherheitskriterien als Verschlußsache eingestuft sind. Das Bundesamt gibt nicht bekanntgemachte Sicherheitskriterien Herstellern, Vertreibern und sachverständigen Stellen bekannt, wenn diese gegenüber dem Bundesamt ein berechtigtes Interesse und die Einhaltung notwendiger Sicherheitsvorkehrungen nachweisen.

Diese Art der Sicherheitszertifizierung ist nicht überzeugend. Besonders fragwürdig ist der Umstand, daß nach dem Gesetz für den Fall zuwiderlaufender staatlicher Interessen *überhaupt kein* Zertifikat ausgestellt werden dürfte, nicht aber eines über ein tatsächlich nicht oder nicht vollständig geprüftes Produkt.

1.5.2 Konkrete Betrachtung einer Zertifizierung

Um diese Aussage zu untermauern wird beispielhaft die Zertifizierung eines in JAVA geschriebenen Programmpaketes zur Absicherung von Dienstleistungen im Internet, vornehmlich „Telebanking“, „Online-Zahlungsverkehr“ und „Online-Auftragsabwicklung“, näher beleuchtet. Auf die Einzelheiten des Zertifizierungsreports [140] wird verwiesen.

1.5.2.1 Integrität der Klientensoftware bei der Übertragung

Das Produkt besteht hauptsächlich aus JAVA-Bibliotheken zum Aufbau der Klientenseite und dem Serverprogramm auf der Anbieterseite. Die JAVA-Software für die Klientenseite wird dabei jedoch nicht auf einem vertrauenswürdigen gesonderten Kanal – z. B. durch persönliche Übergabe einer CD-ROM durch die Bank an den Kunden – sondern über das Internet und damit über einen per se höchst unsicheren Kanal übertragen. Von der Integrität und der Authentizität der JAVA-Software hängt jedoch die Sicherheit des Gesamtsystems ab. Zu dieser entscheidenden Frage findet sich im Zertifizierungsreport die Bemerkung:

> *Der EVG*[9] *bietet selbst keine Möglichkeiten zur Authentisierung des Web-Servers des Dienstleistungsanbieters. Eine indirekte Authentisierung dieses Web-Servers ohne Beteiligung des EVG erfolgt jedoch durch die Nutzung von Schlüsselzertifikaten der Firma VeriSign Inc. Diese indirekte Authentisierung wurde nicht evaluiert.*
>
> . . .

[9] EVG = Evaluationsgegenstand

Der öffentliche Schlüssel des RSA-Schlüsselpaares von VeriSign der Länge 1024 bit ist in dem Java-Browser-Code enthalten.

Diese Vorgehensweise setzt sich über die Problematik der Problemverlagerung (s. Abschnitt 4.3) hinweg. Weder ist geklärt, wie die Integrität und die korrekte Funktionsweise des Betriebssystems oder des „Web-Browsers“ sichergestellt werden können, noch wird berücksichtigt, daß gängige Web-Browser die Identität des Programmautors nur auf eine Benutzeranfrage hin anzeigen, was aber die Mehrzahl der Benutzer vom Verständnis her überfordert. Der Browser zeigt bei Aufforderung an, daß eine Signatur vorliegt, daß sie korrekt ist und von wem sie stammt. Ob der aber mit dem übereinstimmt, von dem sie stammen *soll*, kann der Benutzer nicht ohne weiteres erkennen. Eine Bewertung der Vertrauenswürdigkeit der Firma VeriSign findet nicht statt. Damit ist die Integrität der Übertragung der Applets nicht dargelegt.

1.5.2.2 Integrität des Programmlaufes

Selbst wenn die Klientensoftware (JAVA-Applets) unverändert beim Benutzer ankommt, so ist damit nicht gewährleistet, daß der Programmlauf dem Programm entspricht. Der Programmlauf hängt auch von den darunterliegenden Schichten und Programmschalen ab, nämlich (u.a.)

- den JAVA-Laufzeitbibliotheken,
- der virtuellen JAVA-Maschine,
- dem Web-Browser,
- den von diesem geladenen Laufzeitbibliotheken,
- der Benutzerschnittstelle und zugehörigen Programmen und Bibliotheken,
- dem Betriebssystem und
- der Hardware und den Zugriffsschutzmechanismen für Platten, Hauptspeicher usw.

Mit einem Angriff gegen eine dieser Komponenten des verwendeten Systems wäre der Programmlauf so zu verändern, daß Vertraulichkeit, Integrität und Authentizität der abgewickelten Geschäfte nachhaltig beeinträchtigt werden, was aber im Zertifizierungsreport unberücksichtigt bleibt.

Das in dem hier relevanten Anwenderbereich derzeit meistverwendete Betriebssystem ist „Windows 95“. Es besitzt keine Zugriffsrechteverwaltung und keinen wirksamen Speicherschutz. Die hohe Dichte an Sicherheitslücken ist geradezu legendär und ernährt eine eigene Branche von Virenschutzprogrammherstellern und ähnlicher Monstrositäten. Installationen sind typischerweise höchst unübersichtlich; für den (meist wenig erfahrenen) Anwender ist nicht ersichtlich, welche Datei welche Aufgabe hat. Da es üblich ist, daß jedes Anwendungsprogramm beim Aufruf oder bei der Installation willkürlich, ohne Benutzerinteraktion und in kaum nachvollziehbarer Weise Systembibliotheken hinzufügt oder ersetzt und damit das Betriebssystem verändert,

ist die Integrität des Betriebssystems und der Systembibliotheken nicht gewährleistet – im Gegenteil, deren Verletzung ist das Funktionsprinzip.

Durch den unzureichenden Speicherschutz und die nicht gewährleistete Integrität des Systems können leicht feindliche Programme installiert werden, die den Programmlauf anderer Programme – hier des Web-Browsers oder der virtuellen JAVA-Maschine – gezielt beeinflußen.

Überdies werden Programme wie der Web-Browser oder die virtuelle JAVA-Maschine regelmäßig ohne Schutz der Integrität installiert. Sie werden üblicherweise ungeschützt über das Internet geladen oder bei der Benutzung einer CD-ROM installiert. Einem Angriff stehen hier Tür und Tor sperrangelweit offen. Auch hier ist die Verletzlichkeit wieder konterkarierendes Funktionsprinzip.

Da sich schon das Laufzeitverhalten der einzelnen Versionen der Web-Browser unterscheidet, ist nicht einmal ohne gezielten Angriff die beabsichtigte Funktion gewährleistet.

Es ist daher fragwürdig, wenn die Anforderungen an den Client-Rechner so umschrieben werden:

> *Für den sicheren Betrieb des EVG muß auf dem Client-Rechner ein Browser installiert sein, der*
>
> - *die Java Versionen 1.0 oder 1.02,*
> - *das Transport-Protokoll SSL 3.0 der Firma Netscape und*
> - *RSA-Schlüsselzertifikate der Firma VeriSign unterstützt.*
>
> *Diese Voraussetzungen werden z. B. vom Browser Navigator Version 2.02 und höher der Firma Netscape unterstützt.*

Sicherheitsanforderungen an den Browser werden nicht gestellt.[10]

1.5.2.3 Vertraulichkeit der geheimen Schlüssel

Die Sicherheit des verwendeten Verfahrens setzt die Vertraulichkeit des geheimen Schlüssels des Servers voraus. Diese wird jedoch nicht bei der Installation lokal erzeugt, sondern – wie dem Zertifizierungsreport zu entnehmen ist – *mit der Installations-CD im Klartext geliefert.*

Wie hier die Vertraulichkeit der Schlüssel gewährleistet sein soll, ist fraglich.

[10] Es wurden übrigens sowohl in JAVA Version 1.0, als auch in frühen Navigator-Versionen einige implementierungsbedingte Sicherheitslücken gefunden.

1.5.2.4 Übereinstimmung mit dem zertifizierten Produkt

Der Zertifizierungsreport enthält eine Auflistung aller zum zertifierten Produkt gehörenden Dateien mit Name, Größe, Erstellungsdatum und Erstellungsuhrzeit. Diese Angaben sind einerseits trivial und ohne Aufwand zu fälschen, so daß Unterschiede umbemerkt bleiben können. Andererseits können sich die Datumsangaben schon bei einem einfachen Umkopieren ändern und damit den Anschein einer Veränderung erwecken.

Eine bessere Vorgehensweise wäre hier gewesen, zu jeder Datei eine kryptographische Prüfsumme (z. B. MD5 oder SHA) anzugeben, was ohne merklichen Aufwand und ohne nennenswerte Verlängerung des Reports hätte geschehen können.

1.5.2.5 Integrität des Servers

Die Sicherheit des Produktes hängt ebenfalls völlig von der Sicherheit des Servers ab. Über den Server wird jedoch nur gesagt, daß er auf einem Rechner des Typs RS6000 mit dem Betriebssystem AIX 4.1 betrieben wird, nicht in einem frei zugänglichen öffentlichen Bereich befindet und von einem „Administrator“ und einem „Operator“ bedient werden. Der Administrator soll den Server installieren und konfigurieren. Der Operator soll den laufenden Betrieb beobachten und Fehler beheben oder durch eine andere Person beheben lassen.

Diese Anforderung ist inadäquat und nicht geeignet, die erforderliche Sicherheit zu gewährleisten.

- Anforderungen an die Fähigkeiten des Adminstrators, des Operators oder der dritten Person sind nicht erkennbar.
- Welchem Zweck die Unterscheidung zwischen Administrator und Operator dienen und warum Installation und Konfiguration einerseits und Beobachtung und Fehlerbehebung andererseits durch unterschiedliche Personen vorzunehmen sind, ist nicht nachvollziehbar.
- Wer die unbestimmte dritte Person ist und was sie auf dem System zu suchen und zu tun hat, ist nicht erkennbar.
- Es werden keinerlei Anforderungen an die Installation und Pflege des Systems aufgestellt.

  So hätte als Anforderung etwa einfließen müssen, daß CERT-Advisories ständig und mit einer möglichst geringen Latenzzeit zu verfolgen sind. Ist das System betroffen, ist innerhalb vorgegebener Zeit Abhilfe zu schaffen oder das System bis zur Abhilfe vom Netzwerk zu trennen.

  Es ist nicht ersichtlich, wie die Maschine zu konfigurieren und zu warten ist. Hier wäre es angebracht gewesen, eine anderweitige Nutzung der Maschine zu

untersagen, Log-Dateien und die Anfertigung von Backups vorzuschreiben, die uid- und Rechtevergabe zu beschreiben und die Abschaltung *aller* anderen Netzwerkdienste zu verlangen.

Es werden ebenfalls keine Anforderungen für die Anbindung der Maschine an das Internet erhoben. Hier wäre zu spezifizieren gewesen, welchen Schutzes die Maschine durch Router, Firewalls, Paketfilter usw. bedarf.

1.5.2.6 Vorgehensweise

Die Vorgehensweise der Zertifizierung ist ungeeignet.

Zu den Sicherheitszielen und Bedrohungen heißt es lapidar:

> *Die Sicherheitsziele des EVG sind die Wahrung der Vertraulichkeit und der Integrität von Transaktionsdaten während der Übertragung über das Internet.*
>
> *Als Bedrohungen werden dabei angenommen:*
>
> *B1 Während der Datenübertragung vom Client zum Server über das Internet wird der Inhalt einer Nachricht einem Unbefugten zugänglich.*
>
> *B2 Während der Datenübertragung werden die Daten unterwegs manipuliert, ohne daß diese Verletzung der Integrität von dem Client bzw. dem Web-Server als Empfänger sofort festgestellt werden kann.*

Abgesehen davon, daß hier als Ziele und als Bedrohungen zweimal das gleiche gesagt wird, sind diese Ziele völlig unzureichend.

Der Einsatz dieses Produktes ist kein Selbstzweck, es wird nicht um seiner selbst willen benutzt. Zweck der Sache ist die Abwicklung von Verfügungen, etwa einer Banküberweisung. Die Sicherheitsziele haben sich danach zu richten, was mit dem Produkt erreicht werden soll, nicht aber danach, was das Produkt gerade zu leisten imstande ist.

Die korrekte Vorgehensweise wäre gewesen, zunächst völlig unabhängig von Produkt, Medium usw. die Anforderungen an die Transaktionen zu definieren. Für eine Banküberweisung könnte man etwa fordern:

> **Beispiel 1.14:**
> **Sicherheitstechnische Anforderungen an eine Banküberweisung**
>
> - Vertraulichkeit des Inhaltes während der räumlichen Übertragung
> - Vertraulichkeit der Kundenidentität während der räumlichen Übertragung
> - Identifizierung und Authentifizierung von Bank und Kunde

- Erhaltung der Integrität und Authentizität in zeitlich großer Ausdehnung, also insbesondere über den räumlichen Übertragungsvorgang hinaus.
- Bindung der Integrität und Authentizität an die Nachricht, nicht nur an den Vorgang[11].
- Beweisbarkeit und Unabstreitbarkeit *des Vorgangs, des Inhaltes und des Übertragungszeitpunktes* in einer Dritten gegenüber beweisfähigen und damit im Streitfall gerichtsverwertbaren Form, also
- Beweisbarkeit bei Abstreiten durch die Bank,
- Beweisbarkeit bei Abstreiten durch den Kunden und
- Beweisbarkeit bei Abstreiten durch Dritte (z. B. zum Beweis einer Zahlung bei der Steuererklärung) und in der Folge dessen auch
- Eindeutigkeit, also die Unwiederholbarkeit eines Vorgangs (d. h. daß eine Überweisung nicht zweimal ausgeführt werden kann).
- Verfügbarkeit (die z. B. nicht mehr vorliegt, wenn alle TANs verbraucht sind).

Die altmodische Weise des Überweisens mittels eines Papierformulars mit Erstellung einer abgestempelten Empfangsbestätigung durch die Bank entspricht diesen Anforderungen normalerweise weitgehend.

Erst auf Grundlage solcher Anforderungen *an die Banküberweisung schlechthin* kann evaluiert werden, ob ein Produkt diese Anforderungen und Spezifikationen erfüllt. Erfüllt es diese, dann kann es *nicht universell*, sondern für den Einsatz *bei Banküberweisungen* zertifiziert werden.

Daher wäre dringendst ein Anforderungskatalog für Transaktionen etc. aufzustellen.

Die in der Zertifizierung dargestellten Sicherheitsziele können den Anforderungen jedenfalls nicht genügen. Stattdessen wird implizit erwartet, daß sich die Anforderungen an Banküberweisungen den Leistungen des Produkts angleichen. Im konkreten Fall ist besonders zu bemängeln, daß der Kunde gar nicht identifiziert und authentifiziert wird und daß keinerlei Dritten gegenüber wirksame Beweise erzeugt werden.

Eine Feindbilderstellung oder eine Differenzierung der Angreiferposition findet nicht statt.

1.5.2.7 Beurteilung der Protokolle

Die Protokolle werden grob beschrieben, aber nicht ausreichend bewertet.

Beispielsweise beruht die Sicherheit des Verfahrens auf einer Zufallszahl, die durch ein auf dem Client-Rechner ablaufendes Applet erzeugt wird. Wie aber ein JAVA-Applet,

[11] Im Unterschied zu heute üblichen Geldautomaten etc.

das in einer virtuellen, stark isolierten, von der realen Maschine weitestgehend abstrahierten und hochdeterministischen virtuellen Maschine ohne die Möglichkeit persistenter Datenspeicherung selbständig kryptographisch feste Zufallszahlen und damit Entropie erzeugen können soll, ist nicht ersichtlich.

1.5.2.8 Stärke des Produkts

Als Prüfergebnis wird festgestellt:

> *„Mindeststärke der Mechanismen:* **hoch***“*

Im Zertifizierungsreport wird jedoch nur angegeben, daß dies die *vom Antragsteller angegebene* Mindeststärke der Mechanismen ist. Der Gehalt der Prüfergebnisses ist daher nicht überzeugend.

„Hoch“ ist keine Aussage. Hier wäre eine Aufwandsabschätzung für einen Zeit- und einen Geldangriff nötig gewesen, also eine Aussage über die erwarteten Kosten eines Angriffs mit geeignet vorgegebener Zeit und die erwartete Dauer eines Angriffs mit vorgegebenen Geldmitteln, sowie eine Abschätzung der Gültigkeitsdauer dieser Abschätzung.

Aufgrund dieser Abschätzung hätte die Zertifizierung die Stärke des Produkts darstellen müssen. Daraus hätte eine Höchstgrenze für überwiesene Beträge und Zahl der Überweisungen pro Zeiteinheit, pro Kunde, pro Server, pro Bank etc. in die Zertifizierung aufgenommen und diese Zertifizierung zeitlich beschränkt bzw. für den Fall unerwarteter technischer Fortschritte widerrufbar gemacht werden müssen.

1.5.2.9 Prüfergebnis

Das Produkt erhielt als Prüfergebnis:

Funktionalität:	Datenverschlüsselung, Nachweis der Datenintegrität
Evaluationsstufe:	E3
Mindeststärke der Mechanismen:	hoch

1.5.3 Bewertung

Wie aufgezeigt wurde, ist nicht sichergestellt, daß das Produkt alle Eigenschaften aufweist, die von Software für Bankverfügungen usw. zu erwarten sind. Teilweise ist sogar ersichtlich, daß diese Eigenschaften gerade nicht vorliegen. Dennoch erhält das Produkt eine vergleichsweise hohe Evaluationsstufe und die Bescheinigung starker Mechanismen.

Die Funktionalitäten „Datenverschlüsselung“ und „Nachweis der Datenintegrität“ sind nicht aussagekräftig genug. Es ist nicht ersichtlich, ob sich dies auf Datenübertragung oder Datenspeicherung bezieht und wem gegenüber der Nachweis erbracht werden kann (ob also etwa der Absender, der Empfänger oder gar ein Dritter sich von der Integrität überzeugen können).

Obwohl die Zertifizierung genau betrachtet eigentlich nicht die Eignung für Bankverfügungen usw. bedeutet, wird diese durch das Evaluationsergebnis und die Produktbeschreibung suggeriert.

Gefährlicher als ein potentiell unsicheres Produkt ist ein solches Produkt mit einer nachlässigen Zertifizierung, die den Anschein erwiesener Sicherheit erweckt.

An der betrachteten Zertifizierung bestehen insbesondere folgende Kritikpunkte:

- Es fehlt eine Beschreibung der Randbedingungen, von denen die Sicherheit des Produktes abhängt, etwa der notwendigen Funktionen, die nicht Teil des Produktes sind oder der neuen Probleme, die sich aus dem Produkt ergeben.

- Das Produkt ist nicht für sich alleine funktionsfähig, sondern auf andere Komponenten – JAVA Laufzeitbibliotheken, virtuelle Maschine, WWW-Browser, Betriebssystem usw. – angewiesen, die nicht evaluiert wurden. Eine Bedrohungsanalyse findet aber nicht statt. Auch eine etwaige Isolierung der Komponenten und Schichten gegeneinander wird nicht betrachtet.

- Die Evaluierung erfolg abstrahiert vom Einsatzzweck. Zertifiziert wird nicht der zweckgerichtete Einsatz des Produkts, sondern das Produkt selbst.

  Die Beurteilung der Eignung wird dem Anwender bzw. dem beweisnehmenden Dritten überlassen; die dazu nötigen Informationen werden nicht geliefert.

- Es wird nicht dargestellt, wer Interessenträger der Sicherheit ist (siehe hierzu auch Beispiel 2.25 auf Seite 60).

1.6 Formale Sicherheitsmodelle

Zur Bestimmung und Vergabe sind verschiedene formale Sicherheitsmodelle entwikkelt worden, die hauptsächlich im militärischen oder kommerziellen Bereich Verwendung finden. Die Angabe eines formalen Sicherheitsmodells wird auch bei Zertifizierungen berücksichtigt (siehe Abschnitt 1.5) und ist Voraussetzung für die Vergabe bestimmter Evaluierungs- oder Sicherheitsstufen. Nachfolgend werden daher einige dieser Modelle beispielhaft kurz dargestellt.

Solchen formalen Modellen ist aber auch gewisse Skepsis entgegenzubringen, was ebenfalls nachfolgend dargelegt wird.

1.6.1 Grundprobleme Formaler Modelle

1.6.1.1 Sicherheitsinteressen

Sicherheit ist keine absolute Eigenschaft. Sie wirkt immer relativ gegen bestimmte Bedrohungen. Eine Sicherheit gegen *alle* Bedrohungen, also so etwas wie die Vereinigungsmenge der Sicherheiten gegen jede einzelne mögliche Bedrohung ist nicht ohne weiteres möglich, weil dies die Beschreibung aller möglichen Bedrohungen erfordern würden und sich außerdem manche Sicherungen gegenseitig aussschließen (z. B. wenn gerade die Herstellung der Anfälligkeit gegen bestimmte Bedrohungen die Abwehrmethode gegen andere Bedrohungen ist).

Sicherheit hängt elementar von der Auswahl der Bedrohungen ab, gegen die gesichert werden soll. Die Auswahl hängt von den Sicherheitsinteressen eines Interessenträgers – der „eigenen Partei“ oder des „Verteidigers“ (siehe Abschnitt 2.1) ab. Man kann aber Interessen nicht formal aus dem Nichts herleiten. Entweder man hat sie, oder man hat sie eben nicht.

Formale Modelle eignen sich daher höchstens dazu, Interessen zu beschreiben oder zu transformieren und voneinander abzuleiten bzw. mit einem Kalkül zu bearbeiten. Sie sind jedoch nicht geeignet, Interessen grundlegend zu definieren.

Gerade darin liegt aber die Gefahr bei der Verwendung formaler Modelle. Wegen ihrer oft einfachen Darstellung, ihrer Abstraktion und ihrer (mehr oder weniger) guten Eignung zur Spezifikation oder Verifikation werden sie gerne verwendet oder aus einer Vielzahl bestehender Modelle „das Schönste“ gewählt.

Darüber wird jedoch oft vernachlässigt, daß nicht Modell, Spezifikation und Verifikation, sondern die grundlegende *Definition* der Interessen der wichtige Anfangspunkt der Sicherungsarbeit ist.

Ein Beispiel für diese fehlerhafte Vorgehensweise ist etwa in der Anwendung des Bell-LaPadula-Modells (siehe Abschnitt 1.6.2) zu sehen. Dieses Modell wurde für militärische Anwendungen verwendet und ermöglichte es, ein formales Sicherheitsmodell auf leichte und klare Weise abstrakt zu beschreiben und darauf aufbauend Spezifikationen zu erstellen und Verifikationen durchzuführen.

Erst bei der Anwendung stellte sich dann heraus, daß das erbaute System zwar den Spezifikationen und dem Modell entsprach, aber nicht das war, was man haben wollte [83]. Der fatale Fehler war, daß man die Existenz des formalen Modells als wichtiger einschätzte, als die saubere Erhebung der Interessen, und wohl sogar dem Irrtum unterlag, ersteres könnte letzteres ersetzen.

Viel wichtiger als das formale Modell ist daher die Erhebung der Interessen (als Teil der Bedrohungsanalyse) und deren klare und systematische Darstellung anhand der in Kapitel 2 aufgezeigten Kriterien. Wenn sich das dann in ein formales Modell pressen läßt – schön.

1.6.1.2 Ziel und Weg

Formale Modelle beschreiben nur ein fertiges System. Sie führen zu Aussagen der Art „Benutzer A darf nicht auf Objekt x lesend zugreifen“, aber sie verraten nichts darüber, wie der Benutzer A konkret zu hindern ist oder wie man das System zu entwerfen hat und auf welcher Wirkungsweise die Hinderung beruhen soll.

Formale Modelle beschreiben nur das idealisierte Verhalten eines fertigen Systems, also nur das Entwurfsziel, aber nicht den Weg dorthin.

1.6.1.3 Abstraktion

Formale Modelle sind abstrakt, Angreifer wollen hingegen ganz konkret und real am Angriff gehindert werden. Sicherheitsmaßnahmen müssen daher auf realen Mechanismen beruhen, etwa Hardware, Betriebssystemen, Verschlüsselungen usw. Die traurige Realität ist nämlich, daß sich nur ganz wenige Angreifer – vornehmlich akademischer Natur – von einem Angriff abhalten lassen, indem man ihnen theoretisch nachweist, daß es ein formales Modell gibt, das ihnen den Angriff verbietet. Die meisten Angreifer hören einem dabei einfach nicht zu oder sehen sogar gerade dies als Herausforderung an.

Die Beschreibung von Sicherheitsmechanismen nur über formale Modelle ist daher so weit von der realen Umsetzung entfernt, daß das Modell und dessen Operationen sich nicht mehr zuverlässig und eindeutig auf die reale Implementierung abbilden lassen. Reale Betriebssysteme und Rechner kennen nicht nur abstrakte Objekte, sondern greifen über eine Vielzahl von Methoden auf Dateien, Geräte usw. zu.

Die Folge ist ein Dilemma: Entweder ist das Modell so einfach, daß man mit ihm arbeiten kann, stimmt aber nicht genügend mit der Realität überein, um auch dort wirken zu können, oder es ist so realistisch, daß man nicht mehr effizient mit ihm arbeiten kann (und es obendrein nicht mehr als „formal“ bezeichnet würde).

Auch hier wird wieder auf das Bell-LaPadula-Modell verwiesen, bei dessen Umsetzung sich – trotz aller Verifikation und formalen Korrektheit – herausstellte, daß ein verdeckter Kanal über Dateinamen besteht (siehe Beispiel 4.3 auf Seite 106). Das Modell kennt nämlich nur Objekte, nicht aber das Schichtenmodell oder gar die Unterscheidung zwischen Hilfs- und Nutzlast (siehe Abschnitt 2.5.3).

Das Modell selbst war sicher, aber so weit von der Realität entfernt, daß die reale Umsetzung nicht mehr analog dem Modell entsprach und die Sicherheitsüberlegungen des Modells nicht mehr anwendbar waren.

In aller Regel hat der Interessenträger ein deutlich höheres Interesse an einem sicheren System als an einem sicheren Modell.

Wird dennoch ein formales Modell verwendet, muß zusätzlich die Übereinstimmung der Implementierung mit dem Modell verifiziert werden (wobei es fraglich ist, ob ein

Modell, daß auf Übereinstimmung mit einer realen Maschine verifiziert werden kann, noch als „formal“ angesehen werden kann oder ob überhaupt ein Vorteil darin liegt, das Modell statt der realen Maschine zu betrachten).

1.6.2 Das Bell-LaPadula-Modell

Das Modell von Bell und LaPadula [10, 83, 102] ist das bekannteste formale Sicherheitsmodell. Es wurde für den militärischen Einsatz entwickelt.

In diesem Modell wird jedem Objekt ein Tupel $(class, cat)$ zugeordnet. $class$ ist dabei eine Einstufung des Sicherheitsbedarfs (nicht klassifiziert, Nur für den Dienstgebrauch, Vertraulich, Geheim, Streng Geheim, usw.). cat ist eine thematische Kategorie.

Jedem Subjekt wird ein Tupel $(clear, NTK)$ zugeordnet. $clear$ ist dabei die Vertrauensstufe, die das Subjekt genießt (gleich wie $class$). NTK (= Need to know) ist eine Menge von thematischen Kategorien, auf die das Subjekt zugreifen können muß.

Nun gibt es zwei Regeln:

Die einfache Regel besagt, daß ein Subjekt nur Daten lesen darf, deren $class$ die eigene Stufe $clear$ nicht übersteigt und dessen Kategorie in NTK enthalten ist. *(„Nicht nach oben lesen“)*

Die *-Regel besagt, daß nur Objekte geschrieben werden können, deren Klassifikation mindestens der der Quellobjekte entspricht und deren Kategorie die aller Quellobjekte umfaßt. *(„Nicht nach unten schreiben“)*

1.6.3 Das „Chinese Wall“ Modell

Das „Chinese Wall“-Modell [22] wurde für den Einsatz im kommerziellen Bereich entwickelt. Im Gegensatz zum Bell-LaPadula-Modell (siehe Abschnitt 1.6.2) werden zur Bestimmung der Zugriffsrechte aber nicht der zugreifende Benutzer, sondern ausschließlich die Eigenschaften der Datenobjekte betrachtet.

Datenobjekte werden hierarchisch geordnet. Dazu werden sie in thematisch zusammenhängende Gruppen eingeordnet und diese dann zu „Interessenskonfliktklassen“ zusammengefaßt.

Ein neuer Benutzer des Systems, der in seinem Anfangszustand als „unwissend“ angesehen wird, unterliegt zunächst überhaupt keiner Einschränkung, er kann auf jedes Objekt zugreifen. Jedes Objekt, auf das er einmal zugegriffen hat, wird ihm aber unwiderruflich als Eigenschaft zugeschrieben. Bei allen künftigen Aktionen werden Zugriffe auf Objekte verweigert, die in der gleichen Interessenskonfliktklasse wie eines der dem Benutzer bereits anhaftenden Objekte liegt.

Dieses auf den ersten Blick skurrile Modell würde sich in einer etwas modernisierten Fassung sehr gut für die Rechtebegrenzung von nicht vertrauenswürdigen Anwendungsprogrammen durch das Betriebssystem eignen:

Beispiel 1.15:
Betriebssystem mit chinesischer Mauer
Statt einem Benutzer betrachtet man die Prozeßinkarnation des Anwendungsprogrammes und der mit ihm kommunizierenden Prozesse, als Datenobjekte alle durch Zugriffsrechte zu kontrollierenden Operationen.

Der Anwendungsprozeß – etwa eines der beliebten Office-Pakete mit allen erdenklichen Funktionen – darf zunächst *alles*, schränkt aber durch jede Aktion seine zukünftigen Rechte ein. In eine Interessenskonfliktklassen könnte man folgende Elemente aufnehmen, die sich somit gegenseitig ausschließen:

- Zugriff auf die Datei mit dem Telebanking-Paßwort und der Kontonummer, sowie Internet-Zugriff zum WWW-Server der Bank
- Jeder sonstige Internet-Zugriff und Dateizugriffe auf eine Sonderdateiverzeichnis, in dem „unsichere“ (dirty) Dateien aus dem Netz abgelegt werden können.
- Schreibzugriff auf ausführbare Dateien.
- Zugriff auf alle sonstigen Daten, deren Vertraulichkeit und Integrität gewahrt werden müssen.

Damit wäre (im Rahmen der Möglichkeiten des formalen Modells, siehe Abschnitt 1.6.1) gewährleistet, daß Bankdaten nicht an andere Rechner per Internet verschickt werden oder in andere Dateien einsickern. Auch kann der aus dem Internet heruntergeladene vertrauensunwürdige Schrott nur in bestimmten Verzeichnissen abgelegt werden. Einem Wurm/Virus wird vorgebeugt, weil das Programm dann, wenn es über das Netz angegriffen wurde, selbst nicht mehr auf ausführbare Dateien zugreifen und den Virus weitergeben kann. Auch sonstige sicherheitsbedürftige Daten können nicht beeinträchtigt oder über das Internet offenbart werden.

2 Die System- und Bedrohungsanalyse

2.1 Überblick

Maßnahmen zur Herstellung oder Verbesserung der Kommunikationssicherheit dienen nicht dem Selbstzweck, sondern regelmäßig dem gleichen Hauptzweck, zu dem die Kommunikation überhaupt unternommen wird[1]. Kommunikation und Absicherung leisten dabei unterschiedliches und sind in ihrer Funktion nicht deckungsgleich; in der Kombination sollen sie *zusammen* eine gestellte Aufgabe erfüllen.

Diese zu erfüllende Aufgabe und die spezifizierten und durch die technische Realisierung implizierten Eigenschaften der Kommunikation müssen daher Hauptgegenstand der Betrachtung sein. Sicherungsmaßnahmen sollen die Funktion des Systems *innerhalb* seiner Spezifikation möglichst wenig verändern oder beeinträchtigen (also möglichst *transparent* sein), während sie *außerhalb* der Spezifikation größtmögliche Wirkung entfalten sollen (also *effektiv* sein). Kurz gesagt: Der befugte Benutzer soll möglichst wenig von den Maßnahmen merken, der Angreifer jedoch trotzdem möglichst wirksam abgewehrt werden.

Entwurf und Beurteilung von Sicherungsmaßnahmen müssen damit zwangsläufig auch alle Besonderheiten und Eigenarten des Systems berücksichtigen. Es genügt dabei nicht, nur die (ohne Beachtung der Sicherheit vorgenommene) Spezifikation beim Entwurf des Systems zu betrachten, weil diese das tatsächliche System nicht ausreichend beschreibt. Entwurf, Implementierung und Realisierung sind eigenständige Arbeitsschritte und beinhalten eine Vielzahl von Entscheidungen, Wahlmöglichkeiten und Randbedingungen, die über die eigentliche Spezifikation hinausgehen. Auch Laufzeitbedingungen und Benutzereingaben können Einfluß auf das tatsächlich wirkende System haben.

Dem steht übrigens nicht entgegen, daß die eigentliche „Baustelle“ der Kommunikationssicherheit nicht das System, sondern dessen Spezifikation ist, denn die Betrachtung

[1] Die Untersuchung dessen fällt leicht, wenn man den Zweck der Kommunikation entfallen läßt und den verbleibenden Sinn der Sicherungsmaßnahmen untersucht.

eines Systems, die Ableitung von Anforderungen daraus und das „hochziehen“ dieser Anforderungen in die Spezifikation gehören zum Vorgang der Absicherung.

Erster Schritt bei Entwurf und Beurteilung von Sicherungsmaßnahmen muß daher eine Erhebung bzw. Beschreibung der vorliegenden Interessen und der zu sichernden Kommunikation, sowie der beteiligten Systeme und Interessenträger sein.

An einem Kommunikationsvorgang sind mindestens beteiligt (vgl. Abbildung 2.1):

- Zwei „befugte“ Parteien (siehe Definition 2.1), nämlich mindestens ein Sender und ein Empfänger, die sich räumlich oder zeitlich voneinander unterscheiden, und die dem Kommunikationszweck entsprechend an der Kommunikation teilnehmen sollen.

  Es wird angenommen, daß die an Sicherheit interessierte Partei stets an der zu sichernden Kommunikation beteiligt und damit eine der Parteien ist, anderenfalls sie die Einhaltung der spezifizierten Maßnahmen nicht durchsetzen bzw. überwachen kann[2]. Sie wird als die *„eigene“ Partei* oder als *Verteidiger* bezeichnet.

- Ein Übertragungsmedium (siehe Abschnitt 2.3)

- Das Schutzobjekt, nämlich die Information bzw. die Daten, die über das Medium zwischen den befugten Parteien übertragen werden sollen.

- Ein Angreifer.

  Zwar bedarf die Kommunikation zur Funktion keines Angreifers, und oft ist ein Angreifer nicht auszumachen oder tatsächlich nicht vorhanden. Zweck der Kommunikationsicherung ist aber die Abwehr von Angriffen, und der Angriff bedarf des Angreifers. Daher wird hier bei der Betrachtung von Kommunikationsvorgängen der – reale oder hypothetische – Angreifer stets als fester Bestandteil mitbetrachtet.

Ein Kommunikationsvorgang ohne Sender, Empfänger, Nachricht und Medium ist nicht sinnvoll. Kann es weder einen realen noch einen hypothetischen Angreifer geben, braucht man keine Sicherung.

Diese Bestandteile werden in den nachfolgenden Unterkapiteln näher untersucht.

Komplexere Übertragungsvorgänge, an denen z. B. verschiedene Medien oder mehr als zwei Parteien beteiligt sind, müssen gegebenenfalls in mehrere einzelne Übertragungsvorgänge unterteilt werden.

[2] Sofern der Interessenträger nicht selbst beteiligt ist, wie dies etwa bei der staatlichen Kommunikationsüberwachung der Fall ist, ergeben sich grundsätzlich andere Problemstellungen, die in Kapitel 5 untersucht werden.

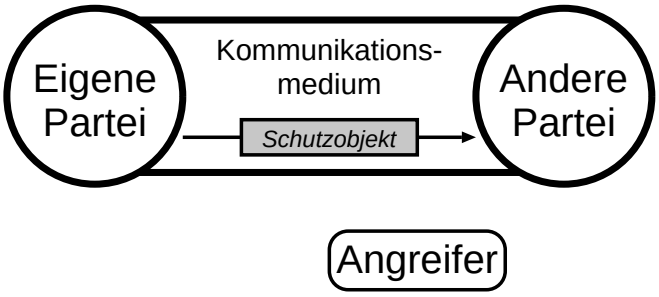


Abbildung 2.1: Schematisches „Organigramm“ eines Kommunikationsvorganges. Wir betrachten stets die befugten Parteien, das Medium, das Schutzobjekt (die übertragenen Daten) und einen an einer vermuteten Position (siehe 2.6) stehenden realen oder vermuteten Angreifer. Komplexere Strukturen müssen gegebenenfalls zerlegt werden.

2.2 Die befugten Parteien

2.2.1 Der Begriff der Partei

Die Motivation der Kommunikationssicherheit rührt aus dem Interesse, sich gegen einen Angreifer zu erwehren, während man mit sich selbst (zeitlich) oder mit einem anderen (räumlich) kommuniziert. Gegenstand der Betrachtung können daher nicht nur Datenobjekte, Geräte etc. sein, weil diesen kein Schutzinteresse innewohnt und diesen auch keine Befugnis im eigentlichen Sinne zugedacht werden kann. Ebenso bedarf der Angreifer eines Angriffsinteresses, um seinen Angriff gezielt zu verfolgen und nicht nur zufällig Schaden anzurichten (in Abgrenzung zur „Safety“, vgl. Abschnitt 1.2).

Interessen alleine genügen jedoch auch nicht, um den Verteidiger oder den Angreifer zu charakterisieren. Die reine Existenz eines Angreifers mit zuwiderlaufenden Interessen begründet noch keinen Schutzbedarf. Erst die Verbindung mit der Handlungsfähigkeit des Angreifers und den Angriffspunkten des Verteidigers, sowie dessen Handlungsfähigkeit zur Verteidigung führt zu einem funktionalen Modell.

Definition 2.1:
„Partei“
Eine Partei ist eine Verbindung aus einem abstrakten Interessenträger, der bezüglich seiner Interessenlage nicht in einander zuwiderlaufende Teilinteressen unterteilt werden kann oder soll, und (zeitlichen oder räumlichen) Übertragungseinrichtungen, die bezüglich ihrer zeitlichen und räumlichen Ausdehnung bei der Übertragung nicht unterteilt werden können oder sollen.

Bemerkung 2.2:
Die drei Grundparteien
Regelmäßig treten mindestens folgende drei Parteien auf:

Die „eigene“ Partei,
auch als „Verteidiger“ bezeichnet.

Die „andere“ Partei,
mit der die dem Verteidigerinteresse entsprechende Kommunikation durchgeführt werden soll.[3]

Die „angreifende“ Partei,
die hier nur als „Angreifer“ bezeichnet wird.

2.2.2 Eigenschaften der Parteien

Die Aufgabe der Kommunikationssicherheit ist es sicherzustellen, daß nur befugte Parteien Zugriff haben, also die abstrakte Befugnis mit technischen Mitteln durchzusetzen. Das führt zwangsläufig dazu, daß eine Abgrenzung und damit eine Unterscheidung zwischen befugten und unbefugten Parteien vorgenommen werden muß.

2.2.2.1 Identität und Adressen

Hinter einer Sicherungsmaßnahme steckt stets ein Schutzinteresse und damit ein Interessenträger. Er hat gewisse Vorstellungen über die Parteien, mit denen er kommunizieren will oder vor denen er sich zu schützen beabsichtigt. Damit ist eine subjektive Erwartungshaltung über den Kommunikationspartner im Normalfall der Kommunikation verbunden, die im Angriffsfall verletzt werden kann.

Die Identität einer Partei spiegelt die Vorstellung des Interessenträgers wieder. Sind bezüglich seiner Interessenlage zwei Parteien unterscheidbar, so sind sie nicht identisch.

Als Ausprägung der Identität kommt in der Regel alles in Frage, was man aus dem normalen Leben unter diesem Begriff kennt wie Menschen, Firmen, Behörden, Vereine, Gerichte, Notare etc. Wegen der technischen Natur der Datenübertragung kommen aber auch Identitäten in Betracht, die nicht unmittelbar mit dem Zweck, sondern der technischen Realisierung der Datenübertragung in Zusammenhang stehen, wie Router, Mail-Relays, Nameserver usw.

Der Interessenträger hat auch eine Vorstellung davon, was diejenigen Parteien, mit denen er kommunizieren will, im Gegensatz zu anderen Parteien dürfen und können sollen, wozu sie also *befugt* sind.

[3] Der Begriff legt die räumliche Kommunikation zwischen verschiedenen Parteien nahe. Im Fall der zeitlichen Kommunikation können beide Parteien zunächst zusammenfallen, im Rahmen der System- und Bedrohungsanalyse jedoch durch zeitliche Trennung wieder zerfallen.

Definition 2.3:
„Partition“
Eine vollständige Unterteilung der (jeweils in Betracht kommenden) Parteien in

- mindestens zwei,
- endlich viele,
- nichtleere und
- paarweise disjunkte

Teilmengen heißt *Partition der Parteien*.

Identität und Befugnis von Parteien liegen in der Vorstellung des Interessenträgers und sind deshalb technisch und formal nicht greifbar. Sie können daher nicht zur Absicherung herangezogen werden; stattdessen muß die Absicherung die Befugnisse technisch durchsetzen und folglich die Identitäten – soweit dazu notwendig – nachbilden bzw. auf technisch (oder formal) greifbare und unterscheidbare Eigenschaften abbilden .

Sowohl für das Funktionieren der Datenübertragung, als auch für die Beschreibung und Festlegung der Befugnisse ist es notwendig, die Parteien zu bezeichnen, d. h. ihnen technisch greifbare Merkmale zuzuordnen, auf die die Vorstellung des Interessenträgers abgebildet werden kann.

Definition 2.4:
„Adresse“
Die den Parteien zugeordneten technisch unterscheidbaren Merkmale, auf die die Vorstellungen des Interessenträgers über die Identität abgebildet werden, werden als *Adressen* bezeichnet.

Definition 2.5:
„passend“
Eine Zuordnung von Adressen heißt *passend* zu einer Partition, wenn es eine Abbildung der Adressen auf die Teilmengen der Partition gibt, die jede Adresse des Adreßraumes eindeutig auf genau eine Teilmenge abbildet und die die Adresse(n) jeder Partei auf die Teilmenge abbildet, zu der die Partei unter dieser Partition gehört.

2.2.2.2 Befugnis und Befähigung

Eine wirksame Absicherung muß Befugnisse – das *Dürfen* – möglichst getreu in Fähigkeiten – das *Können* – umsetzen. Befugnisse müssen über ihre Verbotsbedeutung hinaus durchgesetzt und deshalb mit technischen Mitteln so umgesetzt werden, daß die befugte Partei eine Befähigung hat, die der unbefugten Partei fehlt. Interessenträger als Teil von Parteien sind selbst aber abstrakte – und damit nichttechnische – Gebilde

in der Vorstellung des Verteidigers. Sie können daher unmittelbar keine technischen Fähigkeiten haben und werden deshalb nur zusammen mit Kommunikationseinrichtungen betrachtet.

Eine zunächst naheliegende Eigenschaft von Parteien, die zur Unterscheidung verwendet werden kann, ist ihr räumlicher (und ggf. zeitlicher) *Ort* bzw. ihre Ausdehnung. Soll eine Information einer Partei zur Kenntnis gelangen, so muß sie an den Ort dieser Partei transportiert werden. Soll sie geheim bleiben, so darf sie nicht an den Ort der Partei gelangen.

Bei weiterer Überlegung fällt aber auf, daß der geographische bzw. geometrische Ort einer Partei nicht immer die ausschlaggebende Eigenschaft ist. Wenn eine Information am Ort einer Partei angekommen ist, so bedeutet das, daß die Partei auf die Information durch eine atomare Operation, die im Rahmen der Betrachtung nicht weiter in räumliche und zeitliche Datenübertragungen unterteilt werden kann oder soll, zugreifen kann. Gerade das hängt aber stark von der Betrachtungsweise ab. Während man in einem Fall die ganze Wohnung einer Person als Ort einer Partei ansehen könnte, kann im anderen Fall schon die Übertragung vom Prozessor zum RAM innerhalb des Mikrochips in einer Chipkarte im Geldbeutel derselben Person als räumliche Datenübertragung angesehen werden. Während die Wohnung als Immobilie durch absolute[4] Raumkoordinaten charakterisiert werden kann, liegt der Zweck der Chipkarte gerade in deren Mobilität, weshalb hier deren aktueller Ort eine geringere Bedeutung hat als deren *Ausdehnung*.

Es ist daher sinnvoll, die Betrachtung der atomaren Fähigkeiten einer Partei vom physikalischen oder geographischen Ort zu abstrahieren.

Definition 2.6:
„Position“
Die Gesamtheit der relevanten atomaren Zugriffsfähigkeiten einer Partei wird als deren *Position* bezeichnet.

Unterscheiden sich Parteien in relevanten Fähigkeiten, so haben sie unterschiedliche Positionen. Übernimmt ein Angreifer die Position einer Partei, ist er mit technischen Mitteln nicht mehr von ihr zu unterscheiden.

Beispiel 2.7:
Parteienunterscheidung durch Paßwort
Der Zugriff auf ein Paßwort und das anschließende Nennen desselben können als atomare Operation betrachtet werden.[5] Kennt ein Angreifer das Paßwort, ist er technisch nicht mehr von der befugten Partei zu unterscheiden. Er hat aus Sicht der paßwortprüfenden Partei damit die Position der befugten Partei eingenommen.

[4] Unter Vernachlässigung der Planetenbewegung

[5] Im Gegensatz etwa zum Nennen jedes einzelnen Zeichens oder Bits, die hier nicht betrachtet werden sollen.

Offensichtlich ist das, was unter der Position einer Partei zu verstehen ist, davon abhängig, was man im Einzelfall als relevant und atomar ansieht.

2.2.3 Parteispezifische Rahmenbedingungen

2.2.3.1 Portabilität und Flexibilität

Bei der Beurteilung und dem Entwurf von Sicherheitsmaßnahmen sind alle am Übertragungsvorgang beteiligten Einrichtungen zu betrachten. Hierzu gehört insbesondere der Aufbau im Schichtenmodell (siehe Abschnitt 2.3.3). Oft sind aber zum Zeitpunkt der Analyse nicht alle Belegungen im Schichtenmodell bekannt. Die Ursache kann darin liegen, daß dies im Entwurf und in der Implementierung des zu sichernden Kommunikationssystems nicht festgelegt ist, möglicherweise liegt es aber auch im Parteiinteresse, bestimmte Schichten aus Gründen der Portabilität freizuhalten. Daher ist zu unterscheiden zwischen

- Belegungen, die bereits durch das zu sichernde System festgelegt sind,
- Belegungen, die nicht festgelegt werden dürfen, weil eine Festlegung der Spezifikation des Systems zuwiderlaufen würde und
- Belegungen, die nicht durch das System festgelegt sind, aber im Rahmen des Entwurfs der Sicherungsmaßnahmen festgelegt werden können.

Die parteispezifischen Anforderungen bezüglich der Portabilität bzw. Freihaltung bestimmter Schichten ist zu berücksichtigen.

Beispiel 2.8:
Parteiflexibilität im Schichtenmodell
In einem LAN soll die Kommunikation abgesichert werden. Es besteht die Vorgabe, daß auf den Schichten 3 und 4 TCP/IP zu verwenden ist, und darunter Ethernet. Die oberen Schichten müssen beliebig nutzbar bleiben.

Damit sind die Schichten 2 bis 4 durch das System festgelegt. Die höheren Schichten sind freizuhalten. Schicht 1 ist noch nicht festgelegt.

Es wäre zu untersuchen, ob im Rahmen der Absicherung die Schicht 1 festgelegt werden kann, oder ob diese variabel gehalten werden muß. Kann etwa eine 10BaseT-Verkabelung (TwistedPair) festgelegt werden, kann die Absicherung auch auf die Verwendung von Switches etc. gestützt werden. Besteht jedoch die Anforderung, daß auch eine 10Base2-Verkabelung (Thinwire) verwendbar bleiben muß, können Switches nicht mehr ohne weiteres Verwendung finden.

Es ist hierbei außerdem zu unterscheiden zwischen der Festlegung *der Schnittstellen zwischen den Schichten* (z. B. Socket-Schnittstelle, Paket-Routing im Unix-Kern,

`/usr/lib/sendmail`) und der *Implementierung der Schicht selbst*, z. B. wenn die Verwendung eines bestimmten TCP/IP-Stacks oder eines bestimmten MTA[6] vorgegeben ist.

2.2.3.2 Ressourcen und Kosten

Abwehrmaßnahmen können aufwendig und teuer sein. Daher müssen nicht nur Aufwand und Kosten des Angreifers betrachtet werden, sondern auch die, die dem entstehen, der die Abwehrmaßnahmen betreibt.

Hier sind insbesondere zwei Werte zu untersuchen:

Die absolute Leistungsfähigkeit beschreibt, was der Verteidiger zu leisten imstande ist. Dabei können im Einzelfall starke Einschränkungen vorliegen, wenn etwa der Batteriestrom, die Chipfläche, der Speicherplatz oder die zur Verfügung stehende Rechenzeit begrenzt sind.

Die relative Leistungsfähigkeit beschreibt, was der Verteidiger an Aufwand zu leisten bereit ist und bis zu welchem Aufwand die Sicherung einen Vorteil erwarten läßt. Ein Vorteil ist nicht mehr gegeben, wenn der Schaden durch die Kosten der Sicherung höher ist als der Schaden, den der Angreifer anrichten kann.

Bereits die Notwendigkeit für den Verteidiger, Aufwand zur Sicherung zu betreiben, kann als Erfolg eines Angriffes betrachtet werden.

Beispiel 2.9:
Sicherungsaufwand

Im Gegensatz zu Geldnoten besteht bei Briefmarken[7] eine erheblich geringere Gefahr der Fälschung. Die Herstellung einer Geldnote mit Sicherheitsmerkmalen neuerer Art kostet etwa zwischen 20 und 50 Pfennig. Diese Kosten wären für Briefmarken nicht akzeptabel (relative Leistungsfähigkeit überschritten).

Im Bereich Pay-TV werden u. a. Verschlüsselungsverfahren eingesetzt, bei denen der gesamte Spielfilm mit einem Hauptschlüssel geschützt wird. Der Hauptschlüssel muß ausreichend lang sein, um einen Angriff gegen den ganzen Film zu verhindern, weil mit einer Veröffentlichung des Schlüssels starke Einnahmeverluste verbunden wären. Die Entschlüsselung des ganzen Films in Echtzeit würde bei Verwendung des Hauptschlüssels aber Hardware voraussetzen, die die Geräte zu teuer machen

[6] Mail Transfer Agent
[7] Von Sammlerstücken abgesehen

würden (absolute Leistungsfähigkeit überschritten). Deshalb wird der Hauptschlüssel zur Erzeugung einer Pseudozufallsfolge verwendet, aus der dann kurze Schlüssel für eine schwache Verschlüsselung kurzer Bildsequenzen entnommen werden. Damit kann der Decoder billig gebaut werden, während ein Angreifer zwar leicht einige wenige Sequenzen brechen kann, damit aber keinen nennenswerten Vorteil erreicht oder Schaden anrichtet.

2.2.4 Akausale Kommunikation

Sicherungsmethoden sind keine Problemlösungen, sondern nur Problemverlagerungen. Insbesondere die wichtigen kryptographischen Methoden beruhen oft auf einer Verlagerung auf einen sicheren Kanal. Das erscheint zunächst paradox, denn wenn man schon einen sicheren Kanal hat, braucht man keine Sicherung mehr. Dennoch ist ein solcher Kanal hilfreich, denn die Verlagerung kann z. B. über den Zwischenschritt eines gemeinsamen Geheimnisses erfolgen und damit kausal von der zu sichernden Kommunikation entkoppelt werden, d. h. die Nutzung des sicheren Kanals kann auf einen Zeitpunkt vorverlegt werden, zu dem der Sender selbst die zu sendenden Daten noch nicht kennt. So könnte ein gemeinsamer symmetrischer Schlüssel vereinbart werden.

Daher ist zu untersuchen, ob die Parteien akausal kommunizieren können (vgl. Abschnitt 5.6.3.2 und 5.6.3.3).

2.2.5 Die unabhängige dritte Partei

In bestimmten Fällen ist es notwendig, eine vertrauenswürdige und objektive dritte Partei als Notar heranzuziehen. Das ist ggf. zu berücksichtigen und zu erheben, ob solche Parteien zur Verfügung stehen. Ebenso ist zu untersuchen, ob gegenüber einem unabhängigen Dritten (Richter usw.) Beweise erbracht werden müssen.

2.3 Die Eigenschaften des Übertragungsmediums

2.3.1 Übertragung in Raum oder Zeit

Es wird hier zwischen zwei Formen der Datenübertragung unterschieden, nämlich der Übertragung in der Zeit (Datenspeicherung) und im Raum (Telekommunikation).

Beide Formen sind sich ähnlich und lassen sich in vielerlei Hinsicht in analoger Weise behandeln. Dennoch besteht zwischen der Datenübertragung im Raum und in der Zeit

keine vollständige Symmetrie, sie sind deshalb auch bei der Absicherung unterschiedlich zu behandeln.

Eine eindeutige Zuordnung zu einer der beiden Formen erscheint nicht immer einfach. Speichert man Daten auf einer Diskette und trägt diese an einen anderen Ort, so hat man die Daten sowohl zeitlich, als auch räumlich transportiert. Im Zweifelsfall ist der Übertragungsvorgang daher in mehrere Vorgänge zu zerlegen und als Konkatenation zeitlicher und räumlicher Übertragungsvorgänge darzustellen. Sofern aber eine Form deutlich höhere Bedeutung hat und die andere Form keinen eigenen Zweck erfüllt, sondern nur notwendigerweise mit auftritt und bezüglich der anderen (folgenden) Kriterien keine eigenen Anforderungen nach sich zieht, dann kann diese der anderen untergeordnet und damit vernachlässigt werden.

Beispiel 2.10:
Zeitliche und räumliche Übertragung
Daten werden auf Diskette gespeichert und zum Schrank getragen, wo sie gelagert werden. Die zeitliche Übertragung überwiegt, der räumliche Transport zum Schrank kann normalerweise vernachlässigt werden, es sei denn, der Schrank wird verschlossen.

Werden Daten jedoch auf Diskette gespeichert und zu einem anderen Rechner getragen, so überwiegt die räumliche Übertragung, während der zeitliche Aspekt vernachlässigt werden kann, es sei denn, der zweite Rechner dient als Backup-System.

2.3.1.1 Zahl der befugten Parteien

Nach dem Kommunikationsmodell (vgl. Abb. 2.1) gibt es bei jedem Kommunikationsvorgang mindestens einen befugten Sender und mindestens einen befugten Empfänger. Hier werden jedoch nur Kommunikationsvorgänge mit genau einem Sender und genau einem Empfänger betrachtet. Gibt es mehr Sender oder Empfänger, so zerfällt der Vorgang in mehrere Einzelvorgänge.

Eine Partei hat Interessen und kann an Datenübertragungen teilnehmen (wegen Def. 2.1). Es gibt innerhalb der Partei keine Interessenskollision; eine Übertragung innerhalb einer Partei, d. h. innerhalb ihrer räumlichen und/oder zeitlichen Grenzen, wird nicht als Bedrohung und in den nachfolgenden Betrachtungen nicht als Übertragung im Sinne der Kommunikationssicherheit betrachtet. Parteien sind *atomar*.

In der Regel ist eine Datenübertragung im Raum eine Übertragung zwischen *verschiedenen* Kommunikationsparteien, während eine Übertragung in der Zeit normalerweise als Datenspeicherung von ein und derselben Partei betrieben wird.

Nachfolgend werden daher

- Datenübertragungen *im Raum* mit Übertragungen zwischen *mehreren Parteien* und

- Datenübertragungen *in der Zeit* mit der Übertragung *einer Partei* an sich selbst

gleichgesetzt, sofern nicht anderes erwähnt wird.

Bei der Datenübertragung im Raum – also zwischen mehreren Parteien – ist außerdem ein gewisses Maß an Verständigung über Protokolle, Schlüssel usw. zwischen den Kommunikationsparteien notwendig. Bei einer Datenspeicherung kann davon ausgegangen werden, daß die speichernde Partei beim Senden und Empfangen den gleichen Kenntnisstand über Protokolle usw. besitzt und daher keine Verständigung bzw. Einigung erfolgen muß[8]. Die räumliche Übertragung ist somit wesentlich stärker an *Konventionen* gebunden, die zeitliche Übertragung erlaubt eine gewisse Willkür und folglich wesentlich stärkere Eingriffe in die Kommunikationsprotokolle.

2.3.1.2 Sender- und Empfängerausdehnung

Raum- und Zeitübertragung unterscheiden sich auch in der erwarteten (räumlichen oder zeitlichen) Position von Sender und Empfänger.

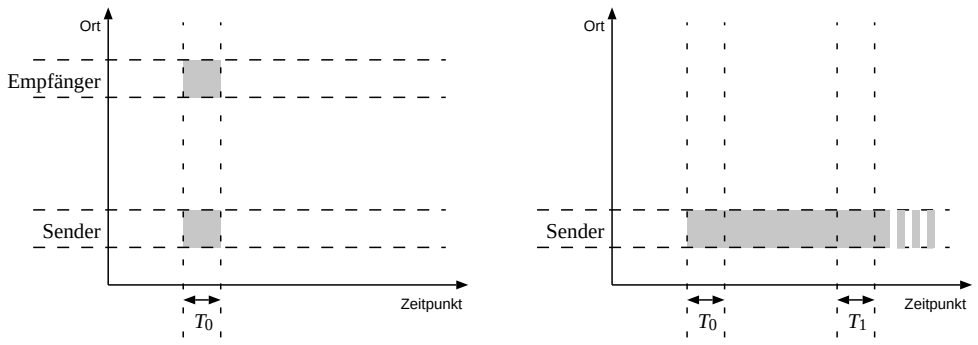
An der Übertragung im Raum sind mehrere Parteien beteiligt, es ist daher von Bedeutung *welche* Parteien beteiligt sind, d. h. welche Identität Sender und Empfänger haben. Die an räumlicher Übertragung beteiligten Parteien haben ein Interesse, daß die Übertragung nur mit befugten Parteien möglich ist; die Befugnis zur Übertragung – Senden und Empfangen – soll auf die befugten Parteien und auf deren räumliche Ausdehnung beschränkt bleiben, da andernfalls auch unbefugte Parteien übertragen könnten.

Eine räumliche Übertragung steht daher normalerweise mit einer mehr oder weniger konkreten Beschreibungen des Absenders und des Empfängers in Verbindung, sie verwendet *räumliche Adressen*.

Im Gegensatz dazu sind Sende- und Empfangszeitpunkt bei der zeitlichen Übertragung im Normalfall nicht festgelegt. Die Sende- und Empfangszeit liegt meistens im Belieben der Partei, es gibt keinen unerlaubten Sende- oder Empfangszeitpunkt (siehe Abb. 2.2). Die zeitliche Übertragung kennt normalerweise keine spezifische *Empfangsadresse*, weil keine Unterteilung in mehr als eine Teilmenge besteht und damit keine Partition vorliegt (vgl. Def. 2.3).

Im Einzelfall kann es jedoch auch nötig sein, bei der zeitlichen Datenübertragung die mögliche Position von Sender und Empfänger einzugrenzen, beispielsweise wenn die

[8] Bedauerlicherweise gilt diese Annahme nur unter vernünftigen Bedingungen, die in der Realität selten vorliegen. Oftmals werden Softwareprodukte von mangelhafter Qualität eingesetzt, bei denen alte Versionen nach gewisser Zeit aus diversen Lizenz- oder Kompatibilitätsgründen nicht mehr einsetzbar sind und neuere Versionen die älteren Protokolle nicht mehr verstehen können. Bei genauer Betrachtung liegt das Problem jedoch darin, daß die sendende Partei undokumentierte Protokolle verwendet und diese deshalb schon zur Sendezeit nicht kennt – und damit also letztlich doch zu beiden Zeitpunkten über den gleichen Kenntnisstand verfügt.



(a) Übertragung im Raum (b) Übertragung in der Zeit

Abbildung 2.2: Datenübertragungen im Raum und in der Zeit sind typischerweise nicht symmetrisch (zur Diagonalen) bezüglich der erwünschten möglichen Position von befugtem Sender und befugtem Empfänger.

Beweisbarkeit gegenüber Dritten (s.u.) verlangt wird oder die zeitübertragende Partei *selbst* als zukünftiger Angreifer angesehen werden muß (z. B. Gefahr der zukünftigen Übernahme durch Erpresser o. ä.). Dies wird in Abschnitt 5.6.4 weiter untersucht.

2.3.1.3 Wiederholbarkeit im Störungsfall

Raum- und Zeitübertragung unterscheiden sich auch in der *Wiederholbarkeit* der Datenübertragung im Fehlerfall. Als Wiederholung ist dabei jede Form der Anhebung des Signal-Rauschabstandes zu verstehen, die die Datenübertragung trotz Störungen und Fehlern (als Rauschen betrachtet), gewährleisten soll.

Die Übertragung im Raum kann sowohl *räumlich*, als auch *zeitlich* wiederholt werden, weil der Sender die Daten mehrfach (mehrere Leitungen, fehlerkorrigierende Codes) parallel, aber auch erneut absenden kann. Eine Datenübertragung in der Zeit kann bei einer Störung nicht zeitlich wiederholt werden, weil die Daten eben aufgrund der Störung nicht mehr verfügbar sind.[9] Sie muß daher *räumlich* durch Mehrfachsendung (Sicherungskopie, Redundanz) wiederholt werden.

Weil die Erkenntnis einer fehlerhaften Übertragung zeitbehaftet ist, findet eine Wiederholung, die nur im Fehlerfall stattfinden soll, als zeitliche Wiederholung statt.

Daher muß eine zeitliche Übertragung zur Sicherung gegen Störungen *prophylaktisch* bzw. *akausal* wiederholt werden, die räumliche Datenübertragung hingegen kann mit einer Wiederholung im Fehlerfall , also einer *kausalen* Wiederholung auskommen.

[9] Könnte der Sender sie erneut – insbesondere an sich selbst – absenden, nachdem er den Fehler festgestellt hat, bräuchte er die Übertragung nicht.

Die Absicherung gegen den Fehlerfall ist prinzipiell zwar nicht die Aufgabe der Systemsicherheit (nicht „Security“, sondern „Safety“), muß aber bei der Wahl der Sicherungsmethoden berücksichtigt werden und wirkt sich u. a. darauf aus, ob etwa eine Schlüsselhinterlegung vorgenommen werden soll, ob Verschlüsselungsverfahren zu wählen sind, die mit Fehlerkorrekturverfahren kombinierbar sind (und Dechiffrierung und Decodierung evtl. kommutieren sollen) oder ob man auch Sicherungsmethoden wählen kann, die mit akausaler Fehlerkorrektur unverträglich sind.

Speziell bei kausaler Fehlerkorrektur ist zu klären, ob die gestörten Daten und die Wiederholung als ein oder mehrere Schutzobjekte (siehe 2.5) anzusehen sind.[10]

Fehlerkorrektur bedeutet Redundanz; Redundanz bedeutet Angriffsfläche für einen Angriff gegen die Vertraulichkeit – frei Haus für den Angreifer bei akausaler Korrektur, als Glücksfall bei kausaler Korrektur oder provoziert durch absichtliche Störungen. Deshalb sind die Korrekturverfahren (und auch andere Redundanzquellen) bei der Auswahl der Sicherungsverfahren miteinzubeziehen.

2.3.2 Kommunikationswege

Die Beurteilung der Kommunikation und die Auswahl der Methoden hängen auch von der räumlichen (und u. U. zeitlichen) Ausdehnung der Kommunikation ab. Sie spielt eine Rolle insbesondere bei der Annahme über die Position des Angreifers (siehe 2.4.1.1), der juristischen Beurteilung (siehe 4.4) und der Überlegung, inwieweit auf die verschiedenen Medien entlang der Strecke eingewirkt werden kann um etwa organisatorische Maßnahmen (siehe 3.6) einzusetzen.

Der reguläre Weg, der zur Datenübertragung verwendet wird, und der oft auf einer oder mehreren Wegewahlentscheidungen beruht, wird als *Route* bezeichnet.

Es muß deshalb untersucht werden

- welche Routen und Routenabschnitte gewählt werden müssen oder können um den Zweck der Übertragung zu erfüllen,
- in welcher Weise aus Sicherungsgründen auf die Routenwahl eingewirkt werden kann,
- welche Routen als mögliche Transportwege in Frage kommen und welche spezifischen Gefährdungen von ihnen ausgehen, insbesondere welche Position der angenommene Angreifer bezüglich der einzelnen Routenabschnitte einnimmt und
- inwieweit die Streckenwahl selbst der Absicherung bedarf.

[10] Beides kann eine Schwächung darstellen. Fehlerkorrektur unter einer Verschlüsselung einerseits bietet genügend Redundanz um die Unizitätslänge stark zu verkürzen. Die Verschlüsselung von Wiederholungen mit verschiedenen Schlüsseln andererseits war einer der Bedienungsfehler der *Enigma*, der eine erheblichen Schwächung des Verfahrens darstellte [64, 78, 73, 6].

2.3.3 Aufbau im Schichtenmodell

Zur Auswahl und Beurteilung der Sicherungsmethoden ist eine möglichst genaue Kenntnis der zu sichernden Kommunikationsverbindung notwendig. So, wie sich die Konstruktion der Übertragungsmechanismen am Schichtenmodell orientiert, sollte auch die Auswahl der Sicherungsmethoden anhand dieses Modells erfolgen.

Daher ist zu klären

- auf welchen Schichten die zu sichernde Kommunikation festgelegt ist,
- welche Protokolle auf diesen Schichten verwendet werden und
- in welcher Weise zum Zweck der Sicherheit in diese und andere Schichten eingegriffen werden kann und darf.

Dabei ist es jedoch wesentlich wichtiger, ein *geeignetes* Schichtenmodell zu verwenden, als ein *bestimmtes*, denn die Schichtung bestimmt sich nach Spezifikation, Entwurf und Aufbau des zu sichernden Systems.

Bemerkung 2.11:
Zur Wahl des Schichtenmodells
Erfahrungsgemäß sind die Verwendung eines Schichtenmodells und die Wahl des ISO-OSI-Modells bzw. eines daran angelehnten Modells immer wieder zu teils heftigen Diskussionen und Meinungsunterschieden. Verschiedene Ansichten werden mit großem Eifer vertreten. Nicht ganz unproblematisch ist die Einbettung von TCP/IP und typischer Internetdienste in dieses Modell. Zudem hängt die Einordnung stark vom Standpunkt des Betrachters ab[11].

Es wird hier das eine oder andere spezielle Schichtenmodell favorisiert. *Wichtig ist die Wahl eines geeigneten Modells und die Anwendung des Prinzips.*

Ein dem ISO-OSI-Modell entsprechendes oder an dieses angelehnte 7-Schichten-Modell und eine Einordnung auch der typischen Internet-Dienste in die Schichten 5-7 hat sich in der Praxis jedoch als praktikabel gezeigt.

Ist ein geeignetes Modell gefunden, ist vor seiner Verwendung das Modell selbst nach den Eigenschaften der verschiedenen Schichten zu analysieren, was in Abschnitt 4.1 eingehend erläutert wird.

[11] Beispiel: TCP/IP über ISDN. Der Anwender setzt IP auf Schicht 3 und die Telefonverbindung zwangsläufig darunter. Der Serviceprovider hingegen setzt sein Telefonnetz auf die Schichten 1 bis (mindestes) 4, und alles, was der Kunde damit treibt, darüber.

Beispiel 2.12:
Sicherungsfähigkeit der Schichten
Sollen allgemeine Internet-Verbindungen abgesichert werden, bedeutet das, daß die Schichten 3 und 4 auf IP, TCP und ggf. UDP festgelegt sind. Die Schichten 1 und 2 sind aus Gründen der Reichweite und weil sie überwiegend in fremdem Einflußbereich liegen, der Sicherung nicht zugänglich. Über die höheren Schichten sind keine allgemeingültigen Annahmen möglich. Die Sicherung muß daher auf den Schichten 3 und 4 angreifen, dabei aber die Spezifikation TCP/IP einhalten.

Eine andere Lage ergibt sich, wenn E-Mail sicher transportiert werden soll, es aber keine Rolle spielt, wie der Transport geschieht. Hier können die Schichten 1 bis 5 beliebig zur Sicherung herangezogen und umgestaltet werden; die Nachrichten könnten etwa durch einen vertrauenswürdigen Boten mit verschlossenem Koffer im Diplomatengepäck transportiert werden (Sicherung auf Schicht 1).

2.3.4 Grad der Interaktion

Es gibt drei Arten der Parteienbeteiligung an einer Kommunikation, nämlich die rein passive Rolle eines Empfängers, eine rein aktive Rolle als Sender und Mischformen. Kommunizieren zwei Parteien in einer Weise, die mindestens zwei Übertragungen in unterschiedlichen Richtungen so erlaubt, daß der Inhalt der zweiten Sendung vom Inhalt der ersten Sendung abhängig gemacht und vom ersten Sender als Reaktion wahrgenommen werden kann, ist die Verbindung *interaktiv* (vgl. aber Definition 5.35).

Interaktive Verbindungen erlauben insbesondere beim Einsatz kryptographischer Methoden einen weitaus höheren Grad der Sicherheit (vgl. Abschnitt 5.6.3.2). Daher sollte berücksichtigt werden, ob die Kommunikationsverbindung bereits interaktiv ist oder mit vertretbarem Aufwand interaktiv gestaltet werden kann.

Die Interaktivität kann sich dabei durchaus auf einzelne Schichten des Schichtenmodells beschränken.

Beispiel 2.13:
Betrachtung der Interaktion im Schichtenmodell
Eine E-Mail wird im Internet gewöhnlich per SMTP [103] übertragen. Die Schichten 3 und 4 sind interaktiv und werden interaktiv genutzt. Die Schicht 5 (SMTP) ist zwar interaktiv, wird aber nur innerhalb eines fest vorgegebenen Schemas verwendet. Schicht 6 [41] ist zur Interaktivität ungeeignet. Schicht 7 ist nicht interaktiv, da Absender nur sendet und der Empfänger nur empfängt, und überdies eine zeitliche Entkopplung vorliegt. Eine Interaktivität der oberen Schichten müßte hier künstlich durch Versenden mehrerer Nachrichten eingeführt werden, wie dies u. a. bei automatischen FTP- oder HTTP-E-Mail-Gateways der Fall ist.

Die Schichten 4 und 5 bieten sich als Ansatzpunkt für interaktive Sicherungen an.

2.3.5 Nebenwirkungen und Risiken der Absicherung

Jede aktive Sicherungsmaßnahme beeinflußt das bestehende Kommunikationssystem und hat Auswirkungen, die die Funktion bestimmter Übertragungsmechanismen beeinträchtigen können. Prinzipiell geht mit stärkeren Sicherungsmaßnahmen auch eine stärkere Beeinflußung einher.

Die meisten Sicherungsverfahren bringen zeitliche Verzögerungen mit sich, was zu einer Überschreitung der zulässigen Latenzzeit führen und damit bereits im Normalbetrieb Störungen der Datenübertragung verursachen kann.

Sicherungsmaßnahmen sollten so ausgelegt sein, daß sie in gewisser Weise fehlertolerant sind, d. h. auch bei leichten bis mittleren Abweichungen von der dem Entwurf zugrundeliegenden Spezifikation des zu sichernden Systems ihre Sicherungswirkung aufrechterhalten. Eine technische Störung oder eine Fehlbedienung durch den Menschen soll nicht gleich zu einer Schwächung der Absicherung führen, weil damit zufällig oder durch den Angreifer inszeniert die Absicherung umgangen werden könnte.

Gerade diese Auslegung kann im Fehlerfall aber zu einer *Übersicherung* führen und sich gegen befugte Parteien richten (z. B. Daten nach Schlüsselverlust nicht mehr lesbar), wenn nämlich in einem Fehlerfall *außerhalb der Spezifikation* der Zugriff des Angreifers und der Zugriff der befugten Parteien nicht mehr eindeutig als solche erkannt und fehlerfrei als unerlaubter Zugriff abgewehrt oder als erlaubter Zugriff zugelassen werden. Eine unbeabsichtigte Wirkung der Sicherung gegen befugte Benutzer kann ernsthafte Folgen haben (Beispiel: medizinische Patientendaten im Notfall nicht verfügbar).

Die Kommunikationsverbindung und die zu übertragenden Daten sind daher darauf zu untersuchen, in welcher Weise sie gegen Beeinträchtigungen oder Versagen der Übertragungsfunktionen und Abweichungen von der Spezifikation anfällig sind.

2.4 Der Angreifer

2.4.1 Das Feindbild

Die System-, Netzwerk- und Kommunikationssicherheit im allgemeinen und die Kryptographie im besonderen sind nicht nur Wissenschaft, sondern auch *Kampfkunst*; sie haben die Abwehr eines Angreifers zum Ziel. Daher bleibt es nicht aus, daß gewisse Gemeinsamkeiten mit den physischen Kampf- und Kriegskünsten bestehen, auch

wenn martialische Gepflogenheiten und kriegerische Stilmittel der wissenschaftlichen Vorgehensweise sonst überwiegend fremd sind.

Ziel der System- und Kommunikationssicherheit ist es, Angriffe abzuwehren. Dazu ist es notwendig, den Angreifer und seinen Angriff zu kennen. Oft kennt man Angreifer und Angriff jedoch erst hinterher, also zu spät. Daraus kann man zwar nachträglich Nutzen ziehen um sich für weitere Angriffe zu rüsten, und man kann auch Angriffe gegen andere auswerten, aber den selbsterlittenen Angriff kennt man meist nicht im voraus.

Daher ist es notwendig, *Annahmen* über Angreifer und Angriff zu machen. Sind die Annahmen unrichtig oder unvollständig, mißlingt die Abwehr. Folglich müssen Annahmen möglichst umfassend und weitreichend sein.

Definition 2.14:
„Feindbild“
Das Feindbild ist die Gesamtheit der Kenntnisse, Annahmen und Vermutungen über den Angreifer.

Dabei gilt der

Grundsatz:
Wer oder was nicht zweifelsfrei zuverlässiger Freund ist, gehört zum Feindbild!

Die Positionierung einer Partei im Feindbild ist keineswegs die Unterstellung böser Absichten, sondern die (auch hypothetische) fehlende Unterstellung hinreichend guter Absichten. Es bedeutet lediglich, daß man einen Angriff über diese Partei in die Überlegungen mit einbezieht.

Beispiel 2.15:
Festlegung des Feindbildes
In einer Klinik soll das lokale Netzwerk gegen Angriffe von außen geschützt werden. Am Netzwerk befinden sich Computertomographiegeräte, die regelmäßig per Fernwartung oder Besuch eines Servicetechnikers durch den Hersteller gepflegt werden. Die Firmenpolitik des Herstellers läßt eine Offenlegung der Software oder anderweitige Eingriffe in das Gerät nicht zu; stattdessen verlangt er das Gerät so zu akzeptieren, wie es geliefert wird. Der Hersteller selbst soll zwar nicht als Angreifer angesehen werden, er kann und will aber seine eigene Systemsicherheit nicht gegenüber der Klinik beweisen.

Lösung:
Sicherheit und Kontrolle des Tomographiegerätes können nicht überzeugend nachgewiesen werden. Ein Angreifer könnte beim Hersteller einbrechen und dort die Software, die bei der nächsten Systemwartung auf das

System übertragen werden wird, angreifen. *Der Tomograph wird in das Feindbild einbezogen.* Das Kliniknetz muß also gegenüber dem Tomographen geschützt werden, etwa durch Zwischenschaltung eines Routers oder geeignete Programmierung einer Bridge als Paketfilter.

Beispiel 2.16:
Festlegung des Feindbildes
Ein Computerbenutzer möchte beliebige Software, die aus dem Internet oder von Disketten unbekannter Herkunft stammt, auf seinem Rechner verwenden. Eine Analyse der Software ist mit vertretbarem Aufwand (und aus rechtlichen Gründen) nicht möglich.

Lösung:
Die Software und der Benutzerprozeß werden in das Feindbild einbezogen. Betriebssystem, andere Prozesse, Datenbestände usw. müssen vor dem Prozeß geschützt werden.

2.4.1.1 Position des Angreifers

Das wichtigste Merkmal des Angreifers ist dessen *räumliche oder zeitliche Position*, also an welcher Stelle der Datenübertragung sein Angriff erwartet wird.

Im einfachsten Fall sind zur Kommunikation drei Teile notwendig, nämlich ein Sender, ein Empfänger und das Transportmedium der Kommunikationsverbindung. Hier ist aber weniger von Bedeutung, wer Sender und wer Empfänger ist, sondern wer das Interesse an der Absicherung hat. Deshalb werden stattdessen zwei Parteien eingeführt. Die Betrachtung erfolgt aus Sicht einer Partei, die ein Interesse an Absicherung hat. Deshalb wird die Partei, die die Absicherung betreibt, als die „eigene Partei“ bezeichnet (siehe Abb. 2.3; natürlich kann auch die andere Partei ein Interesse an Absicherung haben, was aber aus Symmetriegründen nicht betrachtet zu werden braucht).

Damit ergeben sich vier räumliche Einzelpositionen (vgl. Abb. 2.3) für den Angreifer, die nachfolgend in aufsteigender Reihenfolge bezüglich ihrer Bedrohlichkeit betrachtet werden. Greift der Angreifer aus mehreren Positionen an, so ist die für ihn stärkste ausschlaggebend:

1. Die Kommunikation kann so geführt werden, daß der Feind nicht in Kontakt mit den Daten kommt. Eine Barriere kann zwischen Angreifer und Kommunikationsverbindung errichtet werden. Die Schutzwirkung kann durch Stärkung der Grenze erreicht werden, schützt also das *Territorium* (territoriale Sicherung).

   Beispiel: Einrichten eines Firewall-Systems.

2. Die Kommunikation kann nicht am Feind vorbei erfolgen, sondern muß durch Feindesland geführt werden. Der Angreifer erhält dadurch Zugriff auf die Kommunikationsverbindung. Eine Barriere kann nicht errichtet werden, deshalb müssen die Daten geschützt werden (individuale Sicherung).

Beispiel: Verschlüsselung der Daten

3. Der Angreifer hat die Gegenseite erfolgreich übernommen oder ist selbst die Gegenseite[12]. Aufgrund der Auswirkung, die solch ein Angriff auf die jeweils andere Partei haben kann, ist ein Angriff auf eine Partei immer auch als Angriff auf die andere Partei zu werten (siehe auch 2.4.1.4).

   Ein Schutz der Daten ist hier nicht mehr möglich, weil der Angreifer mit dem befugten Benutzer zusammenfällt.

4. Der Angreifer übernimmt die *eigene* Seite erfolgreich. Sofern der Angreifer bereits am Ort und zum Zeitpunkt der Übertragung die eigene Seite erfolgreich übernommen hat und sich damit alle Kenntnisse, Befugnisse usw. zugeeignet hat, ist eine Absicherung nicht mehr möglich, die zwischen der eigenen Partei und dem Angreifer differenziert. Der Ausweg bestünde darin, die eigene Partei in das Feindbild aufzunehmen und die eigenen Befugnisse zu reduzieren. Bei genauer Betrachtung ist dies aber nur eine Zerlegung (Fragmentierung) der eigenen Partei in verschiedene (Unter-)Parteien.

   Wird die Übernahme der eigenen Partei befürchtet, jedoch eine gewisse räumliche oder zeitliche Ausdehnung angenommen, kann eine Fragmentierung der eigenen Partei die Möglichkeit zur Absicherung geben (siehe etwa 5.6.3.2, 5.6.3.3).

Entsprechend dieser Einteilung kann die Angreiferposition schematisch dargestellt werden, nämlich in den Positionen 1, 2, 3 und 4 (Abbildung 2.4).

2.4.1.2 Zeitpunkt des Angriffs

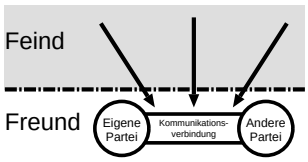
Nachdem der Ort des Angriffs betrachtet wurde, ist es naheliegend, auch den Zeitpunkt des Angriffs als Kriterium mit einzubeziehen. Auch hier bietet sich wieder eine Dreiteilung an, nämlich

- vor,
- während und
- nach

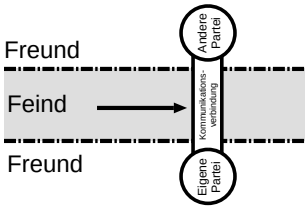
der Übertragung. Diese Einteilung charakterisiert den Angriff aber nur scheinbar. Bei genauer Betrachtung handelt es sich hier um unterschiedliche Angriffe. Der Angriff während räumlicher Übertragung ist ein Angriff auf die räumliche Datenübertragung zwischen den Parteien, die Angriffe vor und nach der Übertragung sind Angriffe auf die zeitliche Übertragung innerhalb einer Partei.

[12] Das ist weniger abwegig als es erscheinen mag. Wer z. B. „Online-Shopping“ im Internet anbieten will, muß sich wohl oder übel mit seinen Kunden herumschlagen, auch wenn diese ihn zu schädigen suchen.

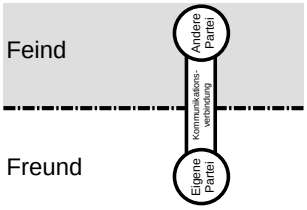
(a) Dreiteiliges Grundschema der Kommunikation: Der Angreifer nimmt eine von vier möglichen Angreiferpositionen ein, abhängig davon, welche der drei Teile er übernommen hat.



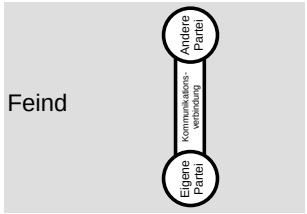
(b) Steht der Angreifer abseits, erfolgt die Kommunikation durch Freundesland und der Angreifer muß sich zuerst Zugang verschaffen. Schutz kann durch Abschottung *(Territorialschutz)* erreicht werden.



(c) Steht der Angreifer im Bereich der Kommunikationsverbindung (innerhalb der Route), muß die Kommunikation selbst abgesichert werden *(Individualschutz)*.



(d) Hat der Angreifer die Gegenseite gegenwärtig oder zukünftig übernommen, genügen äußere Schutzmaßnahmen nicht mehr, weil die Gegenseite sie prinzipbedingt durchdringen kann. Die Kommunikation muß auch *inhaltlich* geschützt werden.



(e) Besteht die Vermutung, der Angreifer hat in der Vergangenheit oder zukünftig die eigene Partei übernommen, muß auch die eigene Datenspeicherung abgesichert werden. Man muß sich *gegen sich selbst* schützen.

Abbildung 2.3: Positionen des Angreifers im Kommunikationsschema

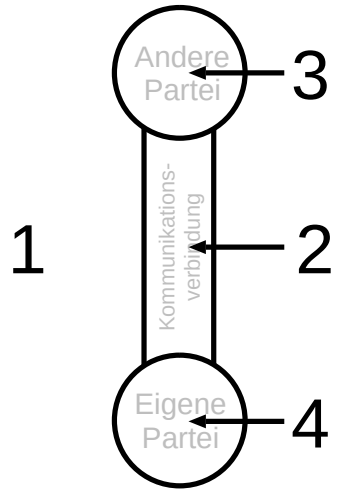


Abbildung 2.4: Die Position des Angreifers kann schematisch in einer dieser vier Positionen relativ zur Kommunikationsverbindung dargestellt werden.

Beispiel 2.17:
Angriff nach Übertragung
Ein Angreifer hört zunächst rein passiv eine verschlüsselte Datenübertragung ab und zeichnet diese auf. Zu einem späteren Zeitpunkt legt er die Aufzeichnung dem Empfänger vor und zwingt ihn unter Gewaltandrohung, die Daten erneut zu entschlüsseln.

Es liegen zwei Angriffe vor. Der erste richtet sich gegen die räumliche Datenübertragung, der zweite gegen die zeitliche Speicherung des Schlüssels.

2.4.1.3 Aktive und passive Angriffe

Wie bereits aus Beispiel 2.17 ersichtlich war, kann sich der Angreifer passiv und aktiv verhalten, also die Rolle eines unbefugten Empfängers (abhören) oder eines unbefugten Senders (fälschen) annehmen.

2.4.1.4 Die Parteien als Angreifer

Bereits in 2.4.1.1 wurde die Möglichkeit in Betracht gezogen, daß ein Angreifer die Position einer befugten Partei einnimmt. Der Angreifer kann durch einen erfolgreichen Angriff auf eine Partei und deren Übernahme in diese Position gelangt sein. In Abhängigkeit davon, was man als Befugnis auffaßt, kann aber auch eine böswillige Partei selbst schon befugter Benutzer sein (Beispiel: Bestellungsannahmen im Internet). Die

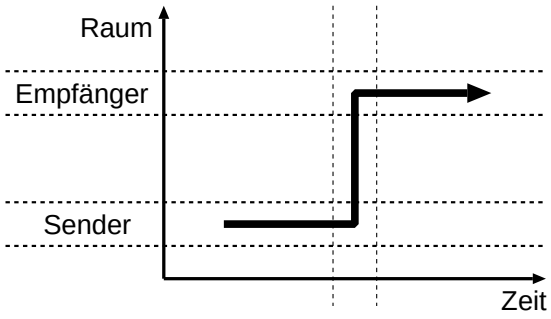


Abbildung 2.5: Eine gewöhnliche Datenübertragung zerfällt in mindestens drei getrennt zu betrachtende Übertragungsvorgänge, nämlich eine zeitliche Übertragung beim Sender, danach eine räumliche Übertragung zum Empfänger und dann eine zeitliche Übertragung beim diesem.

Gegenpartei wird hier bereits während der befugten Kommunikation als feindlich angesehen.

Auch die Vermutung eines *späteren* Angriffs auf eine zur Zeit der Kommunikation noch nicht als feindlich anzusehende Partei kann als Bedrohung aufgefaßt werden und dazu führen, daß die Gegenpartei frühzeitig als feindlich anzusehen ist.

2.4.1.5 Sender

Nimmt der Angreifer die Position des Senders ein, so kann er natürlich die Nachricht – zumindest teilweise – manipulieren. Auch wenn in der Nachricht erhebliche Redundanz steckt und der Empfänger Plausibilitätsprüfungen vornehmen kann, hat der Sender den Spielraum der Entropie. Hätte er hier nämlich keinen Spielraum, könnte er folglich nicht die Auswahl aus verschiedenen möglichen Nachrichten treffen und es könnte nur eine mögliche Nachricht geben[13]. Dann hätte die übertragene Nachricht keinen Informationsgehalt, die Kommunikation wäre nutz- und kapazitätslos und der Sender kein Sender mehr.

Die Nachricht selbst kann also nicht vor dem Angreifer geschützt werden. Maßnahmen zur Sicherung der Authentizität und Integrität helfen auch nicht weiter, denn die Vermutung des Angreifers in Senderposition hat ja gerade zur Folge, daß der Angreifer authentisch und integer arbeitet.[14]

Es besteht aber durchaus die Möglichkeit, den Sender im Unklaren zu lassen, *ob* er eine Nachricht bzw. Entropie übertragen hat und in der Konsequenz dessen auch, welche von mehreren möglichen Nachrichten er abgesandt hat.

[13] Das Unterlassen einer Sendung ist selbst schon als Nachricht zu werten, denn Senden und Nichtsenden sind schon zwei Möglichkeiten, aus denen der Sender wählen kann.

[14] Der Umkehrschluß: Könnte man den Angreifer durch Prüfung der Authentizität und Integrität abwehren, dann hätte er eben nicht die Position des Senders inne.

Die Adresse des Empfängers kann vor dem Sender geschützt werden, wenn die effektive Empfängeradresse durch Verlagerung in die höheren Schichten gesichert und durch weitere Maßnahmen wirksam geschützt wurde (siehe 3.6.2.1), und der Sender stattdessen eine scheinbare Empfängeradresse verwendet, die für ihn keinen Informationsgehalt birgt.

Die wichtigste und bekannteste Schutzmaßnahme gegen einen Angreifer in Parteienposition ist der Schutz des gemeinsamen Geheimnisses durch Verwendung von Public-Key-Verfahren.

2.4.1.6 Empfänger

Genausowenig, wie die Nachricht vor dem Sender geschützt werden kann, ist ein Schutz vor dem Empfänger möglich, denn anderenfalls wäre er nicht Empfänger.

In Analogie zur Unsicherheit des Senders, *ob* er eine Nachricht versandt hat, liegt es zunächst nahe, den Empfänger im Unklaren zu lassen, ob er etwas *empfangen* hat. Das ist aber nicht allgemein durchführbar, denn hier kommt es auf den Einzelfall und die Möglichkeiten des Empfängers an, die Nachricht zu prüfen. Es besteht aber die Möglichkeit, dem Empfänger – in besserer Analogie – Wissen vorzuenthalten, das ihm erlauben würde, gegenüber Dritten nachzuweisen, *daß* der Sender übertragen hat.

Auch hier kann wieder die Adresse der Gegenseite, also des Senders, geschützt werden.

2.4.1.7 Dritte Partei

Ungewöhnlich – aber nicht ausgeschlossen – ist die Position des Angreifers an der Stelle einer dritten Partei, denn es gibt Kommunikationsprotokolle, die eine dritte Partei miteinbeziehen.

Da auch die dritte Partei kommuniziert, sind naheliegenderweise alle Überlegungen anwendbar, die auch auf die normalen Parteien zutreffen. Weil aber die Beteiligung einer dritten Partei eine Besonderheit darstellt, muß auch mit Besonderheiten in der Position des Angreifers gerechnet werden.

Wenn etwa der dritten Partei die Rolle einer Schlüsselbehörde zukommt, ergeben sich besondere Folgen, wenn die Behörde pflichtwidrig handelt, und besondere Abwehrtechniken.

Gibt es eine dritte Partei, so bedeutet das, daß es außer der anzugreifenden Partei mehrere Parteien gibt, die vom Angreifer eingenommen worden sein können. Deshalb sind auch Angriffe mit der Position des Angreifers in mehreren Parteien zu betrachten.

2.4.2 Angriffszweck

Der Angreifer wird seine Angriffstrategie nach dem Zweck ausrichten, den er mit dem Angriff verfolgt. Die Abwehr muß sich ebenfalls darauf einstellen.

Grundsätzlich ist zu erwarten, daß der Angreifer versucht, eine der in Abschnitt 2.5.1 aufgezählten Eigenschaften der der in Abschnitt 2.5.3 dargestellten Sicherungsobjekte zu beeinträchtigen.

Trotzdem kann der Zweck des Angriffs bzw. der Nutzen, den der Angreifer aus dem Angriff zieht, genauer als in Abschnitt 2.5.1 beschrieben differenziert werden.

2.4.2.1 Wissensformen

Ein Angriff gegen die Vertraulichkeit (siehe 2.5.1), also eine Spionage, kann unterschiedliche Wissensformen hervorbringen (siehe hierzu auch Abschnitt 2.5.2.4). Die Differenzierung tritt am stärksten hervor, wenn man sie anhand eines Angriffs auf ein kryptographisches Geheimnis darstellt.

Ausgangspunkt der Überlegung ist das Geheimnis, das ein Element aus einer Menge von potentiell möglichen Geheimnis-Werten ist, denen aus Sicht des Außenstehenden eine bestimmte Wahrscheinlichkeitsverteilung zuzuordnen ist.

Beispiel 2.18:
Angriff gegen Chiffre

Das zu schützende Geheimnis ist ein DES-Schlüssel. Für den Außenstehenden ergibt sich eine Menge von (fast[15]) 2^{56} potentiell möglichen Schlüsseln. Die Wahrscheinlichkeiten sind gleichverteilt.

In der Regel zielt ein Angriff gegen den Schlüssel darauf ab, die Wahrscheinlichkeiten der möglichen Schlüssel mit einer von der Gleichverteilung möglichst stark abweichenden Verteilung bewerten zu können und so den (zu erwartenden) Suchaufwand zu verringern oder das Ergebnis interpretieren zu können.

Geht es aber z. B. darum, in einem Strafverfahren eine strafbare Übermittlung unerlaubter Inhalte zu beweisen, so genügt es nicht, nur einen Schlüssel zu kennen, der bei der Entschlüsselung ein erwartungsgemäßes Ergebnis liefert. Es muß ein Beweis erhoben werden, jeder andere mögliche Schlüssel also ausgeschlossen werden.

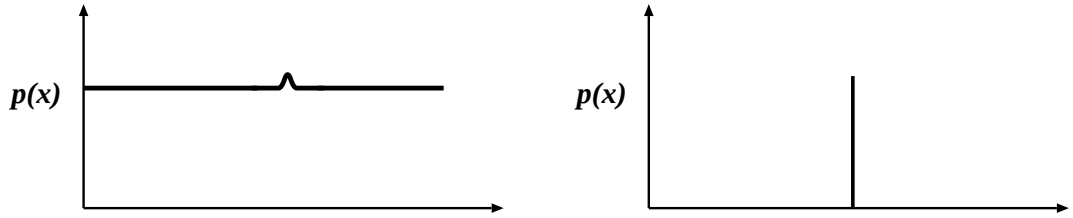
Der Erfolg eines Angriffes kann unterschiedliche Auswirkungen auf die Wahrscheinlichkeitsverteilung aus Sicht des Angreifers haben (siehe Abb. 2.6).

Im einfachsten Fall hat der Angreifer nur Informationen, die ihm nur geringfügige Änderungen an seiner Sichtweise der Wahrscheinlichkeitsverteilung erlauben und ihm so

[15] Abzüglich einiger weniger schwacher Schlüssel

Vorteile verschaffen. Diese Änderung kann sogar im Einzelfall unrichtig oder nachteilig sein; wesentlich ist, daß der Angreifer zumindest *im statistischen Mittel über viele Angriffe* Vorteile zieht, indem er etwa seinen Suchraum signifikant reduzieren oder eine günstige Suchreihenfolge angeben kann. Im Beispiel 2.18 könnte ein solcher Angriff in der Kenntnis gewisser Schwächen des Zufallszahlengenerators liegen, mit dem der Schlüssel erzeugt wurde.

Ein weitergehender Erfolg des Angreifers liegt darin, eine Vielzahl von potentiellen Werten oder sogar alle bis auf einen *ausschließen* zu können, also sicheres Wissen über die verbleibenden Werte zu erreichen und somit keinen signifikanten Aufwand mehr treiben zu müssen. Im Beispiel 2.18 könnte dies darin bestehen, daß der Angreifer den Schlüssel selbst in Erfahrung bringt.



(a) Statistisches Wissen (b) Sicheres Wissen

Abbildung 2.6: Ein gegen die Vertraulichkeit gerichteter Angriff zielt auf Erlangung von Wissen ab. Dabei ist jedoch zu unterscheiden, ob das erlangte Wissen nur zu einer Veränderung der Wahrscheinlichkeitsverteilung aller in Frage kommenden Werte führt, oder ob der Angreifer damit einen Beweis erbringen kann, d. h. alle anderen Werte sicher ausschließen kann.

Eine weitere Steigerung des Angriffserfolgs liegt vor, wenn das erhaltene Wissen der Gestalt ist, daß es unabhängig vom lokalen (und für andere unzuverlässigen) Wissensbestand des Angreifers ist, von jedem Dritten in gleicher Weise akzeptiert wird und *beweisfähig* ist. Ein Beweis liegt vor, wenn alle anderen Möglichkeiten ausgeschlossen sind.

Abwehrmaßnahmen müssen dies berücksichtigen und in unterschiedlicher Weise entgegenwirken, etwa durch Nivellierung der Wahrscheinlichkeitsverteilung gegenüber dem Angreifer, oder durch Erzeugen von Alternativen (Beweiskonter).

2.4.3 Aufwand und Kosten des Angriffs

Die notwendige Stärke und Art der Abwehrmaßnahmen hängt auch davon ab, mit welcher Energie der Angreifer den Angriff betreibt. Dazu müssen der Aufwand und die

Kosten abgeschätzt werden, die dem Angreifer durch den Angriff entstehen. Sicherungsmaßnahmen zielen letztlich darauf ab, den Aufwand und die Kosten eines Angriffs hochzuschrauben.

Dabei sind zwei Schwellwerte relevant:

Der absolute Aufwand orientiert sich an den technischen Möglichkeiten des Angreifers und den Kosten, die ihm entstehen. Dazu gehört u. a., welche Rechenleistung er aufbringen und wieviel Energie, Platz, Zeit und Geld er aufbringen muß um den Angriff durchzuführen.

Ziel von Abwehrmaßnahmen ist normalerweise, den absoluten Aufwand so hoch zu treiben, daß der Angreifer den Angriff unter Aufwendung aller im zur Verfügung stehenden Mittel nicht durchführen *kann*.

Der relative Aufwand ist der absolute Aufwand im Verhältnis zum Nutzen und Vorteil, den der Angreifer aus dem Angriff ziehen kann bzw. dem Aufwand, den der Angreifer zu treiben bereit ist.

Es kann deshalb auch Ziel der Abwehrmaßnahmen sein, den Aufwand so hoch zu treiben, daß der Angreifer nicht mehr angreifen *will*.

Die Beurteilung des Aufwandes, den der Angreifer zu treiben bereit ist, ist ausgesprochen schwierig, denn sie hängt davon ab, daß der Angreifer

- rational und ökonomisch vorgeht,
- in der Lage ist, das Kosten/Nutzenverhältnis realistisch einzuschätzen und
- die Kosten des Angriffs auch tatsächlich selbst zu tragen hat und sich nicht etwa Rechenleistung durch andere Angriffe erschlichen hat.

Bei der Abschätzung von Zeit und Kosten sind die Entwicklung der Computertechnik und der Preisverfall zu berücksichtigen.

2.5 Das Schutzobjekt

2.5.1 Sicherungszweck

Eines der grundlegendsten Kriterien, nach denen Sicherungsmaßnahmen eingeteilt werden können, ist der Sicherungszweck, also die Eigenschaft der Informationsübertragung, die man durch den Einsatz der Sicherungsmaßnahme herstellen will bzw. aus der Sicht des hier verwendeten Modells die *ungünstige* Eigenschaft, die man einer Informationsübertragung *nehmen* will. Im Allgemeinen lassen sich die erzielbaren Eigenschaften grob in vier Kategorien einteilen.

2.5.1.1 Vertraulichkeit

Ist bei einer Informationsübertragung in gewissem Umfang gewährleistet, daß die übertragene Information nur den beabsichtigten Empfängern zur Kenntnis gelangen kann, also eine *Geheimhaltung* vorliegt, so spricht man von Vertraulichkeit.

2.5.1.2 Integrität, Authentizität, Echtheit

Ebenfalls von Bedeutung ist die *Unfälschbarkeit* einer Nachricht. Hierbei wird zwischen der Resistenz gegen Veränderung und der Resistenz gegen falsche Herkunft unterschieden:

Die *Integrität* einer übertragenen Nachricht ist gewährleistet, wenn sichergestellt ist, daß die Nachricht unverändert so beim beabsichtigten Empfänger ankommt[16], wie sie vom befugten Absender erstellt worden ist, also von dem Absender, den der Empfänger – insbesondere aufgrund sekundärer (siehe Abschitt 2.5.3) oder anderer Informationen – für den Absender halten muß bzw. soll. Dies zieht nach sich, daß der Empfänger im Falle des Empfangs einer veränderten Nachricht erkennen kann, daß die Nachricht verändert wurde, und diese Erkenntnis in die Annahme über den Absender mit einbeziehen kann, oder der Empfang einer veränderten Nachricht nicht möglich ist.

Die *Authentizität* einer übertragenen Nachricht ist gewährleistet, wenn sichergestellt ist, daß die Nachricht tatsächlich von dem Absender erstellt wurde, den der Empfänger – insbesondere aufgrund sekundärer (siehe Abschitt 2.5.3) oder anderer Informationen – für den Absender halten muß bzw. soll. Auch hier muß der Empfänger auf den Empfang gefälschte Nachrichten reagieren können, falls dieser nicht durch die Sicherung ausgeschlossen ist.

Die (inzwischen schon klassische) Trennung zwischen Integrität und Authentizität erscheint jedoch nicht aus jedem Blickwinkel als naheliegend und sinnvoll. Während es für den Angreifer zwar einen Unterschied darstellt, ob er nur eine aufgefundene Übertragung verändern oder selbst eine initiieren muß, und es auch für den Sicherheitsentwurf eine Rolle spielt, gegen welchen Angriff man vorgeht, ist aus der Sicht des Geschädigten und der Beeinträchtigung des Schutzobjektes vor allem die Tatsache wichtig, daß die übertragenen Daten *nicht echt* sind. Ob der Angreifer dabei eine zulässige Nachricht oder Kommunikationsverbindung als „Rohmaterial“ verwendet hat, ist nur in Einzelfällen von Bedeutung[17].

[16] Die Betrachtung setzt voraus, *daß* die Nachricht tatsächlich ankommt. Integrität und Authentizität verlangen nicht, daß die Nachricht überhaupt ankommt.

[17] Man kann etwa die Frage aufwerfen, ob das Abfangen einer Banküberweisung über elektronische Medien und das Absenden einer komplett neuen Überweisung mit der abgefangenen TAN eine Verletzung der Integrität oder der Authentizität darstellt. Man neigt dazu, dies als Verletzung der Integrität zu werten, weil der Angreifer auf eine befugte Sendung angewiesen ist. In kryptographischer Hinsicht verändert er aber nicht die Nachricht, sondern erlangt ein Geheimnis und sendet mit diesem selbständig. Die TAN ist nicht Teil der Nachricht, sondern Hilfslast zur Authentifikation. Die

Auch außerhalb der technischen Informationsübertragung wird zwischen dem Angriff auf die Authentizität und dem Angriff auf die Integrität nicht immer signifikant unterschieden:

Zitat 2.19: § 267 I StGB:
Wer zur Täuschung im Rechtsverkehr eine unechte Urkunde herstellt, eine echte Urkunde verfälscht oder eine unechte oder verfälschte Urkunde gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

Dennoch ist es notwendig, die verschiedenen Eigenschaften in Bezug auf die hier angewandte Sichtweise einzuordnen und zu definieren[18]. Besondere Bedeutung kommt hierbei der Absenderadresse zu, die der Empfänger aufgrund impliziter Annahme oder expliziter Angabe für die Absenderadresse hält und daraus auf den Absender schließt.

Definition 2.20:
Integrität, Authentizität, Vollständigkeit, Eindeutigkeit, Echtheit

Integrität
liegt vor, wenn die vom Empfänger einer Nachricht dieser (implizit oder explizit) zugeordnete Absenderadresse mit der (einer) korrekten Adresse des tatsächlichen Absenders der dem Empfänger als Nachricht vorliegenden Nutzlast übereinstimmt.

Authentizität
liegt vor, wenn die Vorstellung des Empfängers vom *tatsächlichen* Absender einer Nachricht auf die der vom Empfänger eben dieser Nachricht (implizit oder explizit) zugeordneten Absenderadresse abgebildet wird (im Anschluß an Definition 2.4).

Vollständigkeit
liegt vor, wenn der unbemerkte Verlust oder die Unterschlagung von Nachrichten unmöglich sind.

Eindeutigkeit
liegt vor, wenn eine Nachricht bzw. eine Kopie davon einem bestimmten Absendevorgang zweifelsfrei zugeordnet werden kann.

Differenzierung zwischen Integrität und Authentizität ist hier weder klar definiert, noch sonderlich hilfreich.

[18] Bei dieser Definition kommt dem Empfänger gegenüber der üblichen (und bislang nicht exakt definierten) Auffassung von Authentizität und Integrität eine höhere Bedeutung zu. Insbesondere erlangen hier Authentizität und Integrität erst dann an Bedeutung, wenn die Nachricht empfangen wurde und der Empfänger eine Zuordnung vorgenommen hat. Nicht die Eigenschaft der Nachricht, sondern die Wirkung beim Empfänger steht im Vordergrund.

Dazu gehört, daß zuverlässig unterschieden werden kann, ob zwei vorliegende Nachrichten Kopien der Nachricht eines Sendevorganges oder zwei Sendevorgängen mit inhaltsgleichen Nachrichten entstammen. Dies ist notwendig, da es bei digital dargestellten Nachrichten kein Original und keine Urkunde im eigentlichen Sinn gibt.

Echtheit
liegt vor, wenn Integrität, Authentizität, Vollständigkeit und Eindeutigkeit vorliegen.

2.5.2 Weitere Sicherungsziele

2.5.2.1 (Un-)Beweisbarkeit gegenüber Dritten

Gelegentlich will der Empfänger einer Nachricht einem Dritten Eigenschaften der Nachricht – Herkunft, Zeitpunkt usw. – nachweisen. Manchmal will aber auch der Sender verhindern, daß der Empfänger den Nachweis führen kann.

Der Sender könnte den Nachweis relativ einfach dadurch verhindern, daß er seine Position als befugte Partei verläßt und wie ein normaler Angreifer handelt – und zwar absichtlich so schlecht, daß der Angriff augenfällig wird und sich der Sender damit leicht auf einen Angriff durch den anderen oder einen fingierten Dritten berufen könnte. Dieser Weg ist aber keine Lösung, denn der Empfänger müßte über den Verlust der Nachweisbarkeit hinaus stets mit einem echten Angriff rechnen, den er nicht erkennen kann. Wenn es keinerlei Differenzierung zwischen befugtem Verhalten und einem Angriff gibt, stellt dies keine Sicherung mehr da.

Die Frage der Nachweisbarkeit kann sich also nicht auf den Nachweis gegenüber dem Empfänger beziehen, denn der Empfänger soll sich stets von den fraglichen Eigenschaften überzeugen können, anderenfalls der Sinn der Sicherung fraglich wäre. Beweisbarkeit und Unbeweisbarkeit beziehen sich nur auf den Nachweis gegenüber dem unbeteiligten Dritten, und zwar *unabhängig* vom Nachweis gegenüber dem Empfänger.

Beispiel 2.21:
Parteienspezifische Beweiskraft
Zwei Parteien haben gleichartigen Zugang zu einer technischen Einrichtung, beispielsweise einem Tresor, zu dem es zwei gleiche Schlüssel gibt.

Wird die Einrichtung durch eine Partei betätigt, beispielsweise als der wertvolle Inhalt des Tresors entnommen, weiß die andere Partei mit Sicherheit, wer die Einrichtung betätigt hat, kann dies aber nicht gegenüber einem Dritten nachweisen. Die Partei, die den Inhalt entnommen hat, kann behaupten, die andere Partei hätte den Inhalt entnommen.

2.5.2.2 Verfügbarkeit

Die Sicherung der Verfügbarkeit wird seltener betrachtet. Sie ist auch nicht in abstrakter Allgemeinheit zu behandeln, sondern hängt sehr stark vom Einzelfall ab.

Eine ordnungsgemäße Kommunikation verursacht Aufwand und Kosten bei den Parteien. Der Sender muß mindestens den Sendevorgang unternehmen, der Empfänger muß mindestens während des Empfangs Speicherplatz aufbringen.

Beide Parteien müssen diesen Aufwand zumindest so lange treiben, wie sie von einer ordnungsgemäßen Kommunikation ausgehen müssen, also bis zur Erkennung eines Angriffs.

Wird ein Angriff erkannt, so ist es in der Regel für die Parteien naheliegend, in irgendeiner Weise auf den Angriff zu reagieren und damit Aufwand zu treiben oder seinen Zustand zu verändern, das heißt in einen anderen Zustand zu wechseln.

Genau darin kann aber die Absicht eines Angriffs liegen. Der Angreifer darauf abstellen sein Opfer dazu zu bringen,

- Aufwand zu treiben bis der Angriff erkannt wird (Prophylaxe) oder
- den Angriff zu erkennen, darauf zu reagieren und Aufwand zu treiben oder den Zustand zu wechseln (Reaktion),

um ihm so Schaden zuzufügen. Ist die Wirkung des Angriffs so hoch, daß die normale Funktion des angegriffenen Systems signifikant beeinträchtigt wird, spricht man auch von einer *Denial-of-Service-Attacke*.

Bemerkenswert ist dabei, daß die Erkennung des vordergründigen Angriffs und Abwehrmaßnahmen die Absichten des Angreifers nicht durchkreuzen, sondern ihnen möglicherweise sogar entgegenkommen. (Siehe auch 3.11)

Beispiel 2.22:
Denial of Service

Mobilfunk-Anbieter stellen normalerweise jedem Kunden einen automatischen Anrufbeantworter zur Verfügung. Der Anrufbeantworter ist dem befugten Benutzer meistens auf zwei Arten zugänglich, nämlich über sein Mobiltelefon (Authentifikation durch die Karte) und über jedes andere Telefon. In letzterem Fall muß der Kunde eine PIN als Paßwort eingeben. Wird dreimal hintereinander die falsche PIN eingegeben, wird der Anrufbeantworter gesperrt.

Kennt der Angreifer die Telefonnummer seines Opfers – was ja nicht schwer ist – kann er dessen Anrufbeantworter anwählen und drei willkürliche PINs eingeben um den Anrufbeantworter zu sabotieren.[19]

[19] Wenn der Angreifer Glück hat, trifft er dabei sogar die richtige PIN.

Beispiel 2.23:
Denial of Service durch Angreiferposition
Nach den Atombomben-Versuchen der französischen Regierung auf dem Mururoa-Atoll wurden verschiedene Rechner und Netzwerke der Regierung wochenlang aus dem Internet mit gefälschten und unsinnigen Internet-Paketen aller Art bombardiert. Zwar gelang kein nennenswerter Einbruch, und keines der Pakete richtete für sich gesehen erwähnenswerten Schaden an, aber die Rechner waren über längere Zeit so stark belastet, daß sie praktisch vom Internet abgeschnitten waren.

2.5.2.3 Frühe Angriffserkennung

Sicherheit ist teuer, sie kostet Geld, Zeit, Rechenleistung usw. Selbst wenn die Erkennung von Angriffen zuverlässig funktioniert, könnte es ein Angreifer, der keinen erfolgreichen Angriff durchführen kann, gerade darauf anlegen, *erkennbare* und damit vordergründig erfolglose Angriffe zu unternehmen und damit die Aufwendung der Kosten zur Angriffserkennung zu provozieren.

Ziel des Entwurfs kann es daher auch sein, die mittleren, zu erwartenden oder maximalen Kosten der Sicherungsmaßnahmen in vorgegebenem Rahmen zu halten.

Diese Anforderung scheint trivial, denn Kostenersparnis ist generell Ziel des Algorithmenentwurfs; sie ist aber nicht trivial. Die Kosten zur Abwehr eines Angriffes hängen vom Feindbild und der Angriffserwartung ab. Je nach Differenzierung und Angriffswahrscheinlichkeit können unterschiedliche Verfahren zu unterschiedlichen Kosten führen.

Beispiel 2.24:
Kombination billiger und starker Verfahren
Es sollen im Internet Bestellungen entgegengenommen werden. Aus Gründen der Diskretion sollen die Bestellungen verschlüsselt übermittelt werden; sie müssen außerdem mit allgemeingültigen Signaturen versehen werden, damit die Bestellung im Streitfall gegenüber Dritten bewiesen werden kann.

Die Prüfung von Signaturen ist jedoch teuer in Bezug auf Rechenleistung. Dieser Aufwand könnte das Ziel eines Angriffs sein, der mit einer Vielzahl von „Bestellungen“ aus Zufallsdaten das System überlastet und die Annahme von ernsthaften Bestellungen beeinträchtigt.

Zur sicheren Verschlüsselung muß ein authentischer Schlüsseltausch erfolgen. Ergänzt man das Protokoll derart, daß die zu verschlüsselnden Daten eine einfache und schnell zu prüfende CRC- oder Quersumme tragen müssen, können auf „preiswerte“ Weise zwei Angreiferpositionen differenziert werden.

Der Angreifer, der sich nicht auf einen authentischen – und damit bei Fehlverhalten ihn kompromittierenden – Schlüsseltausch einläßt oder andere Verbindungen stört, hat keinen gemeinsamen Sitzungsschlüssel mit dem Server. Er kann daher die Prüfsumme nur mit sehr geringer Wahrscheinlichkeit treffen und damit im Mittel nur sehr viel geringere Kosten verursachen.

Der Angreifer, der sich auf einen richtigen Schlüsseltausch einläßt und dann Bestellungen mit korrekter CRC-Summe, aber falscher Signatur sendet, kann höhere Kosten verursachen, seine Identität ist aber nach dem authentischen Schlüsseltausch (bei Verwendung zertifizierter Schlüssel) dem Angegriffenen bekannt (wobei allerdings noch kein Dritten gegenüber wirksamer Beweis vorliegt, weil der Server den Angriff auch leicht simuliert haben könnte).

2.5.2.4 Beweislast

Eine besondere – und dennoch oft vernachlässigte – Rolle kommt der Frage der Beweislast zu, nämlich dann, wenn es darum geht, daß der Verteidiger etwas zu beweisen hat oder der Angreifer etwas beweisen will.

Soll etwa die Vertraulichkeit geschützt werden, so stellt sich die Frage,

- ob bewiesen oder der Beweis verhindert werden soll, daß eine bestimmte Nachricht übertragen wurde,
- ob der Angreifer statistisches Wissen erlangen will (vergleiche Abschnitt 2.4.2.1 und Abbildung 2.6 auf Seite 53) oder
- ob bewiesen oder der Beweis verhindert werden soll, daß eine bestimmte Nachricht *nicht* übertragen wurde.

Anders gesagt: Geht es darum, dem Angreifer den Beweis zu verderben (Ausrede finden), selbst einen (Schein-)Beweis zu erstellen oder sich statistisch neutral zu zeigen?

Eine ähnliche Fragestellung ergibt sich bei der Echtheit (Abschnitt 2.5.1.2):

- Muß der Verteidiger die Un-/Echtheit einer Nachricht beweisen oder
- will der Angreifer die Un-/Echtheit nachweisen?

Die Frage der Beweislast wird ebenfalls regelmäßig vernachlässigt.

Beispiel 2.25:
Beweislast beim „Telebanking“
Bucht eine Bank vom Konto des Kunden Geld ab, so obliegt ihr eigentlich die Beweislast, daß sie dazu ermächtigt bzw. beauftragt war. Sie muß im Streit den unterschriebenen Scheck oder Überweisungsauftrag vorlegen.

Die Einführung von Geldautomaten [97, 1, 2] und von „Telebanking“ über das Internet (s. Abschnitt 1.5.2) hat den Banken außer der Kostenersparnis auch noch eine schleichende Beweislastumkehr gebracht: Die Systeme sind so konstruiert, daß es keinen Dritten gegenüber wirksamen Beweis für die Vornahme oder Nichtvornahme einer Verfügung geben kann. Bei Geldautomaten behauptet die Bank einfach, die PIN wäre eingegeben worden. Beim „Telebanking“ wird nur die TAN eingesetzt, die ebenfalls keinen Beweis liefert, sondern der Bank die Möglichkeit zur beliebigen Behauptung einräumt.

Die Banken haben es erreicht, die fehlerhafte Rechtsmeinung zu verbreiten, es läge ein sog. „Beweis des ersten Anscheins“ und damit eine Beweislastumkehr vor, weshalb der Kunde gezwungen ist, etwas zu beweisen, was er nach der Konstruktion des Systems gar nicht beweisen kann, nämlich die Unechtheit oder das Nichtvorliegen einer Kontenverfügung.

Bemerkenswerterweise rechtfertigt der sog. „Anscheinsbeweis“ keine Beweislastumkehr, sondern stellt nur eine *Beweiserleichterung* dar, wenn ein Sachverhalt nach der „Lebenserfahrung“ auf einen bestimmten (typischen) Verlauf hinweist [40]. Im Falle der unerlaubten Abbuchung aber nach einer undefinierten „Lebenserfahrung“ von deren Korrektheit auszugehen und dem Kunden eine praktisch nicht zu erbringende Gegenbeweislast aufzuerlegen, heißt in diesem Kontext nichts anderes, als die Beweislast der Bank für die Echtheit einer Verfügung schlicht abzuschaffen. Dies ist ein ganz erheblicher Entwurfsfehler, der auch durch den euphorisch erwarteten Einsatz biometrischer Systeme nicht verhindert, sondern im Gegenteil nur noch verschlimmert wird.

Es wäre aber falsch, hieraus zu folgern, daß Geldautomaten und „Telebanking“ keinerlei Sicherheit böten. Diese Systeme bieten im Gegenteil sogar ein sehr hohes Maß an Sicherheit und es muß davon ausgegangen werden, daß diese Sicherheit gewollt und gezielt konstruiert ist.

Die erreichte Sicherheit bezieht sich aber nicht auf die Interessenlage des Kunden, sondern auf die Interessenlage der Bank, aus deren Sicht der widerspenstige Kunde eindeutig zum Feinbild gehört.

Damit stellen diese – auf den ersten Blick als höchst mangelhaft erscheinenden – Systeme in Bezug auf ihre Sicherheit überraschend eine überaus klare und effektive, damit aber auch subtile Konstruktion dar:

- Ein Beweis gegen die Bank ist nicht möglich. Die Bank ist frei in ihren Behauptungen, d. h. sie kann einen Vorgang behaupten, ihn abstreiten oder einen anderen Inhalt (anderer Betrag usw.) behaupten.
- Die Bank kann über den sog. „Anscheinsbeweis“ einen vermeintlichen Beweis gegen den Kunden erbringen.

- Der Kunde ist nicht in der Lage, einen Gegenbeweis zu erbringen. Er kann nicht beweisen, eine Kontoverfügung vorgenommen zu haben oder welchen Inhalt sie hatte. Sogar dann, wenn er ein „Alibi“ hat, wird ihm oft noch unterstellt, er habe die Scheckkarte und die PIN böswillig und in Betrugsabsicht weitergegeben.

Auch das ist als „Sicherheit“ anzusehen, sie ist aber eindeutig nur auf die Interessenlage der Bank ausgelegt. *Zu dieser Konstruktion paßt das Feindbild des befugten Bankkunden besser als das eigentlich naheliegendere Feindbild des kriminellen Dritten.*

Dieses Beispiel zeigt, wie diffizil die Bestimmung der Beweislast sein kann und welche dramatischen Folgen für die Gesamtsicherheit des Systems schon kleine Fehler bei der Einschätzung der Beweislast und der Festlegung des Feindbildes haben können.

2.5.2.5 Fehlerkorrektur und -resistenz

„Safety“ und „Security“ dürfen nicht miteinander verwechselt werden. Das bedeutet aber nicht, daß das jeweils andere ignoriert werden kann.

Gerade dann, wenn eine Übertragung über einen gestörten Kanal erfolgen muß, ist es notwendig, den Signal-Rauschabstand zu erhöhen und somit Redundanz einzubringen, außerdem nicht nur eine Fehler*erkennung* (wie zum Schutz der Integrität), sondern auch eine Fehler*korrektur* vorzunehmen.

Daher ist zu prüfen, ob diese zusätzliche Redundanz, die nicht nur als fehlerkorrigierender Code, sondern z. B. auch als TCP-Header vorliegen kann, die Sicherheit – insbesondere die Vertraulichkeit – nicht beeinträchtigt.

Dabei sind auch Interferenz- und Verstärkungseigenschaften zu berücksichtigten. Tritt bei der Übertragung nur ein einzelner Bit-Fehler auf, so kann dies bei verschlüsselten Daten dazu führen, daß eine Teil der Nachricht (z. B. eine Blockbreite einer Blockchiffre), der Rest der Nachricht (je nach Betriebsart) oder die gesamte Nachricht (vgl. Abschnitt 5.4.2) unlesbar werden. Ebenso kann ein einzelner Bit-Fehler die Signatur einer Nachricht nicht nur teilweise, sondern komplett ungültig machen.

Ein Beispiel für eine kommutative Verbindung aus Chiffre und Fehlerkorrektur ist in [61] zu finden.

2.5.2.6 Begrenzung der Sender- und Empfängerpositionen

Die räumliche und zeitliche Position und Ausdehnung sind wichtige Eigenschaften des befugten Senders und des befugten Empfängers (vgl. Abschnitt 2.3.1 und Abb. 2.2).

Es ist daher naheliegend, durch organisatorische Maßnahmen (Abschnitt 3.6) eine Trennung zwischen Parteien innerhalb der erlaubten Positionen und außerhalb derer

herzustellen. Die Wirkung liegt darin, daß ein Angreifer außerhalb dieser Abgrenzung nicht mehr die gefährlicheren Positionen der befugten Parteien (Abb. 2.3 d und e), sondern nur noch die leichter abzuwehrenden Positionen außerhalb (Abb. 2.3 b und c) einnimmt.

2.5.3 Komponenten

Bei einem Transport werden regelmäßig zwei Lasten transportiert, die eigentliche Nutzlast und Hilfslasten, die den Transport erst ermöglichen. Ein Brief muß außer seinem Inhalt auch immer eine Empfängeradresse mit sich tragen, damit er zugestellt werden kann. Zum Telefonieren müssen Telefonnummern übertragen werden, außerdem die Signale, die über die Verbindung informieren.

Gleiches gilt auch bei Rechenanlagen für zeitliche und räumliche Medien. Fast immer werden der Nutzlast Zusatzinformationen hinzugefügt, die der Adressierung, der Sicherung oder protokollarischen Zwecken dienen (z. B. Startbits bei einer V.24-Schnittstelle in Schicht 1, oder „Mit freundlichen Grüßen“ unter einem Brief). Im Schichtenmodell können in jeder einzelnen Schicht solche Zusatzinformationen hinzugefügt werden. Nutzlast und Zusatzinformationen einer Schicht bilden zusammen die Nutzlast der nächstniedrigeren Schicht (siehe Abb. 2.7).

Die Nutzlast, also die Information, deren Übertragung eigentlicher Zweck einer Kommunikation, wird nachfolgend als *primäre* Information bezeichnet. Die hinzugefügte Hilfslast, also die Informationen, die für die Übertragung selbst benötigt werden, wird nachfolgend als *sekundäre* Information bezeichnet. Informationen, die zum Zweck der Absicherung hinzugefügt werden, werden nachfolgend als *Sicherungsinformationen* bezeichnet.

Es stellt sich zwangsläufig die Frage, wie, wo und in welchem Umfang sich Sicherungsmaßnahmen auf primäre und auf sekundäre Informationen beziehen sollen.

Da Hauptinteresse liegt in einer möglichst weitreichenden und anhaltenden Sicherung vornehmlich der Primärinformationen. Aus dieser Sicht muß die Sicherung möglichst hoch liegen, in den Schichten 5-7. Damit sind die Sekundärinformationen der Schichten 1 bis 4 ungeschützt.

Die Sekundärinformationen der niederen Schichten entfalten aber ein eigenes Schutzbedürfnis gegen passive und aktive Angriffe. Durch Abhören und Auswerten der Sekundärinformationen könnte eine *Verkehrsanalyse* durchgeführt werden, die oftmals unerwünscht ist. Auch können Sekundärinformationen mit Primärinformationen übereinstimmen oder korrelieren[20]. Aktive Angriffe können sich gegen die Funktionen der unteren Schichten richten.

[20] Dazu kann schon die Tatsache, daß überhaupt kommuniziert wird, gehören, ebenso Zeitpunkt und Umfang der Übertragung, Adressen usw.

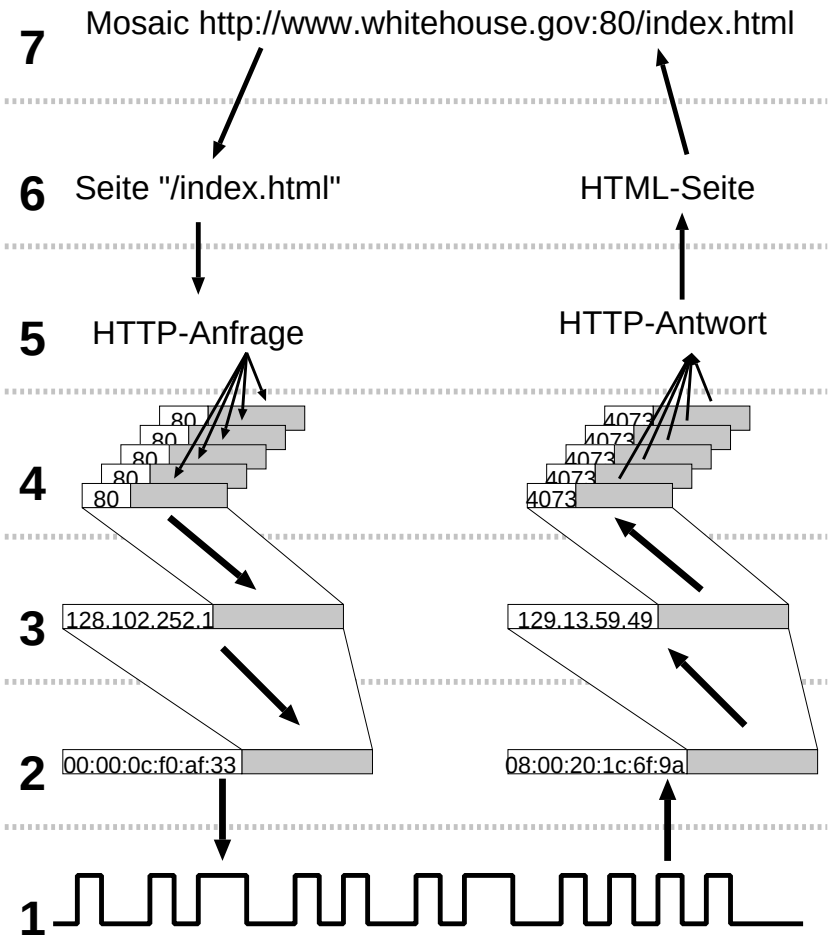


Abbildung 2.7: Nutzlast und Hilfslast im Schichtenmodell: Die Nutzlast und die Hilfslast einer Schicht bilden zusammen die Nutzlast der darunterliegenden Schicht. Das Beispiel zeigt die Anfrage und die Übertragung einer WWW-Seite.

Es ergibt sich die Notwendigkeit einer mindestens doppelten Sicherung, nämlich eine Sicherung auf hohen Schichten, die eine weitreichende Absicherung der Nutzinformationen bewirken, und eine Sicherung auf niederen Schichten, die die Absicherung der Transportfunktionen bewirkt (zur mehrfachen Sicherung vgl. Abschnitt 4.1).

2.5.3.1 Nutzlast

Der eigentliche Inhalt der Datenübertragung kann z. B. durch organisatorische oder die bekannten kryptographischen Verfahren geschützt werden.

2.5.3.2 Hilfslast

Der Vorgang der Datenübertragung erfordert in der Regel technische Hilfsinformationen wie z. B. Adressen, Paketnummern, Prüfsummen usw. (vgl. Abschnitt 2.5.3). Diese Informationen können Verkehrsanalysen oder in Verbindung mit weiteren Informationen Rückschlüsse auf die Nutzlast ermöglichen. Abhilfe kann hier durch Absicherung auf einer niedrigeren Schicht (Abschnitt 4.1) oder Tunnelung – d. h. Einpacken der Datenübertragung in einer anderen, abgesicherten Datenübertragung – erreicht werden.

2.5.3.3 Sender- und Empfängeradressen

Ein besonders sensibler Teil der Hilfslast sind die Absender- und Empfängeradressen. Jede Schicht kann dabei ihre eigenen unabhängigen Schichten haben. Betrachtet werden hier ausschließlich die Adressen, die zum Zweck des Transportes verwendet werden und zum Funktionieren des Transportmechanismus benötigt werden.

2.5.3.4 Sender- und Empfängeridentität

Eine ähnliche Bedeutung wie den vorgenannten Sender- und Empfänger*adressen*, deren Zweck im Funktionieren der Übertragung liegt, und die auch ohne Sicherungsmaßnahmen benötigt werden, kommt auch den Sender- und Empfängerangaben zu, die nicht unmittelbar der Übertragung, sondern der Funktion von Sicherungsmaßnahmen dienen, etwa die Angabe, welcher Schlüssel zum Entschlüsseln oder Prüfen einer Signatur zu verwenden ist.

Diese Angaben können mit den Transportadressen zusammenfallen.

2.5.3.5 Redundanz und Irrelevanz

Darüberhinaus sind auch alle sonstigen Lasten zu betrachten, die weder als Nutzlast (also der eigentlichen Nachricht), noch als Hilflast (also der Übertragung dienend) angesehen werden können, sondern der Funktion der Sicherungsmaßnahmen dienen, beispielsweise Signaturen oder Public-Key-verschlüsselte Sitzungsschlüssel.

2.5.3.6 Vorgang

Den Vorgang der Datenübertragung selbst zu verbergen ist nicht ohne weiteres möglich, es sei denn durch Unterlassen. Die zu übertragende Information muß in irgendeiner Art und Weise auf einem zeitlichen oder räumlichen Datenträger untergebracht werden, der regelmäßig nicht nur endlichen, sondern sogar einen überschaubar kleinen

Umfang hat. Jede Information belegt Platz, der nicht mehr für andere Informationen zur Verfügung steht. Dies kann bemerkt werden.

Ebenso heben sich Informationen normalerweise durch ihr charakteristisches Verhältnis aus Entropie und Redundanz von ihrer Umgebung ab. Zwar kann das für die Umgebung typische Verhältnis oft nachgeahmt werden, aber in einer entropiefreien Umgebung (weißes Blatt Papier, schalltoter Raum, Funkstille) fällt dies schwer. In einer Formation ist *In*formation nicht möglich.

Das Verbergen ist also nur in einer geeigneten Umgebung möglich. Die Übertragung muß dann so verändert werden, daß sie in der Umgebung nicht mehr mit vertretbarem Aufwand gefunden werden kann, weil sie nicht lokalisierbar oder nicht identifizierbar ist.

Diese Techniken werden allgemein unter dem Begriff „Steganographie“ zusammengefasst.

2.5.3.7 Umfang/Energie

Auch der Umfang der Datenübertragung kann Rückschlüsse auf den Inhalt zulassen und damit Schutzobjekt werden.

Hier kann es notwendig sein, die Datenübertragung entweder gänzlich zu verbergen (s.o.), oder den Umfang zu verschleiern, indem unterschiedliche Kompressionsverfahren verwendet bzw. Füllinformationen angehängt werden. Dies macht jedoch in der Regel die Anwendung kryptographischer Methoden notwendig, damit einem Angreifer eine Trennung der Daten in Nutz- und Fülldaten unmöglich wird.

2.5.3.8 Ort und Zeit

Der Zeitpunkt der Datenübertragung kann ebenfalls durch Verbergen der ganzen Übertragung oder durch Auffüllen getarnt werden. Der Zeitraum einer Datenübertragung ist ein lokales Ansteigen in der Übertragungsaktivität. Sorgt man durch Auffüllen für eine regelmäßige oder eine schwer zu beurteilende Aktivität (Rauschen), also dafür, daß der Aktivitätsverlauf entweder gar keine oder die volle mögliche Entropie trägt, so kann damit der Zeitpunkt der Übertragung der Nutzlast verborgen werden.

2.5.3.9 Schutz gegen multiple Angriffe

In die bisherigen Überlegungen wurde nur die isolierte Betrachtung einzelner Übertragungsvorgänge bzw. Nachrichten einbezogen.

Es ist aber auch zu untersuchen, ob die Kombination mehrerer Schutzobjekte ein neues Schutzobjekt hervorbringen kann. Dies könnte etwa dann der Fall sein, wenn der Angreifer aus einzelnen Übertragungsvorgängen noch keine Schlüsse ziehen, aber durch die Korrelation verschiedener Vorgänge untereinander Informationen erlangen kann.

Beispiel 2.26:
Angriff gegen „Anonymous Remailer“
Ein Angreifer, der herausfinden will, wer wann wem Nachrichten schickt, stößt auf Probleme, wenn er einen einfachen, kryptographisch gesicherten „Anonymous Remailer“ abhört. Die ankommenden Nachrichten verraten nicht den effektiven Empfänger, die abgehenden nicht den Absender. Da der Remailer eine Neuverschlüsselung vornimmt, kann keine eindeutige inhaltliche Zuordnung der ankommenden und abgehenden Nachrichten vorgenommen werden.

Dennoch ist eine gewisse Zuordnung über die Korrelation der Länge und der Übertragungszeitpunkte von Nachrichten möglich.

Stärkere Remailer halten die Nachrichten daher über eine zufällige Latenzzeit und sorgen für eine deutliche Durchmischung der Reihenfolge ankommender und abgehender Nachrichten. Außerdem werden Nachrichten durch die zu verwendenden Verschlüsselungsprogramme mit einem „Huckepackrauschen“ versehen, das der Remailer nach Gutdünken verkleinern oder vergrößern kann, um so eine Korrelation über die Nachrichtenlänge zu erschweren.

2.5.3.10 Kosten und Reaktion der Partei

Schließlich sind auch die Kosten der Partei für die Kommunikation im Fall der befugten Übertragung und im Fall des Angriffs in Betracht zu ziehen, ebenso die Reaktion der Partei bei Erkennung eines Angriffs.

Die Verursachung der Kosten und die Provokation der Reaktion müssen als potentielles Angriffsziel berücksichtigt werden.

2.5.4 Zeitliche und räumliche Beschränkungen

Die befugten Parteien können durch Sicherungsmaßnahmen in die Lage versetzt werden etwas zu tun, was andere nicht können. Ein Angreifer könnte eine dieser Parteien erfolgreich angreifen und damit die Stelle der Partei derart einnehmen, daß der Angreifer alle Fähigkeiten der Partei übernimmt und von der befugten Partei effektiv nicht mehr unterscheidbar ist. Das hat schwerwiegende Konsequenzen für die nachfolgende Kommunikation, kann aber auch rückwirkend kompromittierend wirken, wenn der Angreifer Aktionen des zuvor befugten Benutzers wiederholen kann, z. B. die Entschlüsselung von Daten, die dem Angreifer nur in verschlüsselter Form vorlagen.

Besteht die Gefahr einer zukünftigen vollständigen Übernahme, können Schutzmaßnahmen, die auf einer *räumlichen* Unterscheidung zwischen der befugten Partei und dem Angreifer beruhen, keinen effektiven Schutz mehr bieten. Die Partei muß *sich selbst in der Zukunft* als Angreifer betrachten und ihre Befugnis zeitlich eingrenzen.

2.5.5 Schadenserwartung

Die Beschreibung eines Schutzobjektes muß auch eine Darstellung des erwarteten Schadens bei Durchbrechen der Sicherung beinhalten, denn der zu erwartende Schaden fließt in die Bestimmung der relativen Leistungsfähigkeit (Abschnitt 2.2.3.2) ein und wird beim Entwurf schadensbegrenzender Maßnahmen (Abschnitt 3.10), der Objektentkopplung (Abschnitt 3.10.1) und anderer Maßnahmen benötigt.

2.5.6 Schutzobjekt Sicherungsmaßnahme

Gegenstand der Betrachtung waren bisher nur Schutzobjekte, die unabhängig von den Sicherungsmaßnahmen sind. Es besteht aber die Gefahr, daß durch Sicherungsmaßnahmen *neue* Schutzobjekte entstehen, denn Sicherungsmaßnahmen sind meist keine Problemlösungen, sondern Problemverlagerungen (s. Abschnitt 4.3).

Darüberhinaus kann aber bereits die Absicherung selbst zum Schutzobjekt werden, wenn nämlich die Anforderung besteht, daß der Angreifer die Sicherung nicht bemerken darf oder ihm gegenüber das Fehlen oder die Nichtbenutzung von Sicherungsmaßnahmen vorgetäuscht werden muß. Hierzu gehören auch sog. „Stille Alarme“ und Sicherungsmethoden, die nur wirken, wenn der Angreifer sie nicht bemerkt (z. B. Angriffsnachweise), aber auch „verbotene“ Sicherungsmaßnahmen.

3 Sicherungsmethoden

3.1 Überblick

In diesem Kapitel werden verschiedene Sicherungsmethoden vorgestellt, die sich in ihren Anforderungen und in ihrer Wirkung gegen einen Angriff unterscheiden. Dabei werden mit *Methoden* die verschiedenen Wirkungsweisen bezeichnet, die einen Angriff verhindern oder erschwerden sollen, mit *Maßnahmen* konkrete technischen Ausgestaltungen von Methoden.

Tabelle 3.1 zeigt schematisch und zeitlich geordnet einen prototypischen Angriff und die (aktiven oder passiven) Aktionen des Angreifers und des Angegriffenen, sowie die jeweils in dieser Phase ansetzenden Methoden.

Bemerkung 3.1:
Methoden nach Angriffserfolg
Besondere Bedeutung kommt den Methoden zu, die *nach* dem Eintreten des Angriffserfolgs ansetzen und damit den Angriff und den Erfolg selbst nicht (mehr) verhindern können.

Diese augenscheinliche Schwäche dieser Methoden bringt jedoch den Vorteil mit sich, daß diese Methoden nicht (oder nur in wesentlich geringerem Umfang) die Gefahr der *Übersicherung* (siehe Abschnitt 4.3.3) in sich bergen. Sie sind deshalb besonders für die Einsatzbereiche geeignet, bei denen der Schaden durch eine Übersicherung höher wäre als der Schaden durch einen Angriff oder für die angriffsverhindernde Methoden wegen ihrer Nebenwirkungen oder aus anderen Gründen zu gefährlich sind.

Muß etwa zum Schutz der Vertraulichkeit im medizinischen Bereich die Gefahr einer Offenbarung von Patientendaten der Gefahr einer Nichtverfügbarkeit im Notfall durch Übersicherung gegenübergestellt werden, kann es sinnvoll sein, auf angriffsverhindernde Methoden zu verzichten oder diese nur in geringem Umfang einzusetzen.

Partei		Gegenmaßnahme	Siehe
Verteidiger	Angreifer		Abschn.
begibt sich in Gefahr		Bewertung und Auswahl	3.2
agiert unkontrolliert		Spezifikationstreue herstellen	3.3
	entscheidet sich zum Angriff	Verschlechterung Kosten/Nutzen-Verhältnis	3.4
	bereitet Angriff vor	Vorbereitung erschweren	3.5
kommuniziert beabsichtigt	kommt in Kontakt mit Schutzobjekt	Organisatorische Maßnahmen	3.6
exponiert unbeabsichtigt	kommt in Kontakt mit Schutzobjekt	Seiteneffektdämpfende Maßnahmen	3.7
	Nutzt Kontakt aus und hat Erfolg	Kryptographische Maßnahmen	3.8
	Erkennt Erfolg	Verschleiernde Maßnahmen	3.9
	richtet Schaden an	Schadensbegrenzende Maßnahmen	3.10
bemerkt Angriff nicht		Erkennung	3.11
reagiert auf Angriff nicht		Reaktion	3.12
kann Angriff nicht beweisen		Angriffsnachweis	3.11

Tabelle 3.1: Die verschiedenen Sicherungsmethoden können danach differenziert werden, in welcher Phase des Angriffs ihre Wirkung eintritt. Dabei setzen einige Maßnahmen erst *nach* Eintritt des Angriffserfolges ein.

3.2 Bewertungen und dynamische Auswahlverfahren

Die stärkste Methode zur Abwehr von Angriffen ist die Vermeidung von Situationen, in denen überhaupt erst eine Gefährdung bzw. ein Schutzbedürfnis entstehen können. Besteht die Wahl zwischen verschiedenen, unterschiedlich gefährlichen Wegen, so ist es natürlich naheliegend, den ungefährlichsten Weg zu wählen. In den Entwurf von Sicherheitsmechanismen müssen diese Überlegungen freilich einfließen.

Wenn aber die Auswahl des Weges oder die Vermeidung von Gefahrensituationen nicht

schon zur *Entwurfszeit*, sondern erst während der *Laufzeit* möglich sind, dann kann die Auswahl selbst nicht Teil des Entwurfes sein. Stattdessen müssen Bewertungs- und dynamische Auswahlverfahren, die eine Entscheidung zur Laufzeit ermöglichen, Teil des Entwurfs werden.

Zu unterscheiden ist hierbei zwischen der

a priori-Bewertung,
: die nur Kriterien verwendet, die nicht in konkretem Zusammenhang mit einem bereits erfolgten Angriff stehen, z. B. Vertrauensaspekte [77], Routing-Informationen, von der Wegewahl abhängige gesetzliche Beschränkungen, Bewertungen des Schutzobjektes usw., und der

a posteriori-Bewertung,
: in die zusätzlich Erkenntnisse über im Umfeld des Schutzobjektes bereits erkannte Angriffe mit einfließen, vornehmlich aus der Erkennung eines früheren Angriffs (Abschnitt 3.11) und den Reaktionen darauf (Abschnitt 3.12).

  Diese beiden nichtverhindernden Methoden können damit Teil der verhindernden Methoden für neue Angriffe werden.

3.3 Spezifikationstreue und Korrektheit

Die empirische Untersuchung von realen Angriffen zeigt, daß ein großer Teil der erfolgreichen Angriffe Systemlücken ausnutzt, die entstanden sind, weil das tatsächliche System von der Spezifikation abweicht (z. B. weil es verändert wurde), spezifikationswidrig verwendet wird oder schlicht fehlerhaft ist [119, 51, 128, 112, 126, 88, 106, 4].

Die Folge dessen ist, daß sich das System nicht mehr so verhält, wie es spezifiziert war, wie es der Interessenträger erwartet und wie es dem Entwurf oder der Beurteilung von Sicherheitsmechanismen zugrundegelegt wurde. Das System agiert unkontrolliert, die Bewertung des Systems zur Entwurfszeit wird damit unzutreffend und Sicherheitsmechanismen können unwirksam werden.

Eine andere Ursache für Abweichungen von der Spezifikation können die Auswirkungen eines bereits erfolgten (Vor-)Angriffs sein, in dessen Verlauf das System verändert wurde. In diesen Bereich gehören auch Veränderungen von Systemen, die sich zur Laufzeit dynamisch verändern (z. B. Programmteile oder Bibliotheken nachladen[1]).

Deshalb muß gewährleistet werden, daß das System in einem Zustand ist und bleibt, der der Spezifikation entspricht und der dem Entwurf der Sicherheitsmechanismen zugrundegelegt wurde. *Das System wird selbst zum Schutzobjekt.*

[1] Ein sehr unrühmliches Beispiel hierfür sind Betriebssysteme, bei denen es möglich oder sogar üblich ist, im Rahmen der Installation von Anwendungssoftware die Bibliotheken bzw. Programmteile anderer Anwendungsprogramme oder sogar des Betriebssystems zu verändern.

Zu unterscheiden ist hier zwischen Beeinträchtigungen des Systems aufgrund von Fehlern im System oder Fehlbedienung der befugten Partei und aufgrund von Angriffen. Erstere gehören in den Bereich der Korrektheit und Verifikation, was außerhalb des Themas dieser Arbeit liegt. Gegen Angriffe kann das System mit den gleichen Methoden geschützt werden, wie andere Schutzobjekte auch.

Beispiel 3.2:
Systemschutz durch die JAVA Virtual Machine
Die Programmiersprache JAVA und deren Laufzeitumgebung sind so entworfen, daß damit auch nicht vertrauenswürdige Programme aus dem Internet geladen und ausgeführt werden können.

Das Laden solcher Programme stellt eine dynamische Veränderung des Systems dar, die prinzipiell die Gefahr mit sich bringt, daß das System verändert wird und von der Spezifikation abweicht.

Daher sind in JAVA zwei Sicherheitsmechanismen eingebaut:

Die virtuelle Maschine stellt eine *organisatorische* Maßnahme (Abschnitt 3.6) dar.

Der „Bytecode Verifier“ ist eine *angriffserkennende* Maßnahme (Abschnitt 3.11) dar.

Beide sind in ihrer Funktion auch Maßnahmen zur Gewährleistung der Spezifikationstreue.

In diesen Bereich gehören auch die in [129] vorgestellten Sicherheitsmechanismen.

3.4 Veränderungen des Kosten/Nutzen-Verhältnisses

In der Regel ist ein Angriff für den Angreifer mit einem gewissen Aufwand verbunden, dem Angreifer entstehen Kosten in Form von Strom, Rechenzeit, Arbeitszeit etc.

Der Angreifer *kann* seinen Angriff daher nur durchführen, wenn er diesen Aufwand effektiv erbringen kann, d. h. wenn ihm die nötigen Ressourcen zur Verfügung stehen (absolute Leistungsfähigkeit).

Der Angreifer *will* seinen Angriff nur durchführen, wenn der zu erwartende Erfolg in einem für ihn günstigen Verhältnis zum Aufwand steht (relative Leistungsfähigkeit). Es kann allerdings sehr schwierig oder unmöglich sein, abzuschätzen, was der Angreifer als günstig ansieht, denn der Angreifer handelt nicht notwendigerweise rational oder macht sich darüber überhaupt Gedanken.

Eine Anhebung des Angriffsaufwandes, insbesondere eine Verschlechterung des Verhältnisses zum Nutzen des Angriffs für den Angreifer wirkt daher dem Angriff entgegen[2].

3.4.1 Anhebung der Angriffskosten

Eine Anhebung der (minimalen, maximalen oder mittleren) Angriffskosten kann sich gegen die relative und gegen die absolute Leistungsfähigkeit des Angreifers richten.

Wie die Angriffskosten tatsächlich in die Höhe getrieben werden können, hängt vom Einzelfall ab. „Klassische“ Methoden sind:

- Erhöhung der Schlüssellänge bei kryptographischen Verfahren
- Mehraugenprinzip zur Erhöhung des notwendigen Bestechungsgeldbetrages
- Einführen eines Risikos für den Angreifer, z. B. Strafandrohung, Hinterlegung von Pfand usw.
- Ressourcen für den Angreifer knapp halten, z. B. durch Exportverbote.

3.4.2 Senkung der Leistungsfähigkeit des Angreifers

Sollen die Kosten des Angriffs die Leistungsfähigkeit des Angreifers übersteigen, so kann dies auch durch Senkung der Leistungsfähigkeit des Angreifers erreicht werden, sofern ein ausreichend reales Feindbild existiert. Können die Ressourcen des Angreifers gebunden oder deren Verfügbarkeit beeinträchtigt werden, sinkt dessen Leistungsfähigkeit und die Kosten des Angriffs steigen. Erreicht werden kann dies etwa durch

Opferobjekte
: Dem Angreifer wird ein vermeintlich interessanteres Ziel geboten, das ihm lohnender als das eigentliche Ziel erscheint, und das ihn veranlaßt, seine Ressourcen anderweitig einzusetzen.

Provokation
: Dem Angreifer wird ein offenkundiges Ziel geboten, das ihn verleitet, seine Ressourcen zum Angriff zu verbrauchen und sich auszutoben.

Scheinobjekte
: Dem Angreifer wird ein scheinbares Ziel geboten, das er nicht wirklich angreifen oder aus dessen Angriff er keinen wirklichen Nutzen ziehen kann, an dem er aber seine Ressourcen verbraucht.

[2] Freilich laufen alle Methoden darauf hinaus, den Angriff zu erschweren. Hier aber liegt der Schwerpunkt auf der Verursachung von *Kosten* für den Angreifer.

Gegenangriffe
: Der Angreifer wird derart angegriffen, daß er seine Ressourcen zur Verteidigung benötigt[3].

3.4.3 Senkung des Angriffsnutzens

Ergänzend zur bisher dargestellten Vorgehensweise ist auch die Senkung des Angriffsnutzens als Sicherungsmethode möglich. Auch hier kann wieder nur im Einzelfall bestimmt werden, wie die Senkung konkret auszusehen hat.

Auch hier sind aber wieder zwei Fälle zu unterscheiden, nämlich

a priori,
: d. h. der Nutzen wird vor dem konkreten Angriff gesenkt, was eine gewisse Prognose über den Angriff voraussetzt, und

a posteriori,
: d. h. als Reaktion nachdem der Angriff erkannt wurde.

Zu den Senkungen a priori gehören auch die Schadensbegrenzung (Abschnitt 3.10), also beispielsweise auch die Beschränkung der Nutzungsdauer kryptographischer Schlüssel und die Erzeugung von Schlüsselderivaten. Ebenso gehören hierzu Senkungen des zu erwartenden *mittleren* Angriffsnutzens, etwa durch Einführung von wertlosen Pseudoobjekten, die die Trefferwahrscheinlichkeit eines Angriffes senken.

Ein Beispiel zur Senkung des Angriffsnutzens a posteriori wäre etwa, kompromittierende Informationen, deren Vertraulichkeit verletzt wurde, öffentlich preiszugeben, um diese für weitere Veröffentlichungen zu entwerten und so einer Erpressung zu entgehen.

3.5 Erschwerung der Angriffsvorbereitung

Die Betrachtung erfolgreicher Angriffe zeigt, daß ihnen in vielen Fällen eine Vorbereitung des Angreifers auf den Angriff vorausgeht. Können über die für einen Angriff notwendigen Vorbereitungsschritte hinreichend genaue Annahmen gemacht werden, so kann die Erschwerung dieser Vorbereitungsschritte andere Maßnahmen unterstützen.

Da jede Sicherungsmaßnahme letztlich auf eine Erschwerung des Angriffs hinauslaufen soll, ist eine gesonderte Betrachtung erst dann gerechtfertigt, wenn eine Differenzierung zwischen dem Angriff und der Angriffsvorbereitung möglich ist und die

[3] Anzumerken ist allerdings, daß es sich hier nicht mehr um eine reine Sicherungsmaßnahme, sondern einen Angriff des „Verteidigers“ gegen den „Angreifer“ handelt.

Vorbereitung nicht ohne weiteres als Teil des Angriffs angesehen werden kann. Eine Differenzierung ist möglich, wenn der Gegenstand der Vorbereitung der Angriff auf ein anderes Schutzobjekt ist, als es Ziel des Hauptangriffes ist.

Bemerkung 3.3:
Angriffsvorbereitung
Damit ist die Angriffsvorbereitung selbst wieder ein Angriff, der mit dem Hauptangriff nicht identisch ist, dessen Erfolg aber den Hauptangriff erleichtert.

Die Erschwerung der Angriffsvorbereitung ist daher keine einzelne Sicherungsmaßnahme, sondern der eigenständige Schutz der aus dem Hauptschutzobjekt, den gewählten Sicherungsmethoden und den bestehenden Sicherungsmechanismen abgeleiteten eigenständigen Schutzobjekte.

Auch hier ist eine genaue Bestimmung wieder nur im Einzelfall möglich. Aus der in dieser Arbeit vorgestellten Systematik zur Vorgehensweise lassen sich jedoch „kanonische“ Ziele von Vorbereitungsschritten – und damit auch neue Schutzobjekte – ableiten:

- Interessenlage und Identität des Interessenträgers
- Eigenschaften und Lage der Parteien
- Abbildung der Interessenlage auf technische Merkmale und Adressen
- Eigenschaften der Übertragung
- Identität, Wert, Lage, Eigenschaften etc. des Schutzobjektes
- Gewählte Sicherungsmethoden und -mechanismen

Neben den Schutz des eigentlichen Schutzobjektes tritt daher der Schutz der abgeleiteten Objekte.

Bemerkung 3.4:
Schwerer Fehler: „Security by Obscurity“
Ein oft zu beobachtender und sehr schwerer Fehler ist es, den Schutz des Hauptobjektes mit dem Schutz der abgeleiteten Objekte zu verwechseln oder die Sicherungsmaßnahmen sogar auf diese zu beschränken.

Für die abgeleiteten Objekte gelten grundsätzlich andere Rahmenbedingungen als für das Hauptobjekt, weshalb diese in einer getrennten System- und Bedrohungsanalyse zu betrachten sind. Insbesondere deren nach außen gerichtete Wirkung, die sie ohne Zweifel haben sollen, denn sie sollen ja gegen den Angreifer wirken, ist mit der Gewährleistung höchster Vertraulichkeit prinzipiell nicht zu vereinbaren. Der Schutz der abgeleiteten Objekte fällt daher fast immer anders und deutlich niedriger als der Schutz des Hauptobjektes aus. Oft werden die abgeleiteten Objekte nicht einmal als ernsthaft schutzbedürftig angesehen.

Die immer wieder anzutreffenden Annahmen der Art, daß ein Angriff nicht zu befürchten wäre, weil etwa der Angreifer die Netzstruktur des LANs, die IP-Adresse des Servers usw. nicht kennt, gehören zu den schwersten und verhängnisvollsten Fehlern in der System- und Kommunikationssicherheit.

Eine Steigerung erfährt dieser Fehler durch die gelegentlich zu beobachtende Fahrlässigkeit, erst gar nicht für eine klare Systemstruktur und klar definierte Sicherungsmaßnahmen zu sorgen und auf die Verwirrung des Angreifers zu hoffen, sich dabei aber auch selbst den Überblick unmöglich zu machen.

Die Vertraulichkeit der abgeleiteten Objekte gegenüber dem Angreifer zu gewährleisten kann sinnvoll sein. Die Sicherheit des Hauptobjektes darf aber nicht davon abhängig werden. Daher ist zu untersuchen, inwieweit ein erfolgreicher Angriff auf das abgeleitete Objekt das Hauptobjekt gefährdet. Insbesondere darf der Schutz des abgeleiteten Objektes nicht zu Lasten des Schutzes des Hauptobjektes gehen.

Bemerkung 3.5:
Nichttechnische Bereiche: Social Engineering
Die vorliegende Arbiet hat ausschließlich technische Sicherheit zum Gegenstand. Die Grenzen der Angriffsvorbereitung und der abgeleiteten Objekte sind aber weiter zu fassen, auch außerhalb der Technik liegende Bereiche sind in Betracht zu ziehen.

Ein besonders wichtiger Bereich ist das Umfeld der menschlichen Benutzer und befugten Parteien. Eine oft erfolgreiche Angriffstechnik ist das sogenannte „Social Engineering“, bei der der Angriff über erschlichenes Vertrauen, Sorglosigkeit, Arglosigkeit und mangelndes Sicherheitsbewußtsein auf menschlicher Ebene stattfindet (Beispiel: bestochene Sekretärin, sorgloses Personal). Auch diese Vorbereitungstätigkeiten sind zu berücksichtigen.

3.6 Organisatorische Maßnahmen

Die wichtigsten Maßnahmen sind die *organisatorischen* Maßnahmen. Der dem normalen Sprachgebrauch entnommene Begriff „organisatorisch“ beschreibt zwar schon ungefähr die Eigenschaften, eine genaue Definition ist aber notwendig:

Definition 3.6:
„organisatorisch“
Eine Sicherungsmaßnahme heißt *organisatorisch*, wenn sie den Zugriff mindestens einer unbefugten Partei (Def. 2.1) auf das Schutzobjekt auf

technischem Weg *unmittelbar* verhindert (oder erschwert), und dabei befugte und unbefugte Parteien technisch durch Merkmale – also Adressen (Def. 2.4) – unterschieden werden.

Bemerkung 3.7:
Organisatorische Maßnahmen und Partitionen
Eine organisatorische Maßnahme setzt voraus, daß eine entsprechende Partition (Def. 2.3) der Parteien besteht und passende (Def. 2.5) Adressen existieren.

Sie ist umgekehrt genau das technische Mittel, das entsprechend einer Partition Befugnisse in Befähigungen umsetzt.

Organisatorische Maßnahmen zielen darauf ab, die beabsichtigten, spezifizierten Kommunikationswege so zu legen, daß ein potentieller Angreifer nicht in Kontakt mit dem Schutzobjekt, also den zu schützenden Daten oder Rechnern, kommen kann, und die tatsächlichen Kommunikationswege möglichst auf die spezifizierten Wege einzuschränken.

Bemerkung 3.8:
Position im Angreifermodell
Eine organisatorische Sicherungsmaßnahme wirkt, indem sie den Angreifer vom Kontakt mit dem Schutzobjekt abhält.

Die fundamentale Eigenschaft organisatorischer Sicherungsmaßnahmen ist es daher, den Angreifer in der Position 1 (vgl. Abbildung 2.4 auf Seite 49) *zu halten* oder ihn durch Ausgestaltung der Kommunikationswege und -einrichtung in diese Position *zu bringen*.

Von besonderer Bedeutung ist hier die Auswahl des Transportweges, die oftmals aufgrund von Adreßinformationen und bestimmten Regeln ausgewählt wird.

Nicht nur die übertragene Information, sondern auch Adressen und Regeln zur Wegewahl selbst müssen daher Objekt von Sicherungsmaßnahmen sein.

Beispiel 3.9:
Paketfilter
Im Internet werden Router nicht nur dazu verwendet, den Transport überhaupt zu ermöglichen, sondern oft auch als Paketfilter, der anhand gewisser Regeln entscheidet, ob Pakete transportiert werden, und so organisatorische Sicherheit bietet.

Ursprünglich gehört das Filtern von Paketen zum Zwecke der Systemsicherheit aber nicht zur Spezifikation von Routern, deren eigentliche Aufgabe nur ist, Datenpakete in Richtung des Empfängers zu transportieren. Es hat daher Router gegeben, die bei hoher Last wegen geringer eigener

Rechenleistung nicht mehr in der Lage waren, den normalen Betrieb zu erhalten. Für diesen Fall haben die Router zum Notbetrieb „auf Durchzug“ geschaltet und unbesehen jedes Paket durchgereicht. Dies kann im Rahmen ihrer tatsächlichen Spezifikation (nämlich Netzwerkfunktion, nicht Security) durchaus als zulässig angesehen werden. Erst die Zweckentfremdung als Sicherheitselement hat die Spezifikation verschoben und damit zu spezifikationswidrigem Verhalten geführt und die Sicherheit beeinträchtigt.

Beispiel 3.10:
Zusammenbruch einer organisatorischen Sicherung
Manche Router verwenden auch ein „dynamisches“ Routing, was bedeutet, daß die Auswahlregeln nicht starr und langfristig programmiert sind, sondern im laufenden Betrieb ständig und automatisch geändert werden können. Diese Technik soll helfen, Fehler in der Programmierung zu vermeiden und die Arbeit häufigen Umprogrammierens zu sparen.

Es sind aber auch Fälle vorgekommen, in denen Router Regeländerungen von außen angenommen haben, die zu schwerwiegenden Fehlern in der Wegeauswahl führten. In ungünstigen Fällen können gleich mehrere Router davon betroffen sein und Daten, die eigentlich nur über einige hundert Meter transportiert werden sollten, in andere Kontinente leiten.

3.6.1 Ausgewählte Beispiele für organisatorische Sicherungsmaßnahmen

3.6.1.1 Firewalls

Ein allgemein sehr bekanntes und weit verbreitetes Beispiel für eine organisatorische Sicherungsmaßnahme ist die „Firewall“, mit der Netzwerksegmente voneinander getrennt werden und so eine der Netztopologie entsprechende Parteienpartition erzeugt wird. Eine Firewall ist eine Netzwerkkomponente (normalerweise in der Größenordnung und Funktion zwischen Router und Workstation), die anhand der Konfiguration und der gewählten Regelwerke Kommunikationsverbindungen zulässt oder sperrt. Genaueres zu Firewall-Rechnern ist in [121] zu finden.

Die Firewall ist ein technisches Mittel zur Trennung verschiedener Netzwerksegmente und damit ideal zur Zonentrennung.

3.6.1.2 Zugriffsrechte

Eine vornehmlich im Betriebssystembereich anzutreffende organisatorische Maßnahme, bei der die Beschreibung der Zugriffsrechte zum Teil sogar selbst als Adresse

verwendet wird, sind die Zugriffsberechtigungen, wie sie etwa bei VMS oder in den Ausprägungen von Unix anzutreffen sind. Auch hier werden Partitionen über den Benutzern erzeugt und diesen Partitionen gewisse Rechte zugewiesen, die als unmittelbares Unterscheidungsmerkmal dienen, ob ein Zugriff ermöglicht wird oder nicht.

3.6.1.3 Mehrschichtensicherung

Wie in Abschnitt 4.1.2 beschrieben wird, kann es notwendig sein, mehrere Sicherungen auf unterschiedlichen Schichten vorzunehmen, z. B. eine Doppelsicherung wie in Abbildung 4.2 auf Seite 102. Damit wird eine *Dreiteilung* der Parteien vorgenommen, nämlich in den außen stehenden Angreifer, die an der Übertragung beteiligten Einrichtungen und den Endempfänger der Nachricht.

3.6.1.4 Krypto-Chipkarte

Zweck von kryptographischen „Tokens“ wie Chipkarten u. ä. ist die organisatorische Sicherung des kryptographischen Schlüssels. Das technisch greifbare Merkmal der Parteien ist hierbei, ob sie zum Schaltwerk des enthaltenen Chips gehören oder nicht. Es gibt also eine Zweiteilung zwischen „innen“ und „außen“.

3.6.1.5 Virtuelle Elemente und Umgebungen

Ein weiteres Beispiel sind die virtuellen Elemente und Umgebungen, die oft eingeführt werden, um eine organisatorische Trennung in Form eines Programms zwischen reale Elemente und unbefugte Parteien zu bringen. Hierzu gehören u. a. auch Postscript-Interpreter, die JAVA Virtual Machine, aber auch Unix-Gerätetreiber und bessere Betriebssysteme.

3.6.2 Sicherung der Sekundärinformationen

Eine organisatorische Sicherung ist dann nicht mehr unmittelbar möglich, wenn die Position des Angreifers nicht klar von der Position befugter Empfänger zu trennen ist. Dieses Problem tritt auch beim Schutz der Sekundärinformationen bzw. der Nutzlasten auf, weil diese nicht in beliebiger Weise geschützt werden können. Sie sind für die Funktion der Transportmechanismen notwendig und müssen deshalb für diese auch greifbar sein (z. B. IP-Adressen, URLs, Telefonnummern, E-Mail-Adressen). Würde man diese Information in der gleichen Weise wie die Primärinformation schützen, könnte der technische Transport nicht mehr funktionieren oder nur noch dann, wenn jede Transporteinrichtung ihrerseits als befugter Sender und Empfänger behandelt würde, was mit zu hohem Aufwand verbunden ist.

3.6.2.1 Verlagerung in höhere Schichten

Jedem Transportmedium haftet eine Abstraktionsebene an, die durch die Trennung zwischen Hilfs- und Nutzlasten indiziert wird. Während die Hilfslasten unterhalb dieser Trennebene für die Transporteinrichtungen auch dann zugänglich sein müssen, wenn die Einrichtungen nicht selbst als befugte Partei angesehen werden, kann die Vertraulichkeit der Nutzlasten (also die Primärinformation und die Sekundärinformationen der höheren Schichten) geschützt werden.

Das eröffnet die Möglichkeit, Sekundärinformationen durch Verlagerung in eine höhere Schicht anderen nicht unmittelbar anwendbaren – vornehmlich kryptographischen – Methoden zugänglich zu machen. Daraus ergeben sich freilich zwei Konsequenzen:

- Weil in den Transportmechanismus nicht eingegriffen werden soll, müssen an die Stelle der nach oben verlagerten Sekundärinformationen andere treten, die die geschützen Informationen nicht kompromittieren können.
- Auch die Verlagerung ändert nichts daran, daß die geschützten Informationen letztlich irgendwann Verwendung in ihrer eigentlichen Schicht finden müssen; anderenfalls wären sie überflüssig. Es muß daher mindestens eine Transporteinrichtung geben, die diese Informationen empfangen kann, und deshalb auch als befugte Partei in Erscheinung treten muß.

Diese befugte Transporteinrichtung muß dann auch dafür sorgen, daß die Sekundärinformationen „nach Durchquerung von Feindesland“ wieder auf die zugehörige Schicht gebracht werden.

Beispiel 3.11:
Verlagerung der Sekundärinformationen in höhere Schichten
Bei der Benutzung eines Telefons werden normalerweise die gewählten Telefonnummern registriert. Um die Registrierung der Telefonnummer oder eines Teils der Telefonnummer zu vermeiden, muß die Wahl in eine höhere Schicht verlagert werden, also erst *nach Zustandekommen einer Verbindung* akustisch übertragen werden, also beispielsweise die weitere Vermittlung durch eine Telefonzentrale oder durch einen Callback- oder Callthrough-Anbieter, an den die gewünschte Telefonnummer akustisch übertragen wird.

Eine ähnliche Wirkung kann durch sog. „IP-Tunnel“ erzielt werden, bei denen der gesamte Verkehr zwischen zwei Teilnetzen ab Schicht 3 komplett verschlüsselt und in eine Verbindung mit konstanten Sekundärinformationen „eingewickelt“ wird.

3.6.2.2 Sender/Empfänger-Entkopplung

Eine Erweiterung der Schichtenverlagerung ist möglich, wenn mit der Rückverlagerung der verschobenen Sekundärinformationen gleichzeitig alle Absenderangaben entfernt oder ihrerseits nach oben verschoben werden und die damit befaßte Kommunikationseinrichtung selbst an die Stelle des Absenders tritt.

Damit gibt es zu keinem Zeitpunkt mehr eine Kommunikationsverbindung, die als Hilfslast der entsprechenden Schicht sowohl die effektive Absender-, als auch die effektive Empfängeradresse trägt. Gleichzeitig ist das Verbergen der Absenderadresse vor dem Empfänger möglich.

Beispiel 3.12:
Sender/Empfänger-Entkopplung
Eine solche Entkopplung wird beispielsweise durch „Anonymous Remailer“ und Proxy-Server realisiert.

Benutzer eines WWW-Proxies können so ihre wahre Identität bzw. IP-Adresse etc. vor den Servern der abgerufenen Seiten verbergen. Der Proxy hält (bei richtiger Konfiguration) diese Informationen zurück.

3.6.2.3 Bindung an andere Schichten

Ist die Echtheit der Adreßinformationen zu gewährleisten, kann in Abweichung vom Abstraktionsprinzip der Schichtenmodelle eine schichtübergreifende Bindung hergestellt werden, wenn die Authentizität auf anderen Schichten sichergestellt werden kann *und die durch die Adressen implizierten Partitionen* übereinstimmen oder wenigstens in vorteilhafter Weise ähnlich sind. Die Bindung muß dabei nicht unmittelbar erfolgen, sondern kann auch aus mehreren Bindungen über verschiedene Schichten hinweg erfolgen (z. B. physikalisch → Netzwerkadresse → E-Mail-Adresse).

Beispiel 3.13:
Bindung an andere Schichten
In modernen Telefonnetzen ist es möglich, dem Angerufenen die Telefonnummer des Anrufers zu übermitteln. Trotz teilweise bedenklicher Sicherheitslücken bei den Telefongesellschaften kann dieser Übermittlung ein gewisses Maß an Sicherheit zugebilligt werden. Eine stärkere Methode, die Telefonnummer der Gegenseite sicherzustellen ist der Rückruf.

An diese Telefonnummer können nun die Adreßinformationen der anderen Schichten gebunden werden, z. B. IP-Adressen, Domainnamen (indirekt über IP-Adressen) etc.

Beispiel 3.14:
Bindung an physikalische Adressen
Die in der Praxis wichtigste Bindung ist die Bindung von Schicht-3 (Netzwerk-)Adressen an Schicht-1-Adressen, was normalerweise die Auswahl des physikalischen Mediums ist. Die Auswahl des physikalischen Mediums erlaubt bei geeigneter Netzwerktopologie die Wahl des Netzwerksegmentes. Ein Firewall-System, das mit mehreren Zonen verbunden ist, kann zunächst nur anhand des Netzwerkadapters entscheiden, aus welchem Segment ein Datenpaket stammt. Wird durch Filterregeln sichergestellt, daß Pakete nur aus dem Segment kommen können, dem ihre Absenderadresse zugeordnet ist („Anti-Spoofing“) und wird durch statische Routing-Tabellen gewährleistet, daß Pakete nur an das Segment ausgeliefert werden, dem die Empfängeradresse zugeordnet ist, ist eine Bindung der Schicht-3-Adressen (z. B. IP) an die physikalischen Segmente erreicht und die Zonenintegrität auch auf Netzwerkadreßebene sichergestellt.

Da normalen Anwendungsprogrammen normalerweise nur die Absender- und Empfängernetzwerkadressen, nicht aber die physikalischen Adressen (Netzwerkadapter) ersichtlich sind, können so nun auch Adressen anderer Schichten aus den Anwendungsprogrammen heraus indirekt an die physikalischen Zonen gebunden werden. Naheliegende Beispiele sind die Zugriffsrechte in WWW-Servern oder Ersetzungsregeln in E-Mail-Relays. *Zonenintegrität*

3.7 Seiteneffektdämpfende Maßnahmen

In realen Systemen werden Information nicht immer nur auf den beabsichtigten, spezifizierten Wegen übertragen. In vielen Fällen gibt es versteckte, aus den verschiedensten Gründen nicht ohne weiteres erkennbare oder vermeidbare „Informationslecks“ durch unbeabsichtigte Seiteneffekte.

Ziel von Sicherungsmaßnahmen muß es daher sein, diese Effekte möglichst zu vermeiden und damit unspezifizierten Kontakt eines potentiellen Angreifers mit dem Schutzobjekt zu unterbinden.

Beispiel 3.15:
Kompromittierende Abstrahlung
Rechner von der Chipkarte bis zum Großrechner benötigen Energie und Zeit. Anhand des Verbrauches, der Schwankungen und der Energieabstrahlungen sind Rückschlüsse auf Rechenvorgänge und Daten möglich.

Daher kann es notwendig sein, Rechner so von der Außenwelt abzuschirmen und Software so auszulegen, daß der Ressourcenverbrauch keine Rückschlüsse auf den Programmzustand zuläßt.

Auch auf den höheren Schichten sind Seiteneffekte zu finden:

Beispiel 3.16:
Software mit Seiteneffekten

Verschiedene Programme müssen mit sicherheitsrelevanten Informationen umgehen, beispielsweise Zugangspaßwörtern. Dabei kann es auch bei sorgfältig geschriebenen Programmen vorkommen, daß diese Informationen offenbart werden, wenn etwa das Betriebssystem den Prozeß kurzfristig auf Platte auslagert und die Platten danach nicht vollständig gelöscht werden. Dann ist das Geheimnis auf der Festplatte zu finden.

Ähnliches kann mit dem `/proc`-Filesystem von Linux passieren: Der gesamte Hauptspeicher wird für `root` als normale Datei zur Verfügung gestellt. Läuft ein Backup während ein Programm sicherheitsrelevante Informationen – wie Paßwörter – im Hauptspeicher hält, so landen diese Informationen unbeabsichtigt und im Klartext auf dem Band.

Bemerkung 3.17:
Verhältnis zur Spezifikationstreue und Eingrenzung

Es besteht eine gewisse Ähnlichkeit zwischen den Maßnahmen zur Dämpfung der Seiteneffekte und zur Sicherstellung der Spezifikationstreue (Abschnitt 3.3). Beide richten sich gegen unerwünschtes Verhalten des Systems.

Die Maßnahmen zur Sicherstellung der Spezifikationstreue richten sich aber gegen *fehlerhaftes* Verhalten des Systems und seiner Sicherheitsmechanismen, gehören also vornehmlich zum Themenkreis der *Korrektheit*.

Die Dämpfung von Seiteneffekten soll unerwünschte Eigenschaften des Systems verhindern, die *nicht spezifikationswidrig* sind, weil entweder unsichere Eigenschaften nicht gegen eine Spezifikation verstoßen, die nicht auf Sicherheit ausgelegt ist, oder das System außerhalb der Spezifikation betrieben wird. Beides ist kein Fehler des System im Sinne von Unkorrektheit.

Eigenschaften eines Systems außerhalb seiner Spezifikation zu fordern ist jedoch prinzipiell nicht möglich, weil dies dem Begriff der Spezifikation widerspricht. Sobald man Eigenschaften fordert, hat man sie spezifiziert.

Ansatzstelle für seiteneffektdämpfende Maßnahmen muß daher die Erweiterung der Spezifikation des Systems sein. Sie gehören damit enger zum Problemkreis der Sicherheit (vgl. Def. 1.3).

3.8 Kryptographische Maßnahmen

Aufgrund der Vielfalt kryptographischer Verfahren wird nachfolgend nicht nur von der einzelnen Methode „kryptographisch“ und den darauf basierenden Maßnahmen ge-

sprochen, sondern von der Oberklasse „kryptographisch“ und den kryptographischen Methoden als Unterteilung dieser Oberklasse.

Definition 3.18:
„kryptographisch“
Eine Sicherungsmaßnahme heißt *kryptographisch*, wenn sie über den Parteien eine Partition erzeugt, indem sich die Parteien der Partition entsprechend durch die Kenntnis eines technisch greifbaren Geheimnisses unterscheiden. (Siehe aber auch Definitionen 1.8 und 1.10.)

Kryptographische Maßnahmen sollen erreichen, daß ein Angreifer keinen Nutzen aus einem Kontakt mit dem Schutzobjekt ziehen kann. Kryptographische Maßnahmen basieren darauf, daß der, der ein Geheimnis kennt, etwas tun kann, was ein anderer nur sehr schwer oder gar nicht kann, etwa eine verschlüsselte Nachricht entschlüsseln oder Daten signieren.

Bemerkung 3.19:
Schutzobjekt Geheimnis
Kryptographische Methoden stellen stets eine Problemverlagerung auf das Schutzobjekt Geheimnis dar. Daher ist bei ihrer Anwendung grundsätzlich das Geheimnis als neues Schutzobjekt zu berücksichtigen.

Bemerkung 3.20:
Verhältnis zu organisatorischen Maßnahmen
Wie aus Definition 3.18 hervorgeht, besitzen kryptographische Maßnahmen selbst keine angriffsverhindernde Wirkung. Sie erzeugen lediglich eine Partition, d. h. sie machen Parteien technisch unterscheidbar.

Erst die Kombination mit einer organisatorischen Maßnahme – auch wenn diese dabei trivial ausfallen kann – erbringt die eigentliche Schutzwirkung. So kann etwa durch eine Signatur die Authentizität einer Nachricht bewiesen werden, weil sich der Autor durch die Kenntnis des Geheimnisses vom Angreifer unterscheidet. Die Sicherungswirkung tritt aber erst dann ein, wenn das System zwischen Nachrichten mit passender Signatur und anderen Nachrichten effektiv unterscheidet, Nachrichten ohne passende Signatur etwa zurückgewiesen werden o. ä.

Auch wenn diese organisatorische Maßnahme oft trivial erscheinen mag, so ist sie mindestens so wichtig wie die kryptographische. Welche wichtige Rolle dieser begleitenden organisatorischen Maßnahme zukommt, wird etwa dann deutlich, wenn ihr Wegfall gezielt ausgenutzt wird (siehe Abschnitt 5.6.3.4).

Das erscheint zunächst widersprüchlich, denn einerseits sind sie nicht angriffsverhindernd oder organisatorisch, weil der Angreifer Kontakt zum Schutzobjekt hat. Andererseits kann er den Kontakt nicht ausnutzen und wird technisch von den befugten

Parteien unterschieden, womit doch wieder eine angriffsverhindernde organisatorische Sicherung vorliegt.

Dieser Widerspruch besteht aber nur scheinbar, weil hier tatsächlich unterschiedliche Schutzobjekte betrachtet werden. Der Angreifer erhält bei kryptographischer Absicherung zwar Zugriff auf das Übertragungsmedium und die übertragenen Daten, aber nur aus territorialer Sicht und im Schichtenmodell auf der Schicht der jeweiligen Übertragung. Von der Interpretation der Daten durch die höheren Schichten bleibt er ausgeschlossen. Damit liegt also eine schichtenspezifische Sicherung vor.

Unterhalb dieser Trennungsebene hat der Angreifer Zugriff auf das Schutzobjekt, es liegt also keine sichernde oder gar angriffsverhindernde Wirkung vor.

Oberhalb dieser Trennungsebene wird der Angreifer von der befugten Partei unterschieden und der Angriff verhindert, es liegt also offensichtlich eine organisatorische Sicherung vor. Diese beruht aber nicht auf der kryptographischen Maßnahme, weil diese nur das Erkennungsmerkmal liefert, sondern auf der (nicht immer leicht zu erkennenden) „angeflanschten“ organisatorischen Maßnahme, wie in Bemerkung 3.20 erläutert wurde. Es besteht also kein Widerspruch.

3.9 Verschleiernde Maßnahmen

In den meisten Fällen wird es ein wesentlicher Bestandteil des erfolgreichen Angriffs sein, daß der Angreifer bemerkt, daß und wann er den Erfolg erzielt hat. Ein besonders typisches Beispiel hierfür ist die vollständige Suche im Schlüsselraum beim Angriff gegen eine kryptographische Sicherung.

Die Erschwerung der Erfolgsdetektion kann daher ebenfalls einem Angriff entgegenwirken, unter Umständen kann in der Erkennbarkeit des Angriffserfolges ein eigenständiges Schutzobjekt gesehen werden.

Definition 3.21:
„verschleiernd“
Eine Sicherungsmaßnahme heißt *verschleiernd*, wenn sie dem Angreifer die Erkennung eines Angriffserfolges erschwert.

Verschleiernde Maßnahmen sind nicht notwendigerweise „vollwertige“ Sicherungsmaßnahmen, sondern können auch eine leichte Erhöhung der Sicherheit mit geringem Aufwand erlauben, also „billig“ sein. Sie werden zur Unterstützung anderer Maßnahmen eingesetzt. In Abschnitt 5.4 werden Beispiele hierzu erläutert.

Verschleiernde Maßnahmen zielen in der Regel darauf ab, den Aufwand des Angreifers zu erhöhen. Meist steigt der Aufwand dabei nur um einen konstanten Wert oder höchstens linear. Er fällt damit also aus der Gesamtbetrachtung des Aufwandes (z. B. im O-Kalkül) fast immer ganz heraus und ist damit aus berechenbarkeitstheoretischer

Sicht unbeachtlich. Dennoch aber können solche Maßnahmen einen Angriff erheblich erschweren oder abwehren, etwa wenn sie den Aufwand für den Angreifer so hoch treiben, daß der Angriff praktisch nicht mehr durchführbar ist oder die Kosten höher als der Nutzen sind und der Angriff unrentabel wird. Auch ein berechenbarkeitstheoretisch unbeachtlicher Aufwand kann finanziell beachtlich sein.

3.9.1 Beispiele

Datenkompression

Das wichtigste Merkmal, an dem ein Angreifer den Erfolg eines Angriffes auf ein Chiffrat erkennen kann, ist die in der Nachricht enthaltene Redundanz, die der Angreifer mit einem Erwartungswert vergleicht.

Ein wichtiges Werkzeug zur Verschleierung ist daher die Datenkompression, d. h. die bestmögliche Entfernung aller Redundanz.

Tarnung

Das Gegenstück zur Kompression ist die *Tarnung*, d. h. das Hinzufügen von falscher Redundanz, die eine Nachricht als etwas anderes erscheinen lassen, als sie tatsächlich ist. Hierzu gehören auch die steganographischen Maßnahmen.

Nivellierung der Sicherungsmechanismen

Nicht nur die Redundanz der Nachricht ist ein Anhaltspunkt für die Erfolgsdetektion, auch eine durch Sicherungsmechanismen eingeschleppte Redundanz bzw. eine darin enthaltener versteckter Kanal, durch den Informationen durchscheinen, erlaubt die Angriffsdetektion.

Wichtigstes Beispiel hierfür sind Verschlüsselungen mit im Vergleich zur Nachricht kurzem Schlüssel. Ist ein Chiffrat n Bit lang und hat der Schlüssel nur eine Länge von $s < n$ Bit, dann können höchstens 2^s aller 2^n möglichen Nachrichten $\{0,1\}^n$ ein Klartext zu diesem Chiffrat sein. Damit können nicht nur sehr viele Nachrichten als Klartext ausgeschlossen werden, sondern bei genügender Redundanz (also bei Erreichen der sog. Unizitätslänge) wird die Wahrscheinlichkeit, daß von allen der 2^n Nachrichten mit dieser Redundanz nur noch eine in der Teilmenge der 2^s möglichen Klartexte liegt, so hoch, daß der Klartext identifiziert werden kann. Dies kann durch Nivellierung der Sicherungsmechanismen verhindert werden.

Das Verfahren *„One Time Pad“* gilt als nicht zu brechen. Seine Sicherheit beruht aber nicht darauf, daß der Schlüssel nicht gebrochen werden könnte, denn eine vollständige Suche ist auch hier möglich, sondern darauf, daß die Erfolgsdetektion unmöglich ist.

„Schlüssellose“ Chiffren

Angriffe gegen kryptographische Sicherungen werden oft nur gegen einen kleinen Abschnitt einer Nachricht durchgeführt, beispielsweise wenn mit speziell für diese Angriffsart entworfenen Integrierten Schaltungen schnelle vollständige

Suchen unternommen werden. Die Erfolgsdetektion könnte dabei derart verlaufen, daß mit jedem getesteten Schlüssel nur eine Blockbreite entschlüsselt und mit einem „Known Plaintext“ verglichen wird (siehe auch [135, 138, 34]).

Werden jedoch Maßnahmen getroffen, die keine zusätzliche Schlüsselentropie einführen, aber die teilweise Entschlüsselung verhindern, weil immer die gesamte Nachricht komplett entschlüsselt werden muß (siehe Abschnitt 5.4.2, „Schlüssellose Chiffren“), dann kann die vollständige Suche nicht mehr mit einfachen Vergleichsregistern durchgeführt werden. Stattdessen muß für jeden Versuch die gesamte Nachricht betrachtet werden, was bedeutet, daß jeder an der Parallelverarbeitung beteiligte Rechner über genügend Speicher verfügen muß. Ein solcher Angriff ist z. B. nicht mehr mit einfachen und preiswerten FPGAs zu bewerkstelligen. Dies wird in Abschnitt 5.4.2 genauer erläutert.

Überflutung des Angreifers

„Der beste Platz um eine Nadel zu verstecken, ist nicht der Heuhaufen, sondern der Nadelhaufen.“

Eine aktive Form der Verschleierung ist die Überflutung des Angreifers mit dem Schutzobjekt ähnlichen – aber für Angreifer nutzlosen und damit für den Verteidiger risikolosen – Objekten.

Die Wirkung verschleiernder Maßnahmen hängt freilich nachhaltig von der Art des Angriffs ab:

Bemerkung 3.22:
Schutz gegen absichtslose Angriffe
Durch die Erschwerung der Erfolgsdetektion wirken verschleiernde Maßnahmen gut gegen Angriffe, in deren Erfolgsdetektion nur wenig Energie gesteckt wird oder die erst gar nicht mit einer klaren Vorstellung des Angreifers über den Erfolg betrieben werden.

Hierzu gehören insbesondere absichtslose und unsystematische Angriffe (z. B. ungezieltes und willkürliches Abhören von Kommunikationseinrichtungen) und Zufallsfunde („Gelegenheit macht Diebe“).

3.10 Schadensbegrenzung

Der Nutzen für den Angreifer und der Schaden für den Verteidiger, die durch einen erfolgreichen Angriff entstehen, können, sie müssen aber nicht gleich bzw. von gleichem Umfang sein. Unabhängig von der Senkung des Angriffsnutzen (vgl. Abschnitt 3.4) ist daher der mittlere oder maximale Schaden für den Verteidiger zu begrenzen.

3.10.1 Entkopplung der Schutzobjekte

Die wichtigste Maßnahme zur Schadensbegrenzung ist die Begrenzung eines Angriffserfolges auf möglichst wenige Schutzobjekte, also zu verhindern, daß mit einem Angriff viele Objekte beeinträchtigt werden können.

Man kann dies erreichen, indem man die Schutzobjekte geeignet aufgeteilt und eine dieser Aufteilung entsprechende Parteienpartition vorgenommen und durch Sicherungsmaßnahmen durchgesetzt wird.

Hierzu gehört auch, daß

- für Signaturen und für Verschlüsselungen,
- für zeitliche und für räumliche Übertragungen,
- für unterschiedliche Schutzzwecke (Vertraulichkeit usw.) oder
- für thematisch unterschiedliche Objekte (z. B. privat und beruflich)

jeweils unterschiedliche Schlüssel verwendet werden.

3.10.2 Entkopplung der Mechanismen

Werden zur Sicherung eines Systems verschiedene Maßnahmen oder Mechanismen eingesetzt, ist zu untersuchen, inwiefern die Sicherheit eines Mechanismus von der anderer abhängt und ob das Durchbrechen oder Umgehen eines Mechanismus dem Angreifer Vorteile für den Angriff gegen einen anderen bringt.

Beispiel 3.23:
Ungenügende Mechanismenentkopplung
Das folgende Szenario zeigt eine schlechte Mechanismenentkopplung:

Aus ein- und demselben Zufallszahlengenerator werden sowohl ein Public Key-Schlüsselpaar, als auch eine Vielzahl von kurzen Schlüsseln für eine symmetrische Chiffre erzeugt, beispielsweise um eine 90-minütige Videoaufzeichnung zu verschlüsseln. Wegen der benötigten Geschwindigkeit und gesetzlicher Schranken dürfen nur kurze Schlüssel von 40 Bit verwendet werden. Damit die Aufzeichnung nicht zu leicht zu brechen ist, wird für jede Sekunde ein neuer Schlüssel erzeugt. Gelingt es nun einem Angreifer, doch alle kurzen Schlüssel zu brechen, erhält er damit $90 \cdot 60 \cdot 40 = 216.000$ Bit Information über den Zufallszahlengenerator. Die Rekonstruktion des Zufallszahlengenerators und die Rekonstruktion der für das Public Key-Schlüsselpaar erzeugten Zufallszahlen kann mit einem sehr viel niedrigeren Aufwand verbunden sein als der direkte Angriff des Schlüsselpaars.

Hier wären zwei unabhängige Zufallszahlengeneratoren einzusetzen.

3.11 Angriffserkennung und -nachweis

Gefährlicher als der Angriff ist der vom Verteidiger unbemerkte (erfolgreiche oder erfolglose) Angriff. Der Verteidiger muß daher auch Maßnahmen ergreifen um den Angriff zu erkennen und ihn ggf. sogar Dritten gegenüber nachweisen zu können[4].

3.11.1 Implizite Erkennung

Die implizite Angriffserkennung verwendet nur Merkmale und Eigenschaften, die nicht (oder nicht ausschließlich) zum Zweck der Sicherung erzeugt wurden, sondern die für die Funktion des Systems notwendig oder unabhängig vom System vorgegeben sind. Hierzu gehört insbesondere die *Plausibilitätprüfung*.

Bemerkung 3.24:
Plausibilitätsprüfung
Grundsätzlich sind alle Adressen, Routen und Protokolle der verwendeten Übertragungseinrichtungen auf ihre Eignung zur Plausibilitätsprüfung zu untersuchen.

Beispiel 3.25:
Erkennung von „Spamming“
Ein derzeit überhand nehmendes Problem ist das sog. „Spamming“

Da Spamming wegen seiner Lästigkeit oft zu heftigen Reaktionen der Empfänger führt und in einigen Ländern inzwischen verboten ist bzw. als rechtswidrig angesehen wird, treten die Absender nur sehr selten unter ihrer richtigen IP-Adresse auf. Oft geben sie sich über ihren eigenen Nameserver temporär unerlaubte und nicht registrierte Domainnamen wie `1234567.com`, was dazu führt, daß aus den `Received:`-Zeilen der Mail-Header nicht mehr auf einfache Weise ersichtlich ist, von wo die Nachricht kam.

Kontaktiert ein solcher Versender direkt einen Mail-Relay, der unter der Kontrolle des Interessenträgers steht, dann kann dies durch geeignete DNS-Abfragen erkannt werden. Dazu ist eine doppelte Auflösung vorzunehmen, nämlich zunächst von der IP-Adresse zum DNS-Namen und von diesem wieder zurück zu IP-Adressen. Die Ergebnisse dieser Abfrage sind dann auf Plausibilität bzw. Konsistenz zu prüfen.

[4] Z. B. für Strafanzeigen, Versicherungen usw.

3.11.2 Explizite Erkennung

Angriffserkennende Maßnahmen dienen der frühzeitigen Erkennung des Kontaktes eines Angreifers mit dem Schutzobjekt, auf deren Grundlage geeignete Reaktionen zum Schutz der Daten und Maßnahmen gegen den Angreifer eingeleitet werden können, um so weiteren Schaden zu verhindern oder bereits eingetretenen Schaden zu begrenzen oder sogar wieder zu beheben, allgemein auch um den Angriff Dritten gegenüber nachzuweisen.

Beispiel 3.26:
Angriffserkennung auf Schicht 1
In manchen Bereichen war es üblich, Telefonleitungen in druckluftgefüllten Rohren zu verlegen. Man erhoffte sich, daß ein Angreifer das Rohr beschädigen müßte um an Informationen zu gelangen, und daß man dies durch einen Abfall oder durch Schwankungen im Luftdruck erkennen kann.

Beispiel 3.27:
Angriffserkennung auf Schicht 4
Auf Firewall-Rechnern ist es üblich, sog. Wachhunde auf ungenutzten Dienstzugängen laufen zu lassen, die Kontaktversuche erkennen und protokollieren.

Die Erkennung eines Angriffs erfordert Kriterien, anhand derer Angriffe von legalen Aktionen unterschieden werden können. Das bedeutet, daß einer Aktion (und auch deren Ausbleiben) eine gewisse *Redundanz* innewohnt. Ähnlich wie bei einem fehlerkorrigierenden Code gibt es eine Menge aller technisch möglichen Aktionen bzw. Nachrichten. Nur ein (geringer) Teil der möglichen Aktionen gilt als zulässig. Anders als bei der Fehlerkorrektur wird hier eine unzulässige Nachricht nicht durch die nächstliegende zulässige Nachricht ersetzt (Maximum-Likelihood-Decodierer), sondern als Angriff interpretiert.

Die notwendige Redundanz kann explizit zum Zweck der Sicherung hinzugefügt werden, sie kann aber im Einzelfall auch schon anderweitig hinzugekommen sein (Beispiel: Plausibilitätsprüfung der Pfadangaben bei E-Mail und News).

Wichtig ist, daß der Angreifer die Redundanzinformation, die die Nachricht als zulässig erscheinen läßt, nicht auf einfache oder gar triviale Art erzeugen kann. Bei einer verschlüsselten Übertragung kann ein Angreifer zwar die Daten manipulieren, es fällt aber schwer, die Daten so zu manipulieren, daß sie nach der Entschlüsselung wieder nach normalem Klartext aussehen. Natürliche Sprache ist dabei der bekanntests und einfachste Redundanzträger. Beim Fälschen einer E-Mail per SMTP [41] kann der Fälscher nicht verhindern, daß der nächste Knoten eine Kopfzeile mit der Senderadresse und damit Redundanz einfügt, die zur Plausibilitätsprüfung verwendet werden kann.

Ein Spezialfall der Angriffserkennung unter Einbezug von künstlicher Redundanz sind kryptographische Signaturen.

Die Reaktionen auf erkannte Angriffe sind allerdings mit Bedacht zu wählen, weil sich die Reaktionen auch auf erlaubte Aktionen auswirken kann. Gerade diese Auswirkung könnte aber durch einen Angriff provoziert werden, dessen Ziel es gerade ist, erkannt zu werden und damit Reaktionen auszulösen. Führt dies zu einer Einschränkung der Verfügbarkeit, spricht man auch von einer *Denial-of-Service-Attacke*.

Beispiel 3.28:
Angriffserkennung am Geldautomat
Viele Geldautomaten, Mobilfunktelefone, diebstahlgeschützte Autoradios, in Telefonnetze integrierte Anrufbeantworter, „Telebanking"-Zugänge und ähnliches mehr reagieren mit einer Blockade wenn dreimal die falsche PIN eingegeben wird. Durch Eingabe dreier willkürlicher Zahlen als PIN kann man eine Blockade erreichen.

3.12 Reaktionen während und nach dem Angriff

3.12.1 Objektdestruktive Maßnahmen

Objektdestruktive Maßnahmen haben zum Ziel, sensible Schutzobjekte im Falle eines Kontaktes mit dem Angreifer zu vernichten, bevor dieser (weiteren) Nutzen aus dem Kontakt ziehen kann. Hierzu gehören auch Negativlisten, wie sie z. B. über gestohlene Kreditkarten geführt werden.

Beispiel 3.29:
Transportbehälter für Spionagematerial
Im geheimdienstlichen Umfeld sind Transportbehälter für Mikrofilme aufgetaucht, die den Eindruck erwecken, ein Schutz vor Beschädigung durch Feuer, Wasser usw. zu sein. Der Behälter besteht aus einem Stahlzylinder, an dessen einem Ende ein auffällig stabiler Deckel in Form einer geschlossenen Sechskantmutter aufgeschraubt ist. Öffnet man den Deckel, wird Säure freigesetzt oder Sprengstoff gezündet, der den Mikrofilm vernichtet (und den Angreifer gleich mit).[5]

Beispiel 3.30:
Quantenkommunikation
Man kann Information übertragen, indem man Photonen aussendet. Durch die Ausrichtung der Polarisationsebene eines Photons wird ein Bit codiert.

[5] Will man den Film normal entnehmen, muß man einen Schraubverschluß am anderen Ende des Zylinders öffnen, der so eingelassen wurde, daß er mit dem bloßen Auge nicht erkennbar ist.

Der Empfänger muß seinen Detektor dabei für jedes Photon nach vorher ausgehandelten (geheimen) Regeln ausrichten.

Ein Angreifer, der die richtige Detektorstellung nicht kennt, würde durch seine Messung mit geratener Detektorstellung das Photon beeinflussen und damit die Information vernichten.

3.12.1.1 Adaptive Maßnahmen

Adaptive Maßnahmen sind eine Sonderform der objektdestruktiven Maßnahmen (Abschn. 3.12.1). Während die Objektvernichtung auch für den Verteidiger von Nachteil sein kann, liegt der Schwerpunkt hier auf der Anpassung an die Angriffssituation und dem Ziel, das Schutzobjekt nur für den Angreifer, nicht aber für den Verteidiger zu entwerten.

Beispiel 3.31:
Angriff auf RAID-Systeme

RAID[6]-Systeme können so konfiguriert werden, daß sie den Ausfall einer Platte fehlertolerant verkraften, indem sie Daten mit einem fehlerkorrigierenden Code auf mehrere Platten verteilen[7]. Moderne Systeme sind „hot swapping"-fähig, d. h. Platten können im laufenden Betrieb ohne Funktionalitätseinbußen ersetzt werden. Sie sind auch „selbstheilend", d. h. wenn ein Defekt auftrat oder eine Platte ersetzt wurde, unternimmt das System einen vollen Lese-/Schreibzyklus, um die verlorengegangene Redundanz wieder herzustellen.

Hiergegen wäre nun folgender Angriff denkbar: Ein Angreifer entnimmt eine Platte und setzt dafür eine leere ein. Das System läuft ohne Unterbrechung weiter. Sofern die Log-Dateien des Systems nicht aktiv überprüft und Alarmmeldungen nicht beachtet werden, bleibt der Angriff unbemerkt. Sobald die Redundanz wieder hergestellt ist, ersetzt der Angreifer die zweite Platte usw. bis er einen Plattensatz mit der vollen Entropie hat. Er hat damit unbemerkt eine Kopie des Plattensatzes gezogen.

Eine mögliche Abwehr wäre, alle Daten vor der fehlerkorrigierenden Codierung zu verschlüsseln. Wird das Fehlen einer Platte bemerkt, wird ein neuer Schlüssel erzeugt und bei der anschließenden Redunanzregeneration eine Neuverschlüsselung aller Daten vorgenommen. So bleibt das System funktionsfähig, die nacheinander gestohlenen Platten passen jedoch nicht mehr zueinander und sind nutzlos.

Daraus ergibt sich jedoch das Grundproblem, daß nun auch der Schlüssel mit mindestens der gleichen Ausfallsicherheit abgelegt werden muß,

[6] Redundant Array of Inexpensive/Independent Disks

[7] Meistens wird hierfür allerdings nur die einfache Datenspiegelung verwendet.

mit der auch die Daten gespeichert werden, weil ein Verlust des Schlüssels durch Defekte oder Stromausfall ebenfalls den Verlust der Daten nach sich ziehen würde. Hier könnte der Schlüssel mit einem Shared-Secret-Schema auf den Platten abgelegt werden. Das Schema sollte so gewählt werden, daß genau dann, wenn genügend Platten für die volle Datenentropie verfügbar sind, auch der vollständige Schlüssel vorliegt.

Entwendete Platten offenbaren dann auch keine Teilentropie, sofern der Schwellwert nicht überschritten wird.

3.12.2 Offensive Maßnahmen

Offensive Maßnahmen sind den objektdestruktiven Maßnahmen (Abschnitt 3.12.1) ähnlich; der Unterschied besteht darin, daß die Maßnahme (vornehmlich) gegen den Angreifer gerichtet ist.

4 Bewertung von Sicherheitsmechanismen

4.1 Positionierung im Schichtenmodell

Ein sehr wichtiges und oft vernachlässigtes Kriterium ist die Position der Sicherungsmaßnahmen innerhalb einer logischen Unterteilung der Kommunikationsmechanismen. Hierzu wird üblicherweise das ISO-OSI-Schichtenmodell[1](siehe z. B. [130, 67]) herangezogen.

Der Zweck dieses Modells ist eine funktionale und abstrakte Modularisierung von Kommunikationssystemen; deren Komponenten werden nach diesem Modell in sieben Schichten eingeteilt. Die Schichten bauen aufeinander auf und folglich findet auch zwischen den Schichten eine Kommunikation statt, die aber auf zwei Arten beschränkt ist:

Vertikale Kommunikation findet innerhalb eines Rechners zwischen benachbarten Schichten statt. Eine Schicht erbringt Dienste für die nächsthöhere Schicht und nutzt entweder selbst die nächstniedrigere Schicht oder ist im Falle der Schicht 1 selbst in der Lage, Informationen physikalisch zu transportieren.

Um die Interoperabilität benachbarter Schichten zu gewährleisten werden zwischen den Schichten *Schnittstellen* definiert.

Horizontale Kommunikation findet zwischen den korrespondierenden Schichten zweier (oder mehrerer) Inkarnationen (z. B. Rechner) statt. Bei Schicht 1 findet die horizontale Kommunikation über eine reale, physikalische Verbindung statt. Bei den anderen Schichten findet die horizontale Kommunikation über eine virtuelle Verbindung statt, die von den darunterliegenden Schichten zur Verfügung gestellt wird.[2]

[1] ISO: International Standards Organization, OSI: Open Systems Interconnection

[2] Ein solcher „Stapel“ von Schichten wird zusammenfassend auch als *Stack* bezeichnet, beispielsweise werden die Teile des Betriebsystems, die Kommunikation im Internet-Protokoll ermöglichen, als *IP-Stack* bezeichnet.

Um die Interoperabilität korrespondierender Schichten zu gewährleisten werden zwischen den Schichten *Protokolle* definiert.

Bei der Kommunikation mit anderen, korrespondierenden Schichten stellt sich oftmals das Problem, eine Instanz unter vielen eindeutig zu bezeichnen, wozu ggf. *Adressen* eingeführt werden. Ebenso kann das Problem der Wegfindung auftreten, weshalb spezifische Verfahren zur Wegfindung zur Schicht gehören können („Routing“).

Dieses Schichtenmodell von 1983 ist jedoch nicht ganz unproblematisch. Einerseits ist es neuer als das hier überwiegend betrachtete Internet-Protokoll. Das Internet-Protokoll und die meisten Internet-Dienste wurden nicht nach dem OSI-Schichtenmodell entworfen und fügen sich nicht genau in dieses Modell ein. Andererseits ist es für manche Betrachtungen schon wieder etwas zu alt, denn die technischen Randbedingungen haben sich mittlerweile verändert.

Das Schichtenmodell wurde aus der Sicht der Telekommunikationstechnik entworfen, für die eine rigorose Abstrahierung der Schichten untereinander von Vorteil ist. Für die Systemsicherheit kann diese Trennung jedoch von Nachteil sein, weil die einzelnen Schichten im Allgemeinen weder Zugriff auf die Informationen anderer Schichten haben, noch auf diese ausreichenden Einfluß ausüben können.[3]

Außerdem deckt das Schichtenmodell nur die Schichten ab, die üblicherweise in Hardware bzw. durch Software für den Rechner implementiert werden. Das ist aus Sicht der Telekommunikation adäquat. Aus Sicht der Systemsicherheit spielt es aber eine große Rolle, für wen bzw. in wessen Namen und unter wessen Kontrolle kommuniziert wird. Dabei kann es sich einfach um eine natürliche Person handeln, die etwa den Rechner bedient oder die Software konfiguriert hat, aber auch um abstrakte oder juristische Personen wie eine Schlüsselbehörde, ein Notariat, einen Informationsanbieter oder ähnliches. Es handelt sich hierbei also um den Absichtsträger bzw. den Nutzer, also den Träger der Verantwortung. Wegen der Bedeutung des ? wird das Modell hierfür um eine achte Schicht erweitert.

Im Allgemeinen entzieht sich diese Schicht 8 den Mitteln, die in dieser Arbeit verwendet werden, weil man etwa auf einem Menschen Software nicht oder nur sehr schlecht[4] Hingegen sind die *Schnittstelle* zur Schicht 8 und Adressen der Schicht 8 von sehr großer Bedeutung, wie in nachfolgenden Kapiteln erläutert wird.

Sicherungsmaßnahmen können nun innerhalb einer Schicht angesiedelt werden, wenn die Maßnahmen auf Veränderungen der Funktionen einer Schicht beruhen (und damit

[3] Beispielsweise ist es von der Socket-Schnittstelle aus normalerweise nicht möglich, Informationen über das Übertragungsmedium (z. B. Ethernet- oder ISDN-Adressen) zu erhalten oder IP-Adressen nur von bestimmten Ethernetadressen zuzulassen.

[4] Das Zurufen einer Parole oder das Merken der PIN einer Scheckkarte stellen in gewisser Weise ein Abarbeiten von Software für die Maschine Mensch dar, zeigen aber schon die Schwierigkeiten dabei auf.

Schicht	Bezeichnung	Beispiel für Datenübertragung		übliche
		im Raum	in der Zeit	Position
8	Interesse	Telefonauskunft	Text schreiben	Mensch, Prinzipal
7	Anwendung	World Wide Web	Textprogramm	Anwendung
6	Darstellung	HTML	ASCII	
5	Sitzung	HTTP	Dateiformat	
4	Transport	UDP	Filesystem	Betriebs-
3	Vermittlung	IP	Gerätetreiber	System
2	Bitsicherung	Ethernet	Sektorformat	spezif. Treiber
1	Übertragung	Ethernet	Magnetplatte	und Peripherie

Tabelle 4.1: Beispiele für Belegungen des (etwas modernisierten) Schichtenmodells

i. d. R. auch Veränderungen der bestehenden Protokolle nach sich ziehen). Die Maßnahme wird dabei aber auf die konkrete Implementierung beschränkt, in die die Sicherungsmaßnahmen eingebracht werden. Beispielsweise gehören die IPSEC-Erweiterungen des Internet-Protokolls oder https zu diesen Maßnahmen.

Sie können aber auch *zwischen* zwei Schichten angesiedelt werden, also an der Schnittstelle eingefügt werden. Dies hat den Vorteil, daß bestehende Implementierungen und Protokolle normalerweise nicht geändert werden müssen, bringt aber eine gewisse Alineartität mit sich. Typisch hierfür ist, daß für die Sicherungsmaßnahme die gleiche Schnittstelle zweimal mit unterschiedlichem Geschlecht implementiert wird, also nach oben und nach unten. Damit wird eine zusätzliche Schicht im Schichtenmodell eingezogen. Zu diesen Maßnahmen gehören beispielsweise einige Programmbibliotheken, die auf der Socket-Schnittstelle aufsetzen und damit zwischen den Schichten 4 und 5 liegen.

Um die Position einer zu beurteilenden Sicherungsmaßnahme im Modell genau zu bestimmen, ist es daher notwendig, die horizontalen Kommunikationen aller Schichten darauf zu prüfen, ob sie von der Sicherung erfaßt werden.

In diesem Zusammenhang muß auch berücksichtigt werden, daß die Einteilung der Funktionen im Schichtenmodell durchaus nicht absolut ist, sondern vom Standpunkt des Betrachters abhängt, und sich die Sicherungsinteressen mit dem Blickwinkel ändern können. Wer seinen Rechner bei einem Netzwerkprovider angeschlossen hat, kann ein Interesse daran haben, die Verbindung zu seinem Provider zu sichern. Das Interesse, mit einer anderen Person per E-Mail sicher zu kommunizieren, kann davon völlig unabhängig sein. Sicherungen auf verschiedenen Schichten können also ganz unterschiedlichen Zwecken dienen, weshalb es sinnvoll und notwendig sein kann, unabhängige Sicherungen auf mehreren Schichten anzubringen (zur mehrfachen Siche-

rung vgl. Abschnitt 2.5.3).

4.1.1 Reichweite

Sicherheitsmaßnahmen können unterschiedliche Lebensdauer und Reichweite haben: Wird eine E-Mail über eine verschlüsselte ISDN-Leitung übertragen, nützt diese Sicherung nichts mehr, wenn sie danach auf einem unsicheren Ethernet-Strang weitertransportiert wird. In diesem Fall hilft zwar die Verschlüsselung der Internet-Pakete oder gar der SMTP-Verbindung, aber auch dieser Schutz geht verloren, sobald die E-Mail etwa auf einer Festplatte angekommen ist und dann dort aufbewahrt oder z. B. per UUCP, IMAP oder Fax weiterübertragen wird.

Die Lebensdauer einer Sicherung steht in direktem Zusammenhang mit der Position der Sicherung im Schichtenmodell. Je niedriger die Sicherungsmaßnahmen angesiedelt ist, desto begrenzter ist ihre Wirkung. Bei strikter Trennung der Schichten ist die Wirkung einer Sicherungsmaßnahme stets dann beendet, wenn die Position der Maßnahme durch vertikale Kommunikation erstmals überschritten wird. Beispielsweise ist die Sicherung von IP-Paketen verloren, sobald die gesicherten Daten am Zielrechner angekommen sind, weil an der Socket-Schnittstelle keine Informationen darüber verfügbar sind, wie die Daten paketiert waren und welche Signaturen die Pakete trugen.

Dieser Aspekt wird häufig übersehen, wenn Sicherungsmaßnahmen auf den unteren Schichten angesiedelt werden. Dies ist i. A. leichter und effizienter, kann aber durch „überspringen“ umgangen werden. Diese Überlegung ist nicht abwegig, denn in Netzwerken gibt es sehr häufig Relaisstationen, die – je nachdem, auf welcher Schicht sie arbeiten und ob sie zwischen Protokollen übersetzen – als Repeater, Bridge, Router, Proxy oder Gateway bezeichnet werden. Eine Sicherung auf Schicht 2 (z. B. Ethernetadressen, ISDN-Verschlüsselung) oder Schicht 1 (physikalische Trennung) kann auf höheren Schichten umgangen werden, wenn der Angreifer eine Routerfunktionalität ausnutzen kann.

Ein aufgehackter Rechner, auf dem sich ein Angreifer eine root-Shell verschafft hat, ist als Schicht-7-Proxy anzusehen. Ein verräterischer Mitarbeiter, der Firmengeheimnisse weitergibt, ist ein Schicht-8-Proxy, gegen den eine Sicherung bis zur Schicht 7 nicht hilft. Nur wenn er selbst keinen Zugriff auf die zu schützenden Daten hat, ist eine Sicherung gegeben, weil dann die Sicherung auf der Personenidentität – also auf Schicht-8-Adressen ! – beruht.

Oftmals wird die Trennung zwischen den Schichten 3 und 4 besonders betont, weil hier die Grenze zwischen paket- und verbindungsorientierten Diensten liegt.[5] Diese Grenze ist hier aber nur von geringer Bedeutung und soll deshalb nicht weiter betont werden.

[5] Auch Telefon- und ISDN-Verbindungen werden hier – obwohl eigentlich deutlich verbindungsorientiert – als Paket-Dienst angesehen, weil hier eine Fragmentierung und ein Multiplexbetrieb stattfindet. Zur Datensicherung werden Paketorientierte Protokolle wie HDLC oder X.75 eingesetzt.

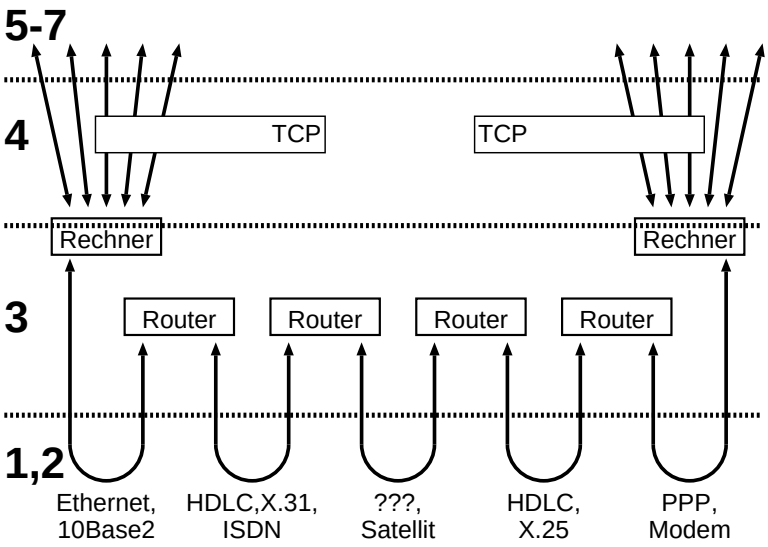


Abbildung 4.1: Der Transport von Daten im Schichtenmodell am Beispiel Internet: Eine Verbindung zwischen zwei Rechnern kann über mehrere Punkt-zu-Punkt-Verbindungen geroutet werden. Sicherungsmaßnahmen unterhalb von Schicht 3 decken daher immer nur einen Teil der Verbindung ab.

Stattdessen soll hier die Grenze zwischen den Schichten 4 und 5 herausgehoben werden, weil diese meistens mit der Schnittstelle zwischen Anwendungsprogramm und Betriebssystem zusammenfällt und deshalb auch allgemeingültig definiert ist.

4.1.1.1 Untere, übertragungsorientierte Schichten

Die Schichten 1 bis 4 werden normalerweise im Betriebssystem oder in der Peripherie des Rechners untergebracht. Sie stehen allen Anwendungsprogrammen in gleicher Weise zur Verfügung und stellen dabei die eigentliche Kommunikationsfunktionalität und den Zugriff zu (räumlichen und zeitlichen) Medien zur Verfügung. Sicherungsmaßnahmen innerhalb dieser Schichten reichen nicht weiter als bis zur Schnittstelle des Betriebssystems.

4.1.1.2 Obere, inhalts- und anwendungsorientierte Schichten

Die Schichten 5 bis 7 sind üblicherweise im Anwendungsprogramm untergebracht und in ihrer Funktion stark von der jeweiligen Anwendung abhängig, stehen aber auch unter der Kontrolle des Anwendungsprogrammes.

Im Rahmen dieser Arbeit werden keine Annahmen über die Struktur und den Aufbau von Anwendungsprogrammen gemacht und keine Anforderungen gestellt, denn die

Schicht	Orientierung	Lebensdauer	Transparenz
8	*Interesse*	*unbegrenzt*	*Parteispezifisch*
7	Inhalts-orientiert	abhängig von Laufzeit und Medien	Unter der Kontrolle des Applikationsprogramms
6			
5			
4	Übertragungs-orientiert	Socket zu Socket	Implementierungsabh.
3		Rechner zu Rechner	Nur über die Schnittstelle sichtbar, Rest unsichtbar
2		Router zu Router	
1		Hardware zu Hardware	

Tabelle 4.2: Funktionale Charakterisierung der Schichten

Sicherungsmaßnahmen sollen mit allen Anwendungsprogrammen verwendbar sein. Deshalb kann weder eine klare Trennung der Schichten im Programm vorausgesetzt werden, noch ist ein Zugriff auf einzelne der Schichten oder die beiden Schnittstellen möglich. Die Schichten 5 bis 7 werden als monolithischer Block angesehen.

Innerhalb dieses Blockes kann eine inhaltliche – syntaktische oder semantische – Interpretation der übertragenen Daten stattfinden. Auch werden vornehmlich hier Informationen zwischen verschiedenen Medien übertragen, gemischt, in ihrer Darstellung transformiert und mit der Schicht 8 ausgetauscht.

Deshalb wirken Sicherungsmaßnahmen auf dieser Ebene sehr viel länger, weil sie nicht an ein einzelnes, räumlich oder zeitlich begrenztes Medium gebunden sind sondern sich über die Lebensdauer aller verfügbaren Medien ausdehnen können. Beispielsweise bleibt der Schutz einer in den oberen Schichten verschlüsselten E-Mail auch erhalten, wenn diese E-Mail am Zielrechner angekommen und dort auf einer Festplatte gespeichert wird.

4.1.1.3 Die Schicht 8

In Abweichung von üblichen Schichtenmodellen wird hier eine zusätzliche Schicht aufgenommen, nämlich die Schicht des Interessenträgers bzw. der Partei.

Hierfür gibt es drei Gründe:

Das Modell wird dadurch *abgeschlossen*, denn die Informationsübertragung ist erst dann sinnvoll beendet, wenn die Nutzlast den Interessenträger erreicht hat. Wäre der Interessenträger nicht Teil des Modells, wäre eine vollständige Betrachtung des Informationsflußes nicht möglich oder würde erfordern, das Modell am oberen Ende wieder zu verlassen.

Das Modell wird auch *vollständig*, denn auch der Interessenträger ist selbst ein – wenn auch nicht technisches – Informationsverarbeitendes System und muß in die Sicherheitsbetrachtungen miteinbezogen werden. Eine Vielzahl von Sicherheitsproblemen

beruht darauf, daß die Schicht-8-Partei (der Mensch) selbst als „Proxy“ funktioniert und Informationen von einem sicheren System in ein unsicheres System überträgt (Überspringen), daß Vorgänge dem Menschen unsichtbar bleiben und damit seiner Kontrolle unzugänglich werden (Unterlaufen) oder daß der Mensch selbst anfällig gegen Angriffe ist (z. B. „Social Engineering“).

Das Modell erhält außerdem eine zusätzliche *Schnittstelle*, nämlich die Schnittstelle zur Schicht 8, die die Mensch-Maschine-Schnittstelle darstellt und in die Sicherheitsbetrachtungen genauso einbezogen werden muß, wie die Schnittstellen zwischen den anderen Schichten auch.

4.1.2 Schutz der Primär- und Sekundärinformationen

Bei den Betrachtungen zum Schutz von Primär- und Sekundärinformationen wird zwischen *kurzfristiger* und *langfristiger* Wirkung unterschieden. Kurzfristig bedeutet dabei, daß die Sicherungswirkung auf die Dauer (bzw. bei räumlicher Übertragung auf die räumliche Ausdehnung) der übertragungsbedingten Verbindung zwischen Primär- und Sekundärinformation – Nutz- und Hilfslast – beschränkt ist. Langfristig bedeutet, daß die Sicherungswirkung davon unabhängig ist.

4.1.2.1 Langfristiger Schutz der Primärinformationen

Je höher eine Sicherungsmaßnahme im Schichtenmodell angeordnet ist, desto langfristiger ist einerseits ihre Wirkung (vgl. Abb. 4.1), die so auf den obersten Schichten sogar vom Übertragungsvorgang abstrahiert werden kann, desto geringer ist andererseits aber auch ihre Ausdehnung auf Sekundärinformationen.

Eine „hohe“ Absicherung zur Gewährleistung von Integrität und Authentizität kann u. U. sehr teuer werden, da vor einer Angriffserkennung jeweils der gesamte Stack[6] durchlaufen werden muß. Bezieht sich eine Signatur auf ein Schicht-7-Paket von erheblicher Größe (E-Mail, Web-Seite usw.), so muß erst das gesamte Paket gelesen und verarbeitet werden, bevor der Angriff erkannt werden kann. Die Erbringung des Aufwandes zur Abarbeitung der Schichten unterhalb der Sicherung kann Angriffsziel sein.

Durch die größere Ausdehnung der Sicherungswirkung können aber auch die Kosten „pro Byte“ im Mittel niedriger liegen.

4.1.2.2 Kurzfristiger Schutz der Primär- und Sekundärinformationen

Die Alternative zur „hohen“ Absicherung ist die Plazierung auf den unteren Schichten. Das bringt den Vorteil, daß die Sicherung auch auf die Sekundärinformationen

[6] Die verschiedenen Programmteile, in denen die jeweiligen Schichten implementiert sind, werden zusammen als „Stack“ bezeichnet.

der unteren Schichten wirkt und damit u. a. Verkehrsanalysen usw. erschwert und die Implementierungen der unteren Schichten vor Angriffen schützt.

Der Nachteil liegt in der kürzeren Reichweite.

4.1.2.3 Konsequenz Mehrfachsicherung

Wie gezeigt wurde, gibt es keine optimale Schicht für Sicherungsmaßnahmen; sowohl die „hohe“, als auch die „niedrige“ Absicherung haben Vor- und Nachteile. Die Konsequenz daraus ist, daß dann, wenn die Eigenschaften verschiedener Schichten genutzt werden müssen, eine mehrfache Absicherung stattfinden muß (siehe Abb. 4.2).

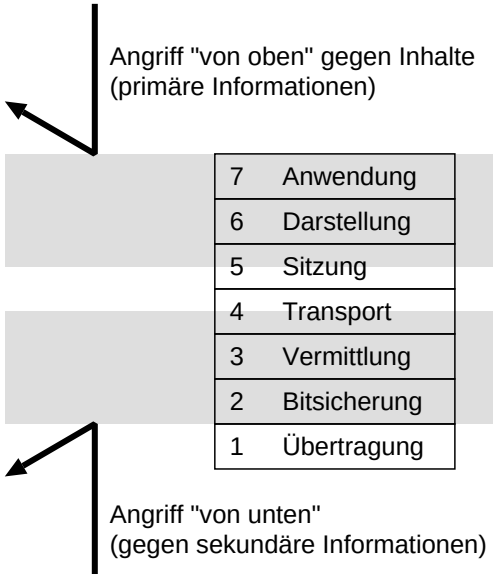


Abbildung 4.2: Eine zwei- oder mehrfache Absicherung kann notwendig werden, wenn die primären Informationen der oberen Schichten weitreichend und die sekundären Informationen der unteren Schichten gegen Verkehrsanalysen und aktive Angriffe geschützt werden sollen.

Beispiel 4.1:
Doppelsicherung bei E-Mail

Die Vertraulichkeit von E-Mail-Übertragungen soll umfassend gewährleistet werden. Zum Schutz der Nutzlast wird auf den oberen Schichten eine Verschlüsselung der Daten, also *des Inhaltes der E-Mail* („Body“) durchgeführt.

Um auch die Hilfslasten (Adressen usw.) zu schützen und eine Verkehrs- und Energieanalyse zu verhindern, wird zusätzlich auf Schicht 3 verschlüsselt, indem die IP-Pakete verschlüsselt in andere Pakete eingepackt

werden. Außerdem werden die verkehrsrelevanten und empfängerspezifischen Schicht-3-Adressen – die IP-Adressen – nach oben verlagert, indem Proxy-Dienste, Remailer und Multiplexer eingesetzt werden. Um die Verteilung der Verkehrsenergie einzuebnen werden Übertragungen nur zu bestimmten Uhrzeiten (z. B. alle 10 Minuten) und mit immer gleichen Datenmengen vorgenommen, etwa indem man bei hohem Nachrichtenaufkommen Nachrichten zeitlich verschiebt oder über andere Mail-Relays laufen läßt und bei zu geringem Aufkommen durch das Verschicken von Rauschen an Dummy-Adressen ergänzt. Man erzeugt dadurch einen Kanal fester Kapazität, der stets voll ausgelastet ist, damit die übertragene Datenmenge keine Rückschlüsse erlaubt.

Um dem Angreifer durch unterschiedlichen Reaktionen auf Angriffe keine Rückschlüsse auf die Wichtigkeit der durch eine Störung verlorengegangenen Nachrichten zu ermöglichen (vgl. Abschnitt 2.5.6), erfolgt die Reaktion auf einen erkannten Angriff immer in gleicher Weise.

4.1.3 Resistenz gegen Umgehung

Jeder Sicherungsmechanismus bleibt wirkungslos, wenn der Angreifer einen Weg findet, der am Mechanismus vorbeiführt. Meist werden solche Umgehungswege dann als „verdeckter Kanal“ bezeichnet. Mechanismen müssen daher so entworfen und zusammengestellt werden, daß eine Umgehung unmöglich ist. Wie ein Mechanismus umgangen werden kann, läßt sich erschöpfend nur im Einzelfall beurteilen. Gerade im Zusammenhang mit einem Schichtenmodell lassen sich aber Angriffe darstellen, die selbst auf der Ausnutzung des Schichtenaufbaus der Kommunikationseinrichtungen beruhen. Diese Angriffe lassen sich klassifizieren und mit Hilfe dieser Einteilung systematisch ausschließen.

Das Ausschließen einer Umgehung bedeutet, daß der Angreifer auf diesem Weg nicht mehr an das Schutzobjekt gelangen kann, und ist deshalb eine organisatorische Maßnahme. Ist eine Umgehung möglich, dann ist der organisatorische Schutz unzureichend.

4.1.3.1 Überspringen

Die – besonders in TCP/IP-Netzwerken – meistverwendete organisatorische Absicherung ist eine Absperrung bzw. Isolierung auf den unteren Schichten. Dazu gehört die physikalische Trennung auf Schicht 1. Sofern auf höheren Schichten keine (beabsichtigte, unbeabsichtigte oder durch den Angreifer provozierte) Relais-Funktionaliät besteht, liegt eine vollständige Isolation vor und ein Überspringen ist nicht möglich.

Oft existiert aber eine Instanz, die Zugang zu beiden Seiten der Absperrung hat, mit beiden Seiten kommuniziert und evtl. selektive Relais-Dienste zur Verfügung stellt. Die Konstellation tritt typischerweise beim Einsatz von

- programmierbaren Bridges[7] (Trennung auf Schicht 1, Relaisfunktion auf Schicht 2),
- Routern (Trennung auf den Schichten 1 und 2, Relaisfunktion auf Schicht 3) und
- Firewallmaschinen (Trennung mindestens bis Schicht 4, Relais- bzw. Proxy- und Gateway-Funktion auf den Schichten 3 bis 7)

auf. Diese Art der Sicherung ist naheliegend, wenn grundsätzlich jede Kommunikation verboten werden soll, hiervon aber bestimmte Ausnahmen möglich sein müssen („Positiv-“ oder „weiße Liste“).

Ein Angreifer kann nun eine solche Instanz mit zwei Netzwerkverbindungen zur Umgehung nutzen (siehe Abb. 4.3). Er kann dazu eine beabsichtigte oder unbeabsichtigte (z. B. versehentlich eingeschaltete) Relaisfunktion ausnutzen; er kann aber auch zuerst das System mit zwei Zugängen angreifen und eine Relaisfunktion provozieren und diese dann danach für den Hauptangriff nutzen. Ein Beispiel hierfür wäre eine Shell, die sich ein Angreifer auf einer Firewall-Maschine verschafft (Schicht-7-Gateway). Ein anderes Beispiel ist die Verwendung der IP-Source-Routing-Optionen.

4.1.3.2 Unterlaufen

Eine andere Art der organisatorischen Absicherung ist die Absperrung bzw. Isolierung auf höheren Schichten. Mit dieser Eigenschaft ist diese Absicherung in der Regel auf bestimmte Dienste der betroffenen Schichten beschränkt und nutzt die Sekundärinformationen dieser Schichten als Entscheidungskriterium. Diese Art der Sicherung ist naheliegend, wenn für bestimmte Dienste bestimmte Aktionen verboten werden sollen (Negativliste).

Beipiele hierfür wären:

- Datei-Zugriffsrechte bei Unix
- `/etc/hosts.allow` und `/etc/hosts.deny` bei neueren Unix-Netzwerkdiensten
- Sperrung bestimmter URLs im WWW-Proxy
- Negativ-Adressliste eines Mailrelay gegen Spamming

[7] An Stelle der Bezeichung „Repeater“ oder „Bridge“ werden heute die Begriffe „Hub“ oder „Switch“ verwendet, wobei „Hub“ eine „dumme“ Relais-Station bezeichnet, die immer alles weiterleitet, während ein „Switch“ die Topologie der angeschlossenen Segmente erkennen und die Relaisfunktion zur Kapazitätsverbesserung auf das technisch notwendige Maß reduzieren oder durch Tabellen programmiert werden kann.

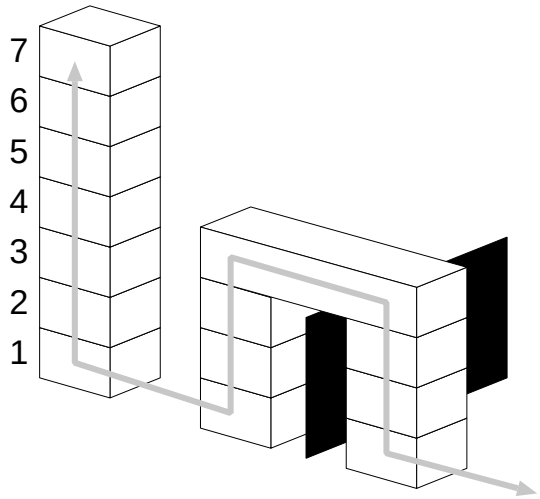


Abbildung 4.3: Eine Absperrung (organisatorische Sicherung, hier schwarz) der unteren drei Schichten wird übersprungen, indem eine Relaisfunktion auf Schicht 4 eines Systems ausgenutzt wird, das zu beiden Seiten Zugang hat. So könnte etwa eine Firewall-Maschine mißbraucht werden.

Die Absicherung richtet sich dabei gegen die *horizontale* Kommunikation der betroffenen Schichten der an verbotener Kommunikation beteiligten Parteien. Sofern diese Sperre wirksam ist, sind damit folglich auch die höheren Schichten blockiert, da sie auf der Funktion der gesperrten Schichten aufbauen (vgl. aber hiergegen die nachfolgend beschriebene horizontale Umgehung).

Nach wie vor können aber die unterhalb der Sperre liegenden Schichten immer noch miteinander horizontal kommunizieren. Sie können zwar dann keine Nutzlast mehr transportieren, aber ihre eigenen Sekundärinformationen. Diese Sekundärinformationen können – soweit sie sich von „oben“ beeinflußen lassen – als Kanal verwendet werden. Der Sender schiebt die Nutzlast in die Sekundärinformationen und der Empfänger betreibt quasi eine Verkehrsanalyse, interpretiert deren Ergebnisse aber als Primärinformationen.

Bemerkung 4.2:
Verlagerung der Schutzobjekte in andere Schichten
Dieser Angriff ist die „Inverse“ zur in Abschnitt 3.6.2.1 beschriebenen Abwehrmethode. Während dort der Verteidiger versucht, möglichst viele Sekundärinformationen in die oberen, sicheren Schichten zu verschieben, versucht hier der Angreifer, möglichst viele Primärinformationen in die unteren, unsicheren Schichten einzulagern.

Zu differenzieren wäre im Einzelfall noch, ob der Angreifer die Verlagerung in die unteren Schichten provoziert bzw. durch einen erfolgreichen Angriff (z. B. trojanisches

Pferd) verursacht hat, oder ob etwa die befugten Parteien durch Unachtsamkeit selbst Informationen in die unteren Schichten sickern lassen (verdächtige Dateinamen usw.).

Beispiel 4.3:
Unterlaufen der Schicht im Bell-LaPadula Modell

Ein Beispiel für eine horizontale Absperrung oberer Schichten ist das von Bell und LaPadula [10, 83, 102] entwickelte Modell zur Gewährleistung der Vertraulichkeit im militärischen Bereich (siehe Abschnitt 1.6.2). Dabei handelt es sich (vereinfacht dargestellt) um ein Zugriffsrechtemodell auf der Ebene von Dateien. Dateien und Benutzern ist jeweils eine Sicherheitsstufe aus einem hierarchisch geordneten Stufenmodell zugeordnet. Zum Lesen oder Schreiben von Daten braucht der Benutzer individuelle diskrete Zugriffsrechte.

Bei der Realisierung des Modells stellte sich jedoch heraus, daß es leicht möglich war, Informationen entgegen der erlaubten Richtung zu übertragen, nämlich über die *Dateinamen*, die auch Benutzern ersichtlich waren, die auf den *Inhalt* der Datei keinen Zugriff hatten[8]. Ein Trojanisches Pferd oder ein böswilliger Benutzer wären dadurch in der Lage, durch Anlegen vieler Dateien über deren Dateinamen schutzbedürftige Daten an einen Benutzer mit niedrigerer Sicherheitsstufe weiterzugeben.

In der Analyse wurde diese Schwäche als „verdeckter Kanal“ angesehen. Diese Erkenntnis ist richtig, aber nur wenig hilfreich, denn die Notwendigkeit, verdeckte Kanäle zu vermeiden, besteht praktisch immer und erlaubt per se noch kein systematisches Vorgehen. Die Betrachtung von Mechanismen im Schichtenmodell bietet hingegen einen Weg, die Kanäle zu finden, die im Zusammenhang mit dieser Struktur stehen.

Zur Abwehr des Unterlaufens gibt es zwei Wege, die sich aus systematischer Vorgehensweise, nämlich der genauen Festlegung des Feindbildes, ergeben. Dazu ist festzulegen, ob man die Schichten unterhalb der Absicherung als feindlich besetzt ansieht:

1. Sollen die unteren Schichten nicht als feindlich besetzt angesehen werden, müssen sie zwangsläufig ebenfalls zum *Schutzobjekt* werden. Sicherungsmaßnahme müssen auch für die unteren Schichten ergriffen werden, deren *horizontale* Kommunikation gesichert.

   In Beispiel 4.3 hätte eine organisatorische Absicherung den Angreifer von den Sekundärinformationen des Dateisystems abhalten können. Ein Weg hierzu wäre gewesen, jeder Sicherungsstufe eine eigenen Datenbereich (Verzeichnisbaum, Plattenpartition o. ä.) zuzuweisen.

[8] Es stellten sich noch andere Schwächen heraus; hier soll aber exemplarisch nur diese eine betrachtet werden.

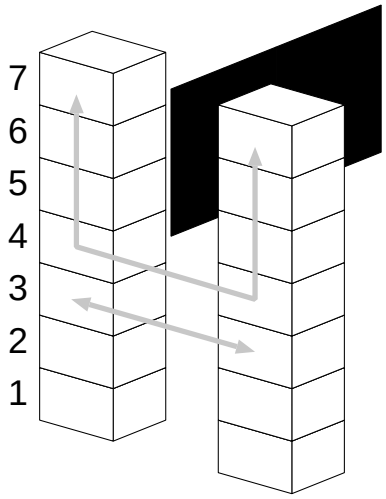


Abbildung 4.4: Eine Absperrung (organisatorische Absicherung) der *oberen* Schichten kann unterlaufen werden, wenn der Angreifer zur Kommunikation die *Sekundär*informationen der unteren Schichten mißbrauchen kann. Im Bild wird daher die logische horizontale Kommunikation der Schichten 3 und 4 gezeigt.

2. Sollen die unteren Schichten jedoch als feindlich besetzt angesehen werden, müssen sie zwangsläufig in das *Feindbild* als Position des Angreifers aufgenommen werden.

   Das bedeutet, daß Sicherungsmaßnahmen zwischen den oberen und den unteren Schichten angreifen müssen, um deren *vertikale* Kommunikation zu sichern. Die oberen Schichten dürfen dabei weder Kenntnis der unteren Sekundärinformationen erlangen noch Einfluß auf diese nehmen.

   In Beispiel 4.3 hätte die etwa eine Maßnahme sein können, die verhindert, daß der Angreifer Nutzen aus dem Kontakt mit dem Schutzobjekt ziehen kann (vgl. Abschnitt 3.8), nämlich eine kryptographische Verschlüsselung der Sekundärinformationen (Dateiname, Datum usw.), die nur der befugte Benutzer entschlüsseln kann.

Beispiel 4.4:
Schwächen der Intel 80x86 Prozessoren

Eine besonders häufig verwendete Art der organisatorischen Absicherung ist die Trennung der Adreßräume von Rechenprozessen unter moderneren Betriebssystemen mit Hilfe von Speicherverwaltungsmechanismen und die Isolierung der Prozesse untereinander durch Schaffung einer virtuellen Maschine.

Beides wird heutzutage von modernen Mikroprozessoren geleistet, die

über eine eigene MMU[9], die Unterscheidung zwischen Benutzer- und Supervisorprozessen und privilegierte Befehle verfügen. Darauf aufbauend können Betriebssysteme ein Zugriffsrechtemodell verwirklichen und durchsetzen.

Es liegt aber auf der Hand, daß die gesamte Sicherheit eines solchen Systems von der Sicherheit der zugrundeliegenden virtuellen Maschine, d. h. der Korrektheit und Sicherheit der MMU, der Trennung von Superivisor- und Anwendermodus etc., abhängt. Ist diese nicht gewährleistet, bricht die Sicherheit des gesamten Systems zusammen.

Dennoch wird diese Schwachstelle regelmäßig bei Sicherheitsüberlegungen mißachtet und die Sicherheit von Mikroprozessoren usw. trotz bekannter Mängel als gegeben angesehen.

Gerade die weit verbreiteten Intel 80x86-Prozessoren (und einige der mehr oder weniger kompatiblen Nachbauten) weisen jedoch Schwächen auf, die diese Prozessoren als für hohe Sicherheitsanforderungen ungeeignet erscheinen lassen.

Wie in [112] beschrieben, weisen diese Prozessoren eine ganze Reihe von Eigenheiten auf, die als *verdeckte Kanäle* zwischen Rechenprozessen verwendet werden können. Die Kanalkapazität ist dabei sehr begrenzt, sie reicht aber bequem, um schnell und unbemerkt etwa kryptographische Schlüsselinformationen von einem Prozeß zu einem anderen zu übertragen. Dabei handelt es sich nicht nur um Implementierungsfehler, sondern auch um Entwurfsfehler, die sich nicht ohne weiteres korrigieren lassen.

In [112] wurden bereits im Jahr 1995 102 verschiedene Schwächen und Fehler dieser Prozessoren zusammengestellt, von denen 17 als sicherheitsrelevant eingestuft wurden. In der Zwischenzeit wurden weitere Probleme entdeckt (z. B. [124]).

Bemerkung 4.5: Trennung von Betriebssystem und Anwendung

Wie in Beispiel 4.4 bereits angedeutet wurde, kann die Sicherheit des Betriebssystems vor Zugriffen aus einem Anwendungsprozeß gefährdet sein, wenn die Speicherschutzmechanismen und die virtuelle Maschine Schwächen aufweisen. Damit wird ein Angriff von *oben nach unten* möglich.

Aber auch der umgekehrte Fall, nämlich der Angriff *von unten nach oben* ist denkbar, wenn etwa ein Zugriff aus dem Betriebssystem auf den Anwendungsprozeß erfolgt, beispielsweise um kryptographische Schlüsseldaten auszulesen. Die Gefahr hierfür bestünde, wenn das Betriebssystem nicht vertrauenswürdig und fehlerfrei ist oder bereits angegriffen

[9] Memory Management Unit

und modifiziert wurde. Heutige Rechnerarchitekturen bieten jedoch keinen Schutz vor Zugriffen aus dem Betriebssystem; das Betriebssystem kann auf alle Bestandteile der Maschine zugreifen.

Eine Absicherung wäre hier durch Einfügen einer Sicherung auf Schicht 1, also der Hardware, möglich. Hierzu müßte eine physikalische Trennung der virtuellen Maschinen erfolgen, also eine Verteilung auf *mindestens zwei reale oder virtuelle* Maschinen mit getrennten Bussystemen, Prozessoren, Hauptspeichern usw., zwischen denen eine Kommunikationsverbindung besteht, auf die die Betriebssystemschnittstelle abgebildet wird. So könnte der Anwendungsbereich vom Betriebssystembereich getrennt werden. Festplatten, Schnittstellen usw. müssen aber durch das Betriebssystem verwaltet werden, das Laden des Anwendungsprogrammes und der Laufzeitdaten, Benutzereingaben usw. müssen ebenfalls über diese Geräte erfolgen.

Das Betriebssystem könnte dabei das Programm beim Laden verändern. Es könnte ebenso den deterministischen Programmlauf mit allen Ein- und Ausgaben auf einer zweiten Maschine simulieren und damit die Vertraulichkeit unterwandern. Eine rein organisatorische Absicherung ist so also nicht möglich.

Hier wäre deshalb die Ergänzung durch eine kryptographische Absicherung notwendig. Die zu ladenden Programme müßten verschlüsselt abgelegt und erst unmittelbar beim Laden in den Hauptspeicher – und damit sicher vor dem Zugriff des Betriebssystems – entschlüsselt und auf Integrität überprüft werden. Ebenso müssen schlüsselrelevanten Ein- und Ausgaben am Betriebssystem vorbei in den Hauptspeicher gelangen. Dies setzt eine organisatorische Trennung und damit eine gewissen Verteilung voraus[10].

4.1.3.3 Horizontale Protokoll-Umgehung

Sollen verschiedene Bereiche eines Netzwerkes durch selektive organisatorische Maßnahmen topologisch getrennt werden (Territorialsicherung), muß sichergestellt werden, daß sich die Absperrung auf *alle* Protokolle und Implementierungen der Schicht, auf der die Absperrung vorgenommen wird, auswirkt. Die Absicherung nur eines Protokolls kann durch Verwendung anderer Protokolle umgangen werden (Abb. 4.5).

[10] Denkbar wäre ein Parallelrechner, auf dem die Daten nach einem Shared-Secret-Schema verteilt sind. Kein einzelner Prozessor könnte die Daten auslesen.

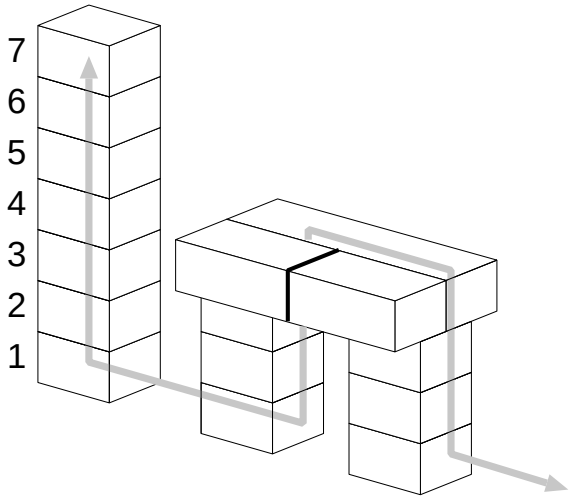


Abbildung 4.5: Die Absperrung eines bestimmten Protokolls zur Trennung verschiedener Netzwerkbereiche kann durch Verwendung eines anderen Protokolls umgangen werden (Horizontale Umgehung).

Beispiel 4.6:
Horizontale Umgehung
Paket-Filter auf den Schichten 3 und 4, die als TCP/IP-Firewall verwendet werden, sind nicht immer sauber konfiguriert und sperren oft nur bestimmte TCP und UDP-Pakete. Ein solcher Filter kann umgangen werden, indem ICMP-Pakete verschickt werden. Normalerweise tragen diese Pakete keine große Nutzlast, es ist aber problemlos möglich, den IP-Rahmen zu vergrößern und diesen Paketen „künstlich“ eine Nutzlast anzuhängen. So können trotz Absperrung Daten transportiert werden.

Viele Beispiele sind auch auf Schicht 7 zu finden. Die Sperrung von WWW-Seiten durch Proxy-Filter kann etwa durch Nutzung externer WWW-E-Mail-Gateways umgangen werden. Der Zugriff auf News-Gruppen beispielsweise durch Benutzung von News-Server mit HTTP-Schnittstelle usw.

4.1.3.4 Vertikale Protokoll-Umgehung

Analog zur horizontalen Protokoll-Umgehung ist auch die vertikale Umgehung möglich (Abb. 4.6). Diese Form der Umgehung ist in der Praxis von geringerer Bedeutung, denn es gibt nur wenige Anwendungen und Betriebssysteme, die eine derartige Sperre vorsehen. Gleichwohl ist diese Umgehungsmöglichkeit beim Entwurf von Sicherungsmaßnahmen zu berücksichtigen.

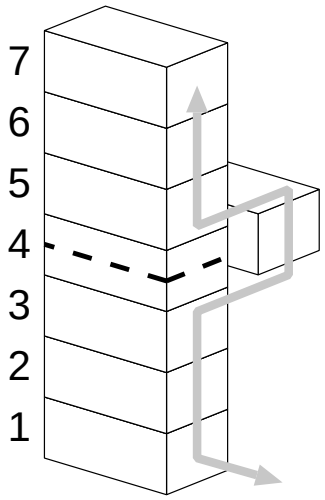


Abbildung 4.6: Auch eine Absperrung zwischen übereinanderliegenden Schichten kann umgangen werden, wenn sich die Absperrung nicht auf alle Protokolle der betreffenden Schicht betrifft.

4.1.3.5 Routen- und Adreß-Umgehungen

In gleicher Weise sind auch Sperren, die nicht auf bestimmte Protokolle, sondern auf Routen- und Adreßinformationen aufsetzen, zu umgehen. Typische Beispiele hierfür sind Remailer, Proxy-Dienste, Spiegel usw.

Diese Form der Umgehung hat besondere Bedeutung erlangt, seit Inhalte im Internet ins Blickfeld der Strafverfolgung und staatlicher Überwachungsmaßnahmen gerückt sind. Wie in vielen Fällen beobachtet werden konnte, zeigt die Sperrung des Zugangs zu bestimmten WWW-Server u. ä. nicht nur keine merkliche Wirkung, sie spornt sogar noch dazu an, die gesperrten Seiten unter anderen Adressen zu spiegeln oder ständig die Adresse der gesperrten Seite zu ändern.

4.1.3.6 Mischformen

Zusätzlich sind auch Mischformen verschiedener Umgehungen möglich und beim Entwurf der Sicherungsmechanismen in Betracht zu ziehen.

Beispielsweise ist die *kompromittierende Abstrahlung* eine Mischform aus Unterlaufen, weil alle Software- und Protokollschranken unterlaufen werden, und einer horizontalen Umgehung auf Schicht 1, weil die vermeintliche elektrische Begrenzung des Rechners auf seine äußeren Abmessungen durch elektromagnetische Abstrahlung oder unbeabsichtigte Übertragungen über Stromkabel usw. umgangen wird.

4.2 Effektivität und Kosten

Sicherungsmechanismus sind nicht immer völlig unüberwindbar; sie sollen und müssen dies oft auch gar nicht sein. Sofern ein geeignetes und zuverlässiges Angreifermodell besteht, genügt es, wenn die absolute oder sogar nur die relative Leistungsfähigkeit des Angreifers den Mechanismus nicht überwinden kann.

Deshalb müssen Beschreibung, Entwurf und Beurteilung von Mechanismen auch deren Stärke und Effektivität, d. h. deren Fähigkeit, einem Angriff zu widerstehen, miteinbeziehen. Dabei ist zu unterscheiden, ob die Angriffskosten den zu erwartenden Gewinn für den Angreifer übersteigen oder mit den ihm zur Verfügung stehenden Mitteln nicht erbracht werden können.

4.2.1 Erfolg und Erfolgsdetektion

Nicht immer besteht der Aufwand für den Angreifer in der Überwindung der Sicherheitsmechanismen alleine. Bei manchen Mechanismen muß der Angreifer zusätzlich erkennen, ob sein Angriff erfolgreich war, ob er beispielsweise aus dem Schlüsselraum den passenden Schlüssel gefunden hat oder ob ein Teilangriff, dessen Erfolg nur mit einer bestimmten Wahrscheinlichkeit eintritt, wirksam war.

Die Beschreibung des Angriffsaufwandes umfaßt daher:

- Die Beschreibung der Komplexität des Angriffes, damit abschätzbar wird, wie sich die Angriffskosten ändern, wenn die Stärke des Mechanismus geändert wird,
- die Beschreibung des außerhalb der theoretischen Komplexität liegenden praktischen Aufwandes (Kostenfaktor) und
- der Aufwand für die Erfolgsdetektion, denn der Erfolg des Angriffes ist für den Angreifer nicht notwendigerweise (leicht) zu erkennen.

4.2.2 Theoretische Schranken

Die – besonders bei kryptographischen Mechanismen – wichtigste Beschreibung der Stärke ist die Darstellung der theoretischen Schranken, und zwar des *Minimalaufwandes*, des *Maximalaufwandes* und des zu erwartenden *mittleren Aufwandes* für einen erfolgreichen Angriff. Die Darstellung erfolgt dabei in theoretischen Größen, etwa der Anzahl der Rechenschritte eines Automaten eines bestimmten Rechnermodells (z. B. Turing-Maschine, RAM, Rechenschritte) in Abhängigkeit von bestimmten Größen wie Länge der Nachricht, Anteil der Redundanz, Schlüssellänge usw., und wird entweder als exakte Gleichung oder im O-Kalkül dargestellt.

4.2.3 Angriffskosten

Nicht nur die theoretischen Schranken, auch tatsächliche Kosten für den Angreifer und die Grenzen verfügbarer Technik können einen Angriff verhindern oder für den Angreifer als nicht sinnvoll erscheinen lassen[11].

Bemerkung 4.7:
Relevanz des Angriffszeitraumes
Bei der Abschätzung der Angriffskosten ist auch jeder mögliche in den Betrachtungszeitraum fallende Anfangszeitpunkt bzw. -zeitraum für den Angriff zu betrachten.

Stehen dem Angreifer ein bestimmter Geldbetrag und ein größerer Zeitraum (mehrere Monate oder Jahre) zur Verfügung, so kann es beim in den letzten Jahren zu beobachtenden Preisverfalls von Rechenanlagen bei gleichzeitiger Steigerung der Rechenleistung für den Angreifer durchaus sinnvoll sein, zunächst einige Zeit gar nichts zu tun und das Geld gewinnbringend anzulegen und erst später die Hardware für den Angriff zu beschaffen, um dann in der verbleibenden Zeit mehr Rechenleistung als bei einer sofortigen Investition erbringen zu können.

Die Zeit, in der kein Angriff erfolgt, ist daher nicht notwendigerweise ein Gewinn für den Verteidiger.

Bemerkung 4.8:
Größen für Angriffskosten
Angriffskosten sollten nicht in festen Größen angegeben werden, sondern in einen zum Schutzobjekt sinnvollen Bezug gebracht werden, insbesondere zu dessen Wert und zur beabsichtigten Wirkungsdauer des Schutzes.

Sinnvolle Größen wären etwa:

- Kosten eines Angriffs innerhalb eines Zeitraumes, der in sinnvollem Verhältnis zur Lebensdauer des Schutzobjektes steht,
- Dauer eines Angriffs, für den finanzielle Mittel in einem sinnvollen Verhältnis zum Wert des Schutzobjektes bereitstehen,
- alle Kosten-/Dauer-Tupel, mit denen der Angreifer unterhalb des zeitabhängigen Wertverfalls des Schutzobjektes bleibt.

4.2.4 Alterung

Der Zeitablauf wirkt nicht nur dann gegen den Verteidiger, wenn der Angreifer die Zeit nutzt. Mechanismen können auch selbst an Wirksamkeit verlieren, etwa wenn die Beweiskraft von Signaturen u. ä. durch Gesetze beschränkt ist. Dies ist ebenfalls zu berücksichtigen.

[11] Was allerdings voraussetzt, daß der Angreifer selbst rational vorgeht.

4.3 Nebenwirkungen und Anforderungen

> *„Zu Risiken und Nebenwirkungen lesen Sie die Systemspezifikation oder fragen Sie Ihren Informatiker!“*

Sicherheitsmechanismen und die ihnen zugrundeliegenden Methoden haben nicht notwendigerweise nur die günstigen Eigenschaften, derentwegen sie eingesetzt werden. Ihre Wirksamkeit hängt regelmäßig auch von der Einhaltung bestimmter Randbedingungen ab und bringt neue Anforderungen mit sich.

Sicherheitsmechanismen können daher nur beurteilt und klassifiziert werden, wenn eine genaue Beschreibung auch dieser Eigenschaften vorliegt.

4.3.1 Abhängigkeit von Systemeigenschaften

Sicherheitsmechanismen verlieren oft ihre Wirkung, weil das tatsächliche System nicht mehr mit dem dem Entwurf zugrundegelegten System übereinstimmt, sondern sich von diesem in wesentlichen Eigenschaften unterscheidet.

Zur Beurteilung und Klassifikation von Sicherheitsmechanismen müssen daher auch die Eigenschaften des Systems mitbetrachtet werden, auf die der Entwurf oder die Auswahl beruhen. Von diesen Eigenschaften hängt es ab, ob sich ein zweites, ähnliches System vom Entwurfssystem in einer für die Sicherheit relevanten Eigenschaft unterscheidet, und ob die Mechanismen auch dieses System übertragbar sind.

In der Folge ist auch jede Änderung des Systems auf Verträglichkeit mit diesen Anforderungen zu untersuchen. Dabei sind nicht nur die „relativen“ Änderungen zum jeweils letzten untersuchten Zustand des Systems zu betrachten, sondern auch die „absoluten“ Änderungen gegenüber dem Entwurfssystem, denn die Änderungen des Systems sind nicht dahingehend „abgeschlossen“, daß mehrere verträgliche Änderungen zusammen wieder eine verträgliche Änderung ergeben müssen.

4.3.2 Eingriffstiefe und Nebenwirkungen

Nicht nur die Wirkung des zu sichernden Systems auf die Sicherheitsmechanismen, sondern umgekehrt auch die Wirkung der Mechanismen auf das System ist zu beschreiben und in die Beurteilung mit einzubeziehen.

Dazu gehören Fragestellungen wie:

- Bleibt das System kompatibel zu anderen, ungesicherten Systemen, zu denen es vormals kompatibel war (kann und soll z. B. ein abgesichertes E-Mail-Programm noch mit ungesicherten Programmen E-Mail austauschen)?

- Welche Protokolle, Implementierungen usw. des gesicherten Systems wurden verändert? Wurde das System als „Black Box“ angesehen?
- Bleiben alle Eigenschaften des Systems erhalten (z. B. Fehlertoleranz etwa gegen Störungen der Übertragung)?
- In welcher Weise unterscheidet sich das gesicherte System vom ungesicherten aus Sicht der befugten Parteien?
- Kann das mit den Sicherheitsmechanismen versehene System auch ungesichert betrieben werden bzw. können die Mechanismen vollständig „abgeschaltet“ werden?
- Kann das gesicherte System zuverlässig von einem ungesicherten unterschieden werden?

4.3.3 Übersicherung

Eine besonders schwerwiegende Nebenwirkung ist es, wenn sich die Sicherungswirkung auch auf die befugten Parteien bezieht und die Funktion des Systems dadurch beeinträchtigt wird. Zwei Fälle sind hier als prototypisch zu betrachten:

- Der Sicherungsmechanismus gerät in einen Zustand, in dem die *Unterscheidung* zwischen befugten und unbefugten Parteien nicht mehr korrekt funktioniert und befugten Parteien daher als unbefugt behandelt werden.
- Die Adressen bzw. Erkennungsmerkmale der befugten Parteien haben ihre Funktion oder semantische Bedeutung verloren, die befugten Parteien sind nicht mehr als solche erkennbar.

Wie das folgende Beispiel zeigt, ist eine Übersicherung nicht in jedem Fall einfach zu vermeiden, manchmal sogar unvermeidlich. Die Gefahr der Übersicherung muß aber zur Beurteilung des Mechanismus und zum Vergleich mit anderen Mechanismen in der Spezifikation beschrieben werden.

Beispiel 4.9:
Übersicherung durch PIN
Verschiedene Sicherheitsmechanismen (Geldautomaten, Telefonkarten usw.) beruhen auf der Eingabe eines Paßwortes, das oft nur auf einer vierstelligen Dezimalzahl (PIN) beruht. Wegen des kleinen Schlüsselraumes ist eine vollständige Suche in kurzer Zeit möglich. Es ist daher notwendig, auf Fehlversuche mit einer Sperrung zu reagieren, um so die vollständige Suche zu unterbinden.

Wird durch dreimalige Eingabe einer falschen PIN eine Sperrung provoziert, läßt sich diese auch durch Eingabe der richtigen PIN nicht wieder

aufheben. Der befugte Benutzer wird dabei nicht mehr vom unbefugten Benutzer unterschieden, es liegt also eine Übersicherung vor[12].

Vergißt der Benutzer seine PIN, dann hat er seine Adresse verloren (Merkmal: Der, der die PIN kennt), und kann nicht mehr von der unbefugten Partei unterschieden werden. Auch hier liegt eine Übersicherung vor.

4.3.4 Problemverlagerungen

Sicherheitsmechanismen und die ihnen zugrundeliegenden Methoden sind – soweit bisher bekannt – allgemein keine Problem*lösungen*, sondern Problem*verlagerungen*.

Mit jeder Methode und mit jedem Mechanismus ergeben sich daher neue Probleme, die – wenn sie nicht schon durch das bestehende System mit den bisher ausgewählten Mechanismen und Methoden gelöst werden – durch neue Mechanismen und Methoden gelöst werden müssen.

Daraus resultieren neue Probleme, die im ursprünglichen System noch nicht gegeben waren und die durch neue Mechanismen und Methoden gelöst werden müssen. So ergibt sich eine Kette von Problemen und Problemlösungen, an deren Ende eine Menge von im Vergleich zum Urproblem leichteren Problemen, die nicht mehr durch technische Mittel lösbar sind, deren Lösung aber außerhalb der Technik gefunden werden kann.

Bei der Auswahl und Beurteilung von Mechanismen ist eine komplette Beschreibung der gesamten Kette und der verbleibenden Restprobleme zu berücksichtigen.

4.3.5 Abbildung auf technische Merkmale

Das Ziel von Sicherheitsmechanismen ist es, die Befugnisse der Parteien entsprechend der Interessenlage des Interessenträgers technisch so umzusetzen, daß das „Können“ dem „Dürfen“ entspricht. Dazu ist es notwendig, die Vorstellungen des Interessenträgers über die Identität der Parteien auf technisch greifbare Merkmale abzubilden, die als Adressen bezeichnet werden (vgl. Abschnitt 2.2.2 und Definition 2.4).

Die Funktion von Sicherheitsmechanismen hängt daher von der *Korrektheit* und der *Sicherheit* der Abbildung der Vorstellungen des Interessenträgers auf technische Adressen und der Erkennung und Verwertung dieser Adressen ab.

[12] Deshalb gibt es bei Mobiltelefonen für diesen Fall eine zusätzliche längere PIN, die die Sperre wieder aufheben kann. Es gibt damit also noch eine weitere befugte Partei, die auch im Falle der Sperrung noch von unbefugten unterschieden wird.

Bemerkung 4.10:
Schutzobjekt Adresse
Bei allen auf Unterscheidung von Parteien ausgelegten Sicherheitsmechanismen ist deshalb grundsätzlich die Problemverlagerung auf die Sicherheit der Adressen und deren Erkennung zu berücksichtigen.

Die Beschreibung der verwendeten Adressen, d. h. der technischen Merkmale, deren Beschreibung als Schutzobjekt und die Abbildung der Vorstellungen des Interessenträgers müssen daher Teil der Spezifikation des Mechanismus sein. Dabei ist zu unterscheiden zwischen

- Merkmalen, die unabhängig vom gesicherten System und dem Sicherungsmechanismus bestehen,
- Merkmalen, die dem Zweck des gesicherten Systems dienen und dafür unabhängig vom Sicherungsmechanismus eingeführt wurden und
- Merkmalen, die dem Sicherheitsmechanismus dienen und dafür eingeführt wurden.

4.4 Nichttechnische Eigenschaften

Das Ziel von Sicherheitsmechanismen ist die technische Um- und Durchsetzung, weshalb technische Eigenschaften fraglos im Vordergrund stehen. Es gibt aber auch nichttechnische – hauptsächlich juristische – Randbedingungen, die bei der Beurteilung von Sicherheitsmechanismen zu berücksichtigen sind. Nachfolgend werden nur einige dieser Aspekte kurz angerissen, weil diese außerhalb des Themas dieser Arbeit liegen.

4.4.1 Verbot und Gebot von Mechanismen

Der Einsatz bestimmter Sicherheitsmechanismen kann im Einzelfall staatlichen oder sonstigen Verboten zuwiderlaufen. Besonders kryptographische Maßnahmen werden zunehmend staatlich mißbilligt.

Daraus folgt zwangsläufig, daß die Legalität eines Mechanismus als wichtiges Kriterium anzusehen ist. Die Legalität ist jedoch nicht immer einfach darzustellen nach dem Schema „erlaubt oder verboten“. Es ist durchaus möglich, daß es vom Einzelfall abhängt, ob der Mechanismus verwendet werden darf oder nicht, z. B. wenn verschlüsselte Verbindungen nur mit Parteien im gleichen Land zulässig sind, oder wenn die Verschlüsselungseinrichtungen nicht exportiert werden dürfen.

Umgekehrt kann es natürlich auch möglich sein, daß bestimmte Mechanismen oder allgemein der Schutz gewisser Objekte gegen gewissen Angriffe *geboten* sind, z. B. durch Datenschutzgesetze, Gewerbevorschriften usw.

Die Verträglichkeit mit den Gesetzen ist daher ein wichtiges Kritierium.

4.4.2 Rechtstreue als Schutzobjekt

Gesetze erhalten ihre Wirkung durch Sanktionen, die mit ihrer Verletzung verbunden werden. Ziel eines Angriffes könnte es sein, einen Gesetzesverstoß erscheinen zu lassen und so Sanktionen gegen den Interessenträger auszulösen. Dies könnte z. B. dadurch geschehen, daß übertragene Nachrichten in einem Land mit Verschlüsselungsverbot durch Zufallsdaten substituiert werden und die Nachricht wie eine verschlüsselte erscheint. Der vermeintliche Absender sieht sich nun dem Vorwurf des Gesetzesverstoßes ausgesetzt und kann auch unter dem Druck von Zwangsmaßnahmen die Nachricht nicht offenlegen, weil es keinen Klartext gibt.

Die Einhaltung von Gesetzen ist ggf. selbst als Schutzobjekt zu betrachten.

4.4.3 Verbote und Gebote als Angriff

Beziehen sich Verbote und Gebote auch auf den Inhalt der Datenübertragung, ist also etwa die Übertragung bestimmter Inhalte verboten, so ist aus technischer Sicht der Versuch dessen, der die Einhaltung überwacht, entweder Wissen von einer unerlaubten Übertragung zu erlangen oder diese nachzuweisen (vgl. Abschnitt 2.4.2).

Dies wird ausführlich in Kapitel 5 behandelt.

4.4.4 Wirksamkeit

Auch die Wirksamkeit von Sicherheitsmaßnahmen kann von gesetzlichen und anderen Rahmenbedingungen abhängig sein. Die beste digitale Signatur unter einer Bestellung oder einer Bankverfügung nutzt im Streitfall nichts, wenn digitale Signaturen nicht als Beweis bzw. als Urkunde anerkannt werden. Methoden zur Angriffserkennung und zum Angriffsnachweis haben deutlich geringere Wirkung, wenn nach dem Rechtssystem des jeweiligen Staates Betrug usw. nur an einer natürlichen Person, nicht aber an einem Rechner begangen werden kann.

5 Besondere Probleme staatlicher Kommunikationsüberwachung

Niemand darf willkürlichen Eingriffen in sein Privatleben . . . oder seinen Briefwechsel . . . ausgesetzt werden.

Aus Art. 12 der Allgemeinen Erklärung der Menschenrechte

1. Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.
2. Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Art. 8 der Konvention zum Schutze der Menschenrechte u. Grundfreiheiten

Die Achtung der Privatsphäre und des Familienlebens, des Ansehens, der Wohnung und des privaten Post- und Fernmeldeverkehrs wird gewährleistet.

Art. 6 Nr. 2 der Erklärung der Grundrechte und Grundfreiheiten des Europäischen Parlaments

Niemand darf das Objekt willkürlicher oder mißbräuchlicher Eingriffe in sein Privatleben . . . , seine Wohnung oder seinen Briefverkehr . . . sein.

Art. 11 Nr. 2 der Amerikanischen Menschenrechtskonvention

1. Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
2. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. [. . .]

Aus Art. 10 Grundgesetz

5.1 Überblick

Wer sich mit Kommunikationssicherheit im allgemeinen oder Kryptographie im besonderen beschäftigt, kommt derzeit selbst bei einer rein technisch-wissenschaftlichen Betrachtungsweise nicht umhin, sich auch mit „Kryptoverboten“ und „Schlüsselhinterlegungsgeboten“ und damit juristischen und politischen Aspekten der Thematik zu beschäftigen, denn diese Rahmenbedingungen wirken sich mehrfach aus:

- Abwehrmaßnahmen gegen nichtstaatliche Angreifer haben sich innerhalb der gesetzlichen Vorgaben zu bewegen, was beispielsweise bedeuten kann, daß nur noch kurze Schlüssel oder gar keine Kryptographie mehr Verwendung finden dürfen.
- Der Staat bekundet damit seine Absicht, die Vertraulichkeit und – je nach Vorgehensweise auch die Echtheit – von Nachrichten zu verletzen.

  Aus technischer Sicht wird der Staat damit zum Angreifer.
- Die Einhaltung von Gesetzen wird üblicherweise durch Strafandrohung zu fördern versucht.

  Daraus ergibt sich ein neues Schutzobjekt, nämlich die Abwehr des Nachweises eines Gesetzesverstoßes. Zweck dieser Betrachtung ist es nicht, Straftaten zu fördern oder vor Verfolgung zu schützen, sondern die Problematik eines Nachweises zu untersuchen und damit Irrtümer und Scheinbeweise zu verhindern.

Zum Zwecke der staatlichen Kommunikationsüberwachung stehen verschiedene Gesetzeskonstruktionen zur Diskussion oder finden in verschiedenen Ländern Anwendung:

- Vollständiges Verbot kryptographischer Methoden
- systematische Schwächung von Verfahren, beispielsweise Beschränkungen der Schlüssellänge oder der Qualität von Chiffren
- Zugang des Staates zu symmetrischen Schlüsseln
- Zugang des Staates zu asymmetrischen Schlüsseln
- Prophylaktische Schlüsselhinterlegung oder nachträgliche Schlüsseloffenlegung
- Technischer Zugang des Staates zur übertragenen Information
- Zwang zur nachträglichen Offenlegung auf Anforderung

Ein weiterer Weg der staatlichen Kommunikationsüberwachung, der hier ebenfalls berücksichtigt werden soll, ist der *geheimdienstliche*. Im Gegensatz zur gesetzlichen Überwachung, bei der der Überwachte wenigstens die grundsätzlichen Methoden und Befugnisse des Überwachers aus dem Gesetzestext kennt, bleiben dem Überwachten hier die Methoden und die Stärke unbekannt. Hierzu gehört auch der Fall der Spionage, wenn nämlich der überwachende Staat nicht der eigene ist oder sich ganz außerhalb der Legitimität bewegt.

Aus diesen beiden Grundproblematiken lassen sich die folgenden Fragestellungen herleiten:

- Wie können Daten so transportiert werden, daß sie vom Überwacher nicht
  - bemerkt,
  - gelesen oder
  - nachgewiesen

  werden können?
- Wie kann der Überwacher vom Überwachten unbemerkt an Schlüssel- oder Teilinformationen gelangen?
- Wie kann die Sicherheit trotz Einhaltung vorgegebener Grenzen für Schlüssellänge etc. erhöht werden?
- Wie kann der Staat (z. B. im Strafverfahren) den Nachweis erbringen, daß unerlaubt verschlüsselt wurde?
- Wie wirkt sich ein Kryptographieverbot auf die für unerlaubte Datenübertragungen zur Verfügung stehende Kanalkapazität aus?

Nachfolgend wird das in Abb. 5.1 auf Seite 122 dargestellte einfache Kanalmodell zugrunde gelegt, das eine an die Fragestellung angepaßte Version des Grundschemas in Abbildung 2.3 auf Seite 48 ist. Es gibt naheliegenderweise einen Sender und einen Empfänger, sowie einen Kanal zwischen beiden.

Außerdem gibt es einen *Zensor*[1], genau *eine* Anzapfstelle am Kanal zwischen Sender und Empfänger, sowie einen Kanal von der Anzapfsstelle zum Zensor, der alle an der Anzapfstelle sichtbaren Zeichen des diskreten Kanals an den Zensor überträgt und damit über (mindestens) die gleiche Kanalkapazität verfügt, wie der Kanal zwischen Sender und Empfänger. Der Zensor ist damit ein Angreifer in der Position der Abbildung 2.3c.

Da der Zensor nach diesem Modell nur eine Anzapfstelle hat, kann er die Kanalqualität (d.h. die Störanfälligkeit) des Kanals vom Sender bis zur Anzapfstelle und von der Anzapfstelle nicht genau beurteilen. Hat er jedoch mehrere Anzapfstellen an verschiedenen Stellen des Kanals, können diese kontrahiert und als eine Anzapfstelle angesehen werden, wobei das Kanalsegment zwischen den äußersten Anzapfstellen vernachlässigt wird.

Die Anzapfstelle ist passiv, d. h. der Zensor nimmt keinen Einfluß auf den Kanal (also keine Störungen, Man in the Middle-Attacken u. ä.).

[1] Duden-Verlag, Das Fremdwörterbuch: 1. niemandem verantwortlicher Beamter im Rom der Antike, der u. a. die Vermögensschätzung der Bürger durchführte u. eine sittenrichterliche Funktion ausübte. 2. a) behördlicher Beurteiler, Überprüfer von Druckschriften; b) Kontrolleur von Postsendungen.

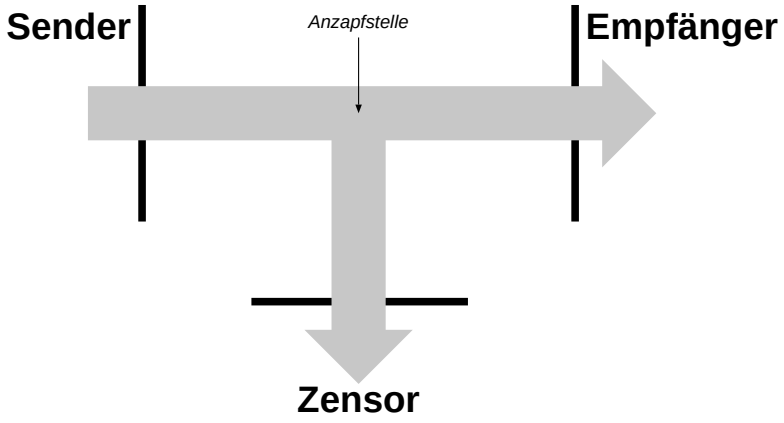


Abbildung 5.1: Kanalmodell zur Kommunikationsüberwachung: Das Kanalmodell aus Abbildung 2.3a (Seite 48) wird um einen Zensor in der festen Position aus Abbildung 2.3c ergänzt.

5.2 Informationstheoretische Grundlagen

5.2.1 Allgemeine Informationstheorie

Nachfolgend werden kurz einige informationstheoretische Grundlagen zusammengestellt, die überwiegend [62] und [127] entnommen wurden, wo auch weitergehende Darstellungen zu finden sind.

Definition 5.1:
Stichprobe und Wahrscheinlichkeitsverteilung
Es sei $Q = \{s_1, s_2, \ldots, s_u\}$ eine endliche Menge von *Stichproben* oder *Elementarereignissen* genannten Elementen. Den Stichproben $s_i \in Q$ sei jeweils eine reelle Wahrscheinlichkeit $p_i := p(s_i) \in [0, 1]$ so zugeordnet, daß $\sum_{i=0}^{u} p_i = 1$ ist.

Der Vektor $\boldsymbol{p} := p(Q) := (p_1, p_2, \ldots, p_u) \in [0, 1]^u$ heißt die *Wahrscheinlichkeitsverteilung* von Q.

Das Paar $(Q, \boldsymbol{p})$ – oder kurz Q – heißt *endlicher Stichprobenraum*.

Es seien F und G zwei nichtleere Mengen. Jedem Paar $\alpha\beta \in F \times G$ von Stichproben $\alpha \in F$ und $\beta \in G$ sei eine *Verbundwahrscheinlichkeit* $p(\alpha\beta) \in [0, 1]$ so zugeordnet, daß $\sum_{\alpha \in F, \beta \in G} p(\alpha\beta) = 1$ ist.

Dann bildet das kartesische Produkt $FG := F \times G$ aller als Elementarereignisse betrachteten Paare $\alpha\beta \in F \times G$ einen Stichprobenraum $(FG, \boldsymbol{p})$, den *Verbundraum* FG.

Auf den Mengen F und G wird durch $p(\alpha) := \sum_{\beta \in G} p(\alpha\beta)$ und $p(\beta) := \sum_{\alpha \in F} p(\alpha\beta)$ jeweils eine Wahrscheinlichkeitsverteilung definiert: Die *Faktoren* F und G des Verbundraumes FG sind in natürlicher Weise Stichprobenräume.

Der Verbundraum FG wird als *Produktraum* bezeichnet, und seine Faktoren F und G heißen *unabhängig*, wenn für alle $\alpha \in F$ und alle $\beta \in G$ stets $p(\alpha\beta) = p(\alpha) \cdot p(\beta)$ gilt.

Definition 5.2:
Bedingte Wahrscheinlichkeit
Es sei FG ein Verbundraum und $\alpha \in F$ ein nicht unmögliches Elementarereignis, das heißt eine Stichprobe des Faktors F von FG mit $p(\alpha) = \sum_{\beta \in G} p(\alpha\beta) \neq 0$.

Für jedes Element $\beta \in G$ definieren wir seine *bedingte Wahrscheinlichkeit*[2] als $p(\beta|\alpha) := \frac{p(\alpha\beta)}{p(\alpha)}$ und entsprechend für alle $\beta \in G$ mit $p(\beta) \neq 0$ $p(\alpha|\beta) := \frac{p(\alpha\beta)}{p(\beta)}$

Es gilt: $p(\alpha|\beta) = \frac{p(\alpha)}{p(\beta)} \cdot p(\beta|\alpha)$ (Bayessche Formel).

Definition 5.3:
Quelle
Unter einer *Quelle* wird in diesem Zusammenhang die Interpretation eines Stichprobenraumes $(Q, \boldsymbol{p})$ als Lieferant von Elementarereignissen verstanden, der entsprechend seiner Wahrscheinlichkeitsverteilung *Zeichen* aus Q abgibt.

Definition 5.4:
Kanal
Ein *Kanal*[3] ist ein Tripel $(F, G, (p_{i,j}))$, bestehend aus einem q-nären *Eingangs-Zeichenvorrat* oder *Eingang* $F = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$ mit $q \geq 2$, einem r-nären *Ausgangs-Zeichenvorrat* oder *Ausgang* $G = \{\beta_1, \beta_2, \ldots, \beta_r\}$ mit $r \geq 1$ und einer stochastischen $q \times r$-Matrix ohne Nullspalten, der *Kanalmatrix* $(p_{i,j})$.

Der Eingang F besteht aus allen möglichen Zeichen α, die der Kanal aufnehmen kann; der Ausgang G besteht aus allen möglichen Zeichen β, die am Kanalausgang beobachtet werden können. Der Koeffizient $(p_{i,j})$ der Kanalmatrix gibt als *Übergangswahrscheinlichkeit* die bedingte Wahrscheinlichkeit $p_{i,j} = p(\beta_j|\alpha_i)$ an, daß nach der Eingabe des Zeichens $\alpha_i \in F$ in den Kanal die Ausgabe des Zeichens $\beta_j \in G$ am Kanalausgang beobachtet wird.

[2] Gelesen „p von β nach α“

[3] Ein diskreter, stationärer Kanal ohne Gedächtnis, hier aber nur als „Kanal“ bezeichnet

Die Verbundwahrscheinlichkeit $p(\alpha\beta) = p(\alpha) \cdot p(\beta|\alpha)$ gibt an, mit welcher Wahrscheinlichkeit ein Beobachter des Ein- und Ausgangs des Kanals die Eingabe eines Elements $\alpha \in F$ und die darauffolgende Ausgabe eines Elementes $\beta \in G$ wahrnimmt.

Die bedingte Wahrscheinlichkeit, daß ein gewisses, in den Kanal eingegebene Zeichen $\alpha \in F$ die Ausgabe eines Zeichens $\beta \in G$ verursacht hat, ist $p(\alpha|\beta) := \frac{p(\alpha\beta)}{p(\beta)}$ und damit von $p(F)$ abhängig.

Definition 5.5:
Informationsgehalt
Der *Informationsgehalt* eines Zeichens s aus einem Zeichenvorrat wird als

$$I_a(s) := \log_a \frac{1}{p(s)} = -\log_a p(s)$$

definiert, wobei a eine willkürlich gewählte reelle Konstante mit $a > 1$ ist.

Soweit nichts anderes erwähnt ist, wird stillschweigend $a = 2$ gewählt und dem Informationsgehalt dann die Maßeinheit bit zugeordnet.

Definition 5.6:
Entropie
Die *Entropie* einer q-nären Quelle $(Q, \boldsymbol{p})$ ist der mittlere Informationsgehalt der von ihr ausgegebenen Zeichen:

$$H_a(Q) := \sum_{s \in Q} p(s) \cdot I_a(s) = -\sum_{s \in Q} p(s) \cdot \log_a p(s)$$

Satz 5.7:
Satz über die Verbundentropie
Es sei FG ein endlicher Verbundraum. Dann gilt:

$$H_a(FG) \leq H_a(F) + H_a(G)$$

Es gilt genau dann

$$H_a(FG) = H_a(F) + H_a(G)$$

wenn F und G unabhängig sind (Beweis in [62]).

Der *bedingte Informationsgehalt* $I_a(\beta|\alpha) := \log_a \frac{1}{p(\beta|\alpha)}$, den ein Beobachter des Kanalausgangs, der die tatsächliche Eingabe α kennt, noch aus der Beobachtung der Ausgabe β gewinnt, muß im Kanal entstanden und damit durch die *Kanalstörungen* verursacht worden sein.

Die *bedingte Entropie* $H_a(G|\alpha) := \sum_{\beta \in G} p(\beta|\alpha) \cdot I_a(\beta|\alpha)$ gibt an, wieviel neue Information im Mittel am Kanalausgang zu beobachten ist, wenn bekannt ist, daß das Zeichen α eingegeben wurde, also wieviel *Rauschen* bei Eingabe von α entsteht.

Die sog. *Irrelevanz* $H_a(G|F) := \sum_{\alpha \in F} p(\alpha) \cdot H_a(G|\alpha)$ gibt an, wieviel Entropie die Rauschquelle im Kanal im Mittel abgibt.

Satz 5.8:
Satz über die Verbundentropie und Irrelevanz
Es sei FG ein endlicher Verbundraum. Dann gilt:

$$H_a(FG) = H_a(F) + H_a(G|F)$$

(Beweis in [62])

Umgekehrt gibt der *bedingte Informationsgehalt* $I_a(\alpha|\beta) := \log_a \frac{1}{p(\alpha|\beta)}$ an, wieviel Information der Beobachter des *Kanaleingangs*, der das tatsächlich ausgegebene Zeichen β kennt, durch die Beobachtung der Eingabe hinzugewinnt, was also im Kanal *verloren* gegangen ist.

Die *bedingte Entropie* $H_a(F|\beta) := \sum_{\alpha \in F} p(\alpha|\beta) \cdot I_a(\alpha|\beta)$ gibt an, wieviel Information im Mittel verloren gegangen ist, wenn am Ausgang das Zeichen β beobachtet wurde.

Die sog. *Äquivokation* $H_a(F|G) := \sum_{\beta \in G} p(\beta) \cdot H_a(F|\beta)$ gibt an, wieviel Entropie der Kanal im Mittel vernichtet.

Satz 5.9:
Satz über die Verbundentropie und Äquivokation
Es sei FG ein endlicher Verbundraum. Dann gilt:

$$H_a(FG) = H_a(G) + H_a(F|G)$$

(Beweis in [62])

Bemerkung 5.10:
Verbundentropie
Die mittlere Information, die man aus der Beobachtung von Ein- *und* Ausgang erhält, also die Verbundentropie $H_a(FG)$, kann man also aus zwei Blickwinkeln sehen, nämlich als das, was man in den Kanal hineinsteckt zuzüglich des im Kanal entstandenen Rauschens (Satz 5.8), oder als das, was aus dem Kanal herauskommt zuzüglich dessen, was im Kanal verloren gegangen ist (Satz 5.9).

Definition 5.11:
Transinformationsgehalt
Die *gegenseitige Information*

$$I_a(\alpha;\beta) := I_a(\alpha) - I_a(\alpha|\beta) = log_a \frac{p(\alpha|\beta)}{p(\alpha)}$$

gibt an, wieviel Informationsgehalt des Zeichens α nicht vom Kanal verschluckt wird, sondern die Übertragung überlebt.

$$I_a(\beta;\alpha) := I_a(\beta) - I_a(\beta|\alpha) = log_a \frac{p(\beta|\alpha)}{p(\beta)}$$

gibt an, wieviel Informationsgehalt des Zeichens β aus der Eingabe von α stammt und nicht vom Kanal erzeugt wurde.

Mit der Bayesschen Formel ergibt sich $I_a(\alpha;\beta) = I_a(\beta;\alpha)$. Dieser Wert wird als *Transinformationsgehalt* von α und β bezeichnet.

$$\begin{aligned} I_a(F;G) :&= \sum_{\alpha\in F}\sum_{\beta\in G} p(\alpha\beta)\cdot I_(\alpha;\beta) \\ &= H_a(F) - H_a(F|G) \\ &= H_a(G) - H_a(G|F) \end{aligned}$$

Definition 5.12:
Kanalkapazität
Die *Kapazität* K eines Kanals $(F, G, (p_{i,j}))$ wird definiert als der maximale Transinformationsgehalt, der sich bei optimaler Nutzung erzielen läßt:

$$k := \max_{p(F)} I_a(F;G)$$

5.2.2 Informationstheorie und Kryptographie

Die besondere Anwendung der Informationstheorie auf kryptographische Problemstellungen geht grundlegend auf [111] zurück. Eine eingehende Darstellung ist in [127] und [107] zu finden.

Definition 5.13:
Kryptosystem
Ein *Kryptosystem* ist ein Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ mit folgenden Eigenschaften:

1. $\mathcal{P}$ ist eine endliche Menge von möglichen *Klartexten*.
2. $\mathcal{C}$ ist eine endliche Menge von möglichen *Chiffraten*.
3. $\mathcal{K}$ ist eine endliche Menge von möglichen *Schlüsseln*.
4. $\mathcal{E} = \{E_k : \mathcal{P} \to \mathcal{C} | k \in \mathcal{K}\}$ ist eine endliche Menge von *Chiffrierfunktionen*.
5. $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{P} | k \in \mathcal{K}\}$ ist eine endliche Menge von *Dechiffrierfunktionen*.
6. $\forall k \in \mathcal{K}, x \in \mathcal{P} : D_k(E_k(x)) = x$.
7. Bei Bedarf werden $\mathcal{P}$ und $\mathcal{K}$ als Stichprobenraum aufgefaßt, d. h. es gibt je eine Wahrscheinlichkeitsverteilung $p_{\mathcal{K}}(k), k \in \mathcal{K}$ und $p_{\mathcal{P}}(x)$, $x \in \mathcal{P}$.

Außerdem sei $C(k) := \{E_k(x) : x \in \mathcal{P}\}$ die Menge aller möglichen Chiffrate zum Schlüssel k.

Sofern nichts anderes erwähnt ist, wird nachfolgend vereinfachend $|\mathcal{P}| = |\mathcal{C}|$ und damit $\forall k \in \mathcal{K} : C(k) = \mathcal{C}$ bzw. $\forall k \in \mathcal{K}, y \in \mathcal{C} : E_k(D_k(y)) = y$ unterstellt.

Daraus ergibt sich auch eine Wahrscheinlichkeitsverteilung über den Chiffraten:

$$\forall y \in \mathcal{C} : p_{\mathcal{C}}(y) = \sum_{k \in \mathcal{K}} p_{\mathcal{K}}(k) \cdot p_{\mathcal{P}}(D_k(y))$$

Außerdem läßt sich die bedingte Wahrscheinlichkeit für ein Chiffrat y bei gegebenem Klartext x angeben:

$$p_{\mathcal{C}}(y|x) = \sum_{k \in \mathcal{K}: y = E_k(x)} p_{\mathcal{K}}(k)$$

Da bei festem k das Chiffrat vom Klartext unmittelbar abhängt (siehe hierzu aber Bemerkung 5.15), läßt sich ebenfalls angeben:

$$p_{\mathcal{C}}(y|k) = p_{\mathcal{P}}(D_k(y))$$

Bemerkung 5.14:
Berechnung von $p_{\mathcal{P}}(x|y)$
Mit der Bayesschen Formel läßt sich damit die bedingte Wahrscheinlichkeit für einen Klartext x bei gegebenem Chiffrat y angeben:

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x)}{p_{\mathcal{C}}(y)} \cdot p_{\mathcal{C}}(y|x) = p_{\mathcal{P}}(x) \cdot \frac{\sum\limits_{k \in \mathcal{K}: y = E_k(x)} p_{\mathcal{K}}(k)}{\sum\limits_{k \in \mathcal{K}} p_{\mathcal{K}}(k) \cdot p_{\mathcal{P}}(D_k(y))}$$

Der Angreifer, der die Wahrscheinlichkeitsverteilungen $p_{\mathcal{K}}$ und $p_{\mathcal{P}}$ kennt und technisch zur Berechnung der Summen – also zur vollständigen Suche – in der Lage ist, kann $p_{\mathcal{P}}(x|y)$ berechnen.

Bemerkung 5.15:
Berechnung von $p_{\mathcal{P}}(k|y)$
Ebenfalls mit der Bayesschen Formel läßt sich die bedingte Wahrscheinlichkeit für einen Schlüssel k bei gegebenem Chiffrat y angeben:

$$p_{\mathcal{K}}(k|y) = \frac{p_{\mathcal{K}}(k)}{p_{\mathcal{C}}(y)} \cdot p_{\mathcal{C}}(y|k) = p_{\mathcal{K}}(k) \cdot \frac{p_{\mathcal{P}}(D_k(y))}{\sum\limits_{k' \in \mathcal{K}} p_{\mathcal{K}}(k') \cdot p_{\mathcal{P}}(D_{k'}(y))}$$

Der gleiche Sachverhalt noch einmal in Entropie-Schreibweise:

Wir betrachten des Gesamtsystem als Verbund aus $\mathcal{K}$, $\mathcal{P}$ und $\mathcal{C}$. Die Entropie $H_a(\mathcal{KPC})$ läßt sich mit den Sätzen über die Verbundentropie umformen. Da $\mathcal{K}$ und $\mathcal{P}$ unabhängig sind, gilt übrigens $H_a(\mathcal{KP}) = H_a(\mathcal{K}) + H_a(\mathcal{P})$:

$$\begin{aligned} H_a(\mathcal{KPC}) &= H_a(\mathcal{C}|(\mathcal{KP})) + H_a(\mathcal{KP}) \\ &= H_a(\mathcal{C}|(\mathcal{KP})) + H_a(\mathcal{K}) + H_a(\mathcal{P}) \\ H_a(\mathcal{KPC}) &= H_a(\mathcal{P}|(\mathcal{KC})) + H_a(\mathcal{KC}) \\ &= H_a(\mathcal{P}|(\mathcal{KC})) + H_a(\mathcal{K}|\mathcal{C}) + H_a(\mathcal{C}) \end{aligned}$$

Damit gilt also:

$$H_a(\mathcal{C}|(\mathcal{KP})) + H_a(\mathcal{K}) + H_a(\mathcal{P}) = H_a(\mathcal{P}|(\mathcal{KC})) + H_a(\mathcal{K}|\mathcal{C}) + H_a(\mathcal{C})$$

In der Literatur wird normalerweise ohne Aufhebens angenommen, daß durch Schlüssel und Klartext das Chiffrat bzw. durch Schlüssel und Chiffrat der Klartext völlig festgelegt sind, ebenso wie wir oben $p_{\mathcal{C}}(y|k) = p_{\mathcal{P}}(D_k(y))$ unterstellt haben, damit also

$$H_a(\mathcal{C}|(\mathcal{KP})) = H_a(\mathcal{P}|(\mathcal{KC})) = 0$$

gesetzt.

Das ist so aber nicht allgemein haltbar.

$H_a(\mathcal{C}|(\mathcal{KP}))$ und $H_a(\mathcal{P}|(\mathcal{KC}))$ beschreiben nämlich das Chiffrier- und das Dechiffrierverfahren. Sie sind nur dann gleich 0, wenn beide Verfahren algorithmisch völlig eindeutig und überdies öffentlich festgelegt, dem Angreifer also bekannt sind.

Dies ist aber gerade dann nicht der Fall, wenn dem Angreifer das Verfahren nicht bekannt ist (wobei vor dieser „Security by Obscurity“ gewarnt werden muß), oder wenn eine ganze Familie von Chiffren Verwendung findet, wobei man darüber streiten kann, ob die Wahl des Verfahrens der Chiffre oder dem Schlüssel zuzuordnen ist. Von Bedeutung ist die dem Verfahren innewohnende Entropie jedenfalls dann, wenn es gilt, mit Schlüssel, Chiffrat und Klartext die Funktionsweise eines unbekannten Verfahrens zu erkunden.

Die Annahme ist ebenfalls dann nicht richtig, wenn die Verfahren nicht eindeutig sind, sondern der Verschlüsselungsvorgang eine Rauschquelle mit einbezieht. Das mag zunächst etwas „an den Haaren herbeigezogen“ klingen, ist aber z. B. beim *Jefferson Wheel* [73] der Fall, bei dem

$H_a(\mathcal{C}|(\mathcal{KP})) \approx 4,64$ bit beträgt und damit klar größer als 0 ist. Betrachtet man die üblichen Hybridverfahren aus asymmetrischen und symmetrischen Chiffren als ein Verfahren, so gilt dies auch hier, weil der Absender zur Wahl des symmetrischen Schlüssels (und evtl. zu dessen Ergänzung auf die Länge des asymmetrischen Schlüssels) eine Zufallszahl verarbeiten muß. Auch die in Abschnitt 5.4.1.6 vorgestellte Blendungsentropie gehört hierzu.

Setzt man aber $H_a(\mathcal{C}|(\mathcal{KP})) = H_a(\mathcal{P}|(\mathcal{KC})) = 0$, so ergibt sich $H_a(\mathcal{K}) + H_a(\mathcal{P}) = H_a(\mathcal{K}|\mathcal{C}) + H_a(\mathcal{C})$, bzw. analog zur obigen Wahrscheinlichkeit

$$H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{K}) + H_a(\mathcal{P}) - H_a(\mathcal{C})$$

Da wegen $H_a(\mathcal{C}|(\mathcal{KP})) = 0$ das Chiffrat durch den Schlüssel und den Klartext feststeht, kann $H_a(\mathcal{C})$ nicht größer als $H_a(\mathcal{K}) + H_a(\mathcal{P})$ sein, der Ausdruck also nicht negativ werden.

Wichtig ist aber, daß $H_a(\mathcal{K}|\mathcal{C})$ erheblich kleiner als $H_a(\mathcal{K})$ werden kann, wenn $H_a(\mathcal{C}) > H_a(\mathcal{P})$, d. h. wenn der Klartext weniger Information enthält, als er nach seiner Länge könnte, also *Redundanz* enthält.

Bemerkung 5.16:
$H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{P}|\mathcal{C}) + H_a(\mathcal{K}|(\mathcal{CP}))$

Aus den bisher gezeigten Sätzen folgt:

$$\begin{aligned} H_a(\mathcal{CKP}) &= H_a(\mathcal{CK}) + H_a(\mathcal{P}|(\mathcal{CK})) \\ &= H_a(\mathcal{CP}) + H_a(\mathcal{K}|(\mathcal{CP})) \end{aligned}$$

Da die Dechiffrierung bei den hier betrachteten Chiffren eindeutig ist, ist der Klartext durch ein Chiffrat und einen Schlüssel bereits festgelegt, weshalb $H_a(\mathcal{P}|(\mathcal{CK})) = 0$ gesetzt werden kann. Im Gegensatz dazu kann $H_a(\mathcal{K}|(\mathcal{CP}))$ nicht gleich 0 gesetzt werden, weil es mehrere Schlüssel geben kann, die ein Chiffrat und einen Klartext aufeinander abbilden, insbesondere wenn $|\mathcal{K}| > |\mathcal{P}|$.

$$\begin{aligned} &\Longrightarrow && H_a(\mathcal{CK}) = H_a(\mathcal{CP}) + H_a(\mathcal{K}|(\mathcal{CP})) \\ &\Longrightarrow && H_a(\mathcal{C}) + H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{C}) + H_a(\mathcal{P}|\mathcal{C}) + H_a(\mathcal{K}|(\mathcal{CP})) \\ &\Longrightarrow && H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{P}|\mathcal{C}) + H_a(\mathcal{K}|(\mathcal{CP})) \end{aligned}$$

$H_a(\mathcal{K}|(\mathcal{CP})$ hängt wesentlich vom Chiffrierverfahren und vom Verhältnis von $|\mathcal{K}|$ zu $|\mathcal{P}| = |\mathcal{C}|$ ab[4].

5.3 Verbot chiffrierter Übertragungen

Das offenkundigste und naheliegendste Werkzeug staatlicher Kommunikationsüberwachung ist das Verbot der Übertragung chiffrierter Nachrichten, das oft so gescholtene „Kryptoverbot“.

Das Interesse des Angreifers (= Staat) liegt hier nicht nur im Angriff gegen die Vertraulichkeit der Nutzlast, sondern auch in der Erkennung oder gar dem Nachweis der Verwendung eines Chiffrierverfahrens. Der Angriff gegen die Vertraulichkeit braucht hier nicht weiter vertieft zu werden, weil er keine Besonderheit staatlicher Kommunikationskontrolle darstellt.

Wesentlich sind hier die Erkennung und der Nachweis chiffrierter Übertragungen.

5.3.1 Position im Schichtenmodell

Ein technischer Aspekt eines Kryptoverbotes ist die Frage, auf welche Schicht im Schichtenmodell sich das Verbot bezieht. Die Bedeutung dieser Frage ist nicht offensichtlich, denn prinzipiell scheint es egal zu sein, auf welcher Schicht man sichert, solange der Angreifer nicht die eigentliche Nutzlast angreifen kann.

Die Bedeutung dieser Frage ergibt sich erst aus der Differenzierung zwischen dem Angriff auf die Vertraulichkeit der Nachricht und dem Nachweis einer Verschlüsselung. Grundsätzlich ist zu unterscheiden (und diese Unterscheidung findet sich z. T. auch in den Telekommunikationsgesetzen wieder) zwischen den Nutz- und Hilfslasten, sowie dem Vorgang der Übertragung (Zeit, Umfang usw.). Es ist ein Unterschied, ob der Angreifer etwa einen Telefoneinzelverbindungsnachweis oder eine Aufzeichnung des Telefonates selbst erhält. Der Unterschied muß hier in der Position im Schichtenmodell liegen, nicht allein in der Unterscheidung zwischen Nutz- und Hilfslast, denn jede Hilfslast ist zugleich auch Nutzlast der niedrigeren Schichten.

Wenn der Gesetzgeber nun für bestimmte Fälle erlaubt, die Verbindungsdaten, noch nicht aber die Nachrichten selbst zu überwachen, so kann man das als Angriff auf die unteren Schichten (bis etwa einschließlich Schicht 4) interpretieren, also beispielsweise Telefonnummer, Nebenstellennummern, ISDN-Dienstekennungen, aber auch IP-Adressen und Portnummern von Internet-Verbindungen.

Ein solcher Zugriff brächte es dann mit sich, daß der Zensor eine Verschlüsselung auf Schicht 3 erkennen könnte, während er eine solche auf Schicht 6 nicht mehr erkennen

[4] Damit bei Blockchiffren aber auch von der Betriebsart und damit indirekt doch wieder von der Länge des Klartextes

darf, denn dazu müßte er die Nutzlasten, also die Inhalte der oberen Schichten auswerten. Damit aber hätte er die Erhebung der Verbindungsdaten verlassen und wäre zum Belauschen der Nachricht selbst übergegangen (bzw. hätte sich dem genähert).

Daraus ergeben sich unvermutete Unterschiede in den Eigenschaften der verschiedenen Schichten.

5.3.2 Probleme der Detektion

In der Diskussion um ein Kryptoverbot wird immer wieder stillschweigend unterstellt, daß man es einem Datenstrom einfach ansehen könne, ob er verschlüsselt ist oder nicht. Diese Annahme ist albern, muß in diesem Kontext aber betrachtet werden.

Zunächst stellt sich die eher philosophische Frage, wann eine Nachricht verschlüsselt ist bzw. was die dazu passende Interpretationsvorschrift ist und wann diese als Entschlüsselung anzusehen wäre. Man stelle sich vor, der Schlüssel zu einer Nachricht sei gut lesbar auf einer Plakatwand angeschrieben, die nur vom Standpunkt einer Person A, nicht aber von dem einer Person B sichtbar ist. A und B werden sicherlich zu unterschiedlichen Ansichten über die Qualität der Verschlüsselung gelangen.

Auch wäre zu klären, was genau überhaupt Klartext ist und auf welcher Schicht im Schichtenmodell er anzusiedeln wäre. Man kann einen Text verschlüsseln und das Chiffrat übertragen. Man kann aber auch das Chiffrat als die eigentliche Nachricht auffassen und diese dann „im Klartext“ übertragen[5]. Auch eine verschlüsselte und per SMTP übertragene E-Mail wird vom Router als Klartext aufgefaßt und so weiterübertragen.

Selbst wenn man den Klartext auf der Schicht der Mensch-Maschine-Schnittstelle festlegen würde, ergäben sich Mehrdeutigkeiten. Zu klären wäre auch, wie sich eine unterschiedliche Behandlung einer Substitutionschiffre auf unterschiedlichen Schichten rechtfertigen ließe, z. B. einer Zeichensubstition auf Schicht 6 und einer auf Schicht 8 (Interpretationsebene, also etwa „Schwiegermutter besuchen“ = „Bank überfallen“).

So ist jedes Kriterium für das Vorliegen einer Verschlüsselung ad absurdum zu führen. Ein genaues und nachvollziehbares Kriterium wäre für ein Kryptoverbot aber notwendig, denn anderenfalls würde man die Gesetzgebungskompetenz vom Gesetzgeber aufgeben und durch eine richterliche Willkürentscheidung ersetzen. Insbesondere würden so die Kriterien erst im nachhinein durch das Gericht festgelegt werden, was dem Grundsatz zuwiderliefe, daß die Strafbarkeit vor der Tat festgelegt sein muß.

Abgesehen von den Definitionsproblemen läßt sich aber auch zeigen, daß es ein solches Kriterium nicht geben kann:

[5] Hier wird die Differenzierung zwischen zeitlichem und räumlichem Charakter einer Sicherung deutlich

Theorem 5.17:
Unzensierbarkeit des voll genutzten Kanals
Der voll ausgenutzte Kanal endlicher Kapazität ist nicht zensierbar.

Beweis 5.18:
Unzensierbarkeit des voll genutzten Kanals
Gegeben sei ein Kanal endlicher Kapazität mit zweiwertiger Zeichenmenge (Bit) zwischen Sender und Empfänger, über den ständig Daten unter voller Ausnutzung seiner Kapazität übertragen werden.

Weiterhin wird angenommen, es gäbe eine „verbotene“ Chiffre und einen passenden Detektor, der die Verwendung dieser Chiffre allein durch Betrachtung der übertragenen Daten erkennen kann. Es wird angenommen, daß er nach spätestens n Bit zu einem endgültigen Ergebnis darüber kommt, ob die verbotene Chiffre verwendet wurde oder nicht.

Der Sender verwendet nun diese Chiffre und schaltet nun nach jeweils n übertragenen Bit beliebig zwischen der chiffrierten und der unchiffrierten Übertragung um (siehe Abb. 5.2).

Der Empfänger verwendet einen solchen Detektor und untersucht jeweils n Bit als Nachricht. Je nachdem, welche Lampe aufleuchtet, schaltet er die Dechiffrierung ein oder aus.

Dadurch wird der Datenstrom wie bisher mit voller Bandbreite und unverändert übertragen.

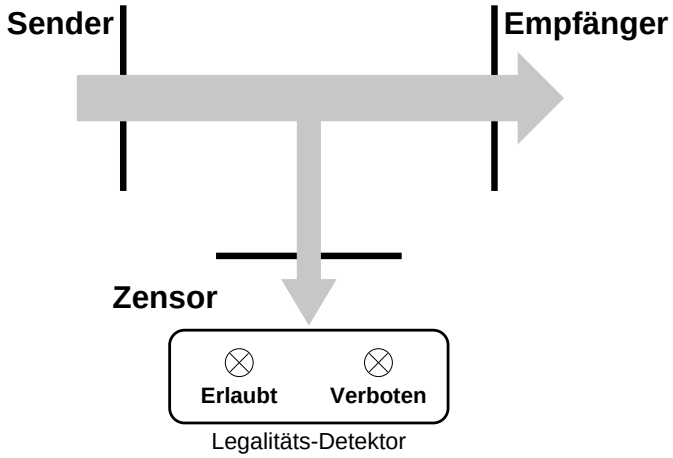
Zusätzlich aber wird pro n Bit ein zusätzliches Bit übertragen, daß der Sender beliebig festlegen und der Empfänger an den Lampen erkennen kann, das also zur Übertragung zur Verfügung steht.

Damit könnte aber das $\frac{n+1}{n}$-fache der Kanalkapazität übertragen werden, was der Annahme widerspricht.

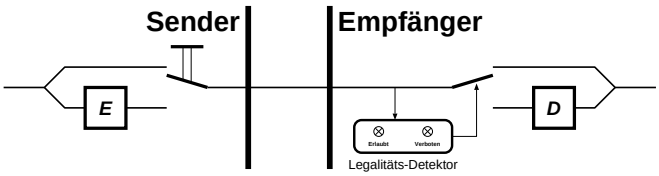
Außerdem könnte das Verfahren kaskadiert werden, über dem so entstandenen neuen Kanal höherer Kapazität das gleiche Spiel gespielt werden, seine Kapazität also erneut gesteigert werden usw.

Die Detektion ist also nicht möglich, wenn die volle Kanalkapazität ausgenutzt wird. Ohne Detektion der Verwendung einer Chiffre ist auch eine inhaltliche (semantische) Zensur nicht denkbar.

(Anmerkung: Wenn der Detektor nur mit einer gewissen Wahrscheinlichkeit das richtige und nicht nur ein rein zufälliges Ergebnis liefert, wird damit ein Teil eines Bits übertragen. Die Detektion stellt dann einen gestörten Kanal dar, über den mit Hilfe fehlerkorrigierender Codes Nachrichten übertragen werden könnten. Sogar eine Detektion mit nur eingeschränkter Zuverlässigkeit ist deshalb unmöglich.)



(a) Der „Legalitätsdetektor“, der über zwei Lampen anzeigt, ob eine verbotene Chiffre verwendet wurde, . . .



(b) . . . und seine Verwendung zur Erhöhung der Kanalkapazität. *E* ist eine illegale (!) Verschlüsselungsvorrichtung, *D* die passende Entschlüsselungsvorrichtung.

Abbildung 5.2: Gelegentlich wird die Auffassung vertreten, daß man einem Datenstrom ansehen können müßte, ob er Klartext oder Chiffrat und damit illegal ist; man würde quasi einen Apparat mit einer roten und einer grünen Lampe anklemmen und den Absender verhaften, sobald die rote Lampe aufleuchtet (a). Wäre dies möglich, könnte man auf jedem beliebigen Kanal stets noch ein zusätzliches Bit übertragen, indem der Sender wählt, ob er legal oder illegal überträgt und der Empfänger dies mit einem solchen Detektor auswertet (b). Zusätzlich zur normalen Übertragung könnte er das „Legalitätsbit“ am Detektor ablesen.

Der voll ausgenutzte Kanal endlicher Kapazität ist nicht zensierbar (Beweis 5.18).

Die prinzipiell gleiche Überlegung kann auch in Entropie-Schreibweise dargestellt werden. Wir betrachten dazu den Kanal zwischen Sender und Empfänger. Der Sender sei die Quelle F, der normale Empfänger beobachtet an seinem Ausgang die Elementarereignisse G. Zusätzlich beobacht

der Zensor die Ereignisse $Z = \{$„unchiffriert“„chiffriert“$\}$, also $|Z| = 2$. Am Ausgang des Kanals ist also der Verbundraum GZ zu beobachten.

Damit die Zensur nicht absurd ist, muß $H_a(Z) > 0$ gefordert werden. Weil der Empfänger die Ereignisse in G erst *nach* der Dechiffrierung betrachtet (siehe hierzu aber Bemerkung 5.19), kann man G nicht mehr ansehen, ob eine Chiffrierung vorlag oder nicht. Deshalb muß $H_a(Z|G) = H(Z)$, oder zumindest $H_a(Z|G) > 0$ gefordert werden[6].

Die Transinformation, also die Menge der tatsächlich übertragenen Information, ergibt sich damit für den Fall mit und ohne Zensor zu

$$
\begin{aligned}
I_a(F;G) &= H_a(G) - H_a(G|F) \\
I_a(F;(GZ)) &= H_a((GZ)) - H_a((GZ)|F) \\
&= H_a(G) + H_a(Z|G) - H_a((GZ)|F) \\
&= I_a(F;G) + H_a(Z|G) + (H_a(G|F) - H_a((GZ)|F))
\end{aligned}
$$

Da keiner der Werte kleiner als Null sein kann, gibt es drei Möglichkeiten (bzw. Kombinationen daraus):

$I_a(F;(GZ)) > I_a(F;G)$
: Der Kanal hat eine höhere Kapazität als $I_a(F;G)$ und wurde deshalb nicht voll ausgenutzt.

$H_a(Z|G) = 0$
: In diesem Fall hängt die Zensur überhaupt nicht mehr davon ab, ob verschlüsselt wurde oder nicht, weil schon bei Kenntnis des Klartextes das Ergebnis der Zensur bekannt ist. Das bedeutet, daß die Zensur entweder nur vom Klartext abhängt, oder daß sogar $H_a(Z) = 0$ ist, d. h. das Ergebnis der Zensur ist konstant und die Strafbarkeit hängt in keiner Weise mehr von der eigentlichen Tat ab[7].

$H_a((GZ)|F) > H_a(G|F)$
: In diesem Fall rauscht der Kanal stärker, sobald der Zensor zuhört. Das würde bedeuten, daß der Zensor den Kanal manipuliert und die übertragenen Daten aktiv verändert, um seine eigenen Informationen übertragen zu können.

  Wie dies konkret aussehen könnte, wird in Abschnitt 5.5.2 gezeigt.

  Letztlich führt dies aber dazu, daß der Kanal durch den eigentlichen Benutzer unfreiwillig auch nicht mehr voll ausgenutzt wird.

[6] Andernfalls würde nicht die Chiffrierung, sondern der semantische Gehalt der Nachricht unabhängig von der Verwendung einer Chiffre bestraft werden.

[7] Ein Schelm, wer diesen Fall als charakteristisch ansieht . . .

Es wird aber auf Bemerkung 5.19 hingewiesen.

Bemerkung 5.19: Randbedingungen

In Beweis 5.18 wurde gezeigt, daß der Zensor bei voller Ausnutzung des Kanals nicht erkennen kann, ob die Übertragung chiffriert ist oder nicht.

Die Sache hat einen Haken: *Aus genau dem gleichen Grund kann es der eigentliche Empfänger auch nicht.*

Sender und Empfänger müssen sich deshalb in irgendeiner Weise darüber einigen, ob sie eine Chiffre benutzen oder nicht (und ggf. über den Schlüssel). Sie müssen sich also auf dem benutzten oder einem anderen Kanal diese Information zukommen lassen. Genau da findet sich aber der Überschuß an Bandbreite, der Beweis 5.18 aushebeln würde. *Das Problem zwischen Sender und Empfänger wurde also nicht gelöst, es wurde nur verlagert.*

Dennoch kann es für den Zensor schwierig werden, diese Verständigung zu finden, denn sie benötigt normalerweise eine sehr viel niedrigere Bandbreite. Auch stehen Möglichkeiten zum verdeckten Schlüsseltausch wie in Abschnitt 5.7.1 zur Verfügung, die dem Zensor verschlossen sind.

Dabei müssen sich die Parteien aber wieder einigen, woran sie z. B. bei dem in Abschnitt 5.7.1 und Beispiel 5.40 vorgestellten Protokoll erkennen, ob eine Broadcast-Sendung für den Schlüsseltausch relevant ist oder wirklich nur einem anderen Zweck dient. Jede Partei liefe sonst Gefahr, bei jeder Sendung unbeabsichtigt den vereinbarten Schlüssel zu ändern, also gar keinen normalen Sendungen mehr durchführen zu können. Auch hierüber wäre eine Einigung notwendig, die zwar eine deutlich niedrigere Bandbreite erfordert, die aber wieder vom Zensor abgehört werden kann.

Fazit: Der Zensor ist nicht absolut auszuschließen, aber man kann es ihm beliebig schwer machen. Der Zensor kann in der Realität die Parteien nicht so überwachen, daß überhaupt keine versteckte Einigung über einen Schlüssel oder die Anwendung von Chiffren möglich wäre, will er nicht jegliche Kommunikation schlechthin unterbinden. Damit hat der Zensor doch die schlechtere Position.

Bemerkung 5.20: Identität von Chiffraten und Klartexten

Eine Folge von Beweis 5.18 ist, daß nicht nur Chiffrate, sondern auch Klartexte nicht eindeutig als solche zu erkennen sind.

Wäre die Übertragung gewisser Daten strafbar, weil diese – aus welchen Gründen auch immer – als chiffriert angesehen würden, würde die Strafe

auch den treffen, der unbeabsichtigt und versehentlich einen damit identischen Klartext übertragen hat. Der Gesetzestreue muß also wissen, welche Übertragungen er zu vermeiden hat.

Als Beispiel sei angenommen, daß Datenpakete mit einer Länge von k Bit verschickt würden und jedes Datenpaket insgesamt als ein Zeichen aufgefaßt würde, jedes dieser Pakete also eines aus 2^k Zeichen darstellt.

Für jeden möglichen Wert dieser Datenpakete würde untersucht, ob seine Versendung zu einer Bestrafung führen würde oder nicht. Dies sei für n Pakete der Fall. Damit werden effektiv n Zeichen aus dem Zeichenvorrat entnommen. Es bleiben somit $2^k - n$ legale Zeichen und damit eine Paketkapazität, die von k auf $\log_2(2^k - n)$ Bit schrumpft.

Beide, der Gesetzestreue und der Gesetzesbrecher, müssen die verbotenen Zeichen meiden und die restlichen verwenden. Für beide ist die Kanalkapazität geschrumpft, aber für beide steht der übriggebliebene Kanal voll zur Verfügung.

Das Verbot hat also nichts als eine Reduktion der Kanalkapazität zur Folge.

Sobald der Zensor jedoch herausfindet, daß der Gesetzesbrecher mit den $2^k - n$ legalen Zeichen verbotene (weil chiffrierte) Nachrichten überträgt, wird er weitere n' Zeichen verbieten, die Zahl der zulässigen Zeichen also weiter auf $(2^k - n - n')$ reduzieren usw.

In der Folge muß der Zensor die Kommunikation ganz verbieten.

5.3.3 Entfernung kompromittierender Redundanz

In Beweis 5.18 wurde gezeigt, daß die Detektion verbotener Chiffren dann nicht möglich ist, wenn die volle Kanalkapazität ausgenutzt wird.

Folglich wird immer dann, wenn die Verwendung einer Chiffre erkennbar ist, nicht die volle Kanalkapazität genutzt, sondern kompromittierende Redundanz mitgeschleppt. Der Ausweg muß darin bestehen, diese Redundanz zu entfernen.

Die einfachste Form dieser Redundanz ist die in der Praxis häufig zu beobachtende Codierung nach einer vom Verschlüsselungsprogramm vorgegebenen Syntax, die eine Nachricht als mit diesem Programm verschlüsselt kennzeichnet, Hinweise zum Empfänger oder zur Schlüssellänge gibt, Kanalcodierungen vorgibt usw., und den Zweck hat, dem Empfänger die Handhabung zu erleichtern. Wird nur das reine Chiffrat ohne Zusätze usw. übertragen, ist bei Verwendung hochwertiger Chiffren eine Redundanz nicht mehr feststellbar. Da die Überlegungen aber grundsätzlich auch auf andere verbotene Übertragungen anwendbar ist, ist prinzipiell von einer in den verbotenen Übertragungen enthaltenen Redundanz auszugehen, die durch Datenkompression zu entfernen ist.

Die Detektion wird aber erst dann unmöglich, wenn auch die unverschlüsselten Übertragungen den Kanal voll ausnutzen. Sie müssen deshalb komprimiert werden.

Bemerkung 5.21:
Anforderung an das Kompressionsverfahren
Sobald der Zensor Redundanz in den erlaubten oder den unerlaubten Übertragungen findet, kann er mit dieser Kenntnis einen Detektor entwickeln. Der Verteidiger muß also mindestens auf dem Wissensstand des Angreifers über statistischen Eigenschaften seiner Datenübertragungen sein und seine Kompressionsverfahren ständig anpassen und verbessern.

Ein Kryptoverbot hat also die positive Nebenwirkung der Entwicklung verbesserter Kompressionsverfahren und damit einer besseren Ausnutzung der Übertragungskanäle.

Durch die Verwendung geeigneter Kompressionsverfahren macht der Verteidiger Klartext und Chiffrat ununterscheidbar.

5.3.4 Täuschung des Zensors durch falsche Redundanz

Die Entfernung jeder Redundanz und die volle Ausnutzung der Kanalkapazität macht die Detektion unmöglich.

Eine andere Verteidigungsstrategie ist es, Redundanz hinzuzufügen und die Übertragung gerade so zu gestalten, daß eine Detektion (scheinbar) leicht möglich ist, die Redundanz aber so zu konstruieren, daß der Detektor nur „erlaubten Klartext“ detektiert. Auch hierzu ist die Kenntnis der statistischen Modelle erlaubter und verbotener Übertragungen, die der Angreifer seinem Detektor zugrundelegt, notwendig. Diese Vorgehensweise wird üblicherweise auch als „steganographisch“ bezeichnet (vgl. Abschnitt 1.3).

Der Unterschied zu Abschnitt 5.3.3 liegt darin, daß erlaubte Nachrichten unverändert übertragen werden, während unerlaubte zunächst mit den „illegalen“ Kompressionsverfahren komprimiert und dann mit einem „legalen“ Dekompressionsverfahren wieder aufgeblasen werden. Die Art der Einbettung durch das Dekompressionsverfahren kann als *Syntax* aufgefaßt werden.

Beispiel 5.22:
Tarnung durch falsche Redundanz
Es wird ein sehr einfaches Beispiel betrachtet, in dem Bit-codierte Nachrichten übertragen werden sollen. Einige bestimmte Nachrichten gelten als verboten und sind zu vermeiden.

Es wird angenommen, es gäbe eine bool’sche Funktion `erlaubt(x)`, die zu jedem Zeitpunkt angeben kann, ob die bereits übertragene oder

empfangene Bitfolge zusammen mit dem nächsten Bit `x` eine verbotene Nachricht ergibt (oder zwangsläufig zu einer verbotenen Nachricht führt, d. h. daß alle Nachrichten, die mit dieser Bitfolge und `x` anfangen, verboten sind).

Ein einfacher Codierer für „illegale“ Nachrichten könnte so aussehen:

```
WHILE (noch Bits verfügbar)
  IF (erlaubt(0) AND erlaubt(1)) THEN
    SendeBit(LeseBit())
  ELSIF (erlaubt(0)) THEN
    SendeBit(0)        (* Füllmaterial *)
  ELSIF (erlaubt(1)) THEN
    SendeBit(1)        (* Füllmaterial *)
  ELSE
    Abbruch (* Fehler in Funktion "erlaubt" *)
```

Wie man leicht sieht, werden nur erlaubte Bitfolgen übertragen. Sind „0“ und „1“ erlaubt, kann ein Bit übertragen werden. Ist nur „0“ oder nur „1“ erlaubt, muß dieses Bit zur Umgehung des Verbotszustandes übertragen werden, kann aber keine Information übertragen. Gerät das Programm in den Zustand, in dem gar nichts mehr erlaubt ist, dann hätte die Funktion `erlaubt(x)` bereits mindestens einen Schritt früher das entsprechende Bit verhindern müssen, ist also fehlerhaft.

Ein passender Decodierer ist einfach, er muß nur lediglich die Bits, die als Füllmaterial dienten und keinen Informationsgehalt tragen, wieder ausfiltern:

```
WHILE (noch Bits verfügbar)
  IF (erlaubt(0) AND erlaubt(1)) THEN
    SchreibeBit(EmpfangeBit())
  ELSIF (erlaubt(x))
    EmpfangeBit()   (*  Füllmaterial ignorieren *)
```

Sofern dem Verteidiger das statistische Wissen des Angreifers zur Verfügung steht, kann er die Übertragung so gestalten, daß nur die „grüne Lampe“ leuchtet.

Bemerkung 5.23:
Gefahr falscher Verdächtigung
Ein Verbot der Übertragung chiffrierter (oder anderer verbotener) Nachrichten bringt die Verbesserung der Kompressionsverfahren mit sich und erschwert damit die Detektion.

Aus der Verbesserung der Kompressionsverfahren ergibt sich aber eine ganz andere Gefahr:

Je besser das Kompressionsverfahren für illegale Nachrichten ist, desto besser ist folglich die Fähigkeit des zugehörigen Dekompressors, aus beliebigen Daten (Rauschen) konsistente (d. h. mit der passenden Redundanz ausgestattete) und illegale Nachrichten zu „synthetisieren“[8].

Verfügt der *Zensor* über die Kompressions- und Dekompressionsprogramme, dann kann er den illegalen Dekompressor auf jeden Datenstrom anwenden und damit gegen jeden den (Schein-)Beweis einer illegalen Übertragung erbringen und ihm vorhalten, er habe diese illegale Übertragung durch Kompression geschützt, sei aber dabei ertappt worden.

5.4 Beschränkungen der Schlüssellänge

Eine Form der gesetzlichen Beschränkung der Datenverschlüsselung ist die Beschränkung der zulässigen Schlüssellänge der symmetrischen Chiffre und damit der Anzahl der möglichen Schlüssel, die zur Verschlüsselung verwendet werden dürfen. Der Effekt einer solchen Beschränkung kann – je nach verwendeter Chiffre, insbesondere bei Chiffren mit variabler Schlüssellänge – in einer über die Schlüsselkürzung hinausgehenden Schwächung der Chiffre selbst liegen, etwa wenn eine Chiffre mit zu großer Schlüssellänge auf eine kürzere Schlüssellänge „zurechtgestutzt“ wird, indem der lange Schlüssel aus dem kurzen durch Wiederholung oder Auffüllen mit Nullen gewonnen wird bzw. der lange Schlüssel durch Offenlegung der zusätzlichen Bits wieder geschwächt wird.

Das Ziel einer Beschränkung der Schlüssellänge liegt darin, den Schlüsselraum so zu verkleinern, daß mit akzeptablem Aufwand eine vollständige Suche, d. h. ein Ausprobieren jedes möglichen Schlüssels, erfolgen kann.

Die Sicherheit für den Überwachten beruht dabei auf der höchst fragwürdigen und keinesfalls überzeugenden Annahme, daß die zum Brechen des Schlüssels notwendige Rechenleistung einerseits für den legitim überwachenden Staat so billig ist, daß er einfach und im gewünschten Umfang Zugriff auf die Kommunikation erhält, während sie andererseits für unbefugte Angreifer zu teuer ist und dies sogar trotz der ständig steigenden Rechenleistung immer billigerer Rechner auch auf ausreichende Zeit bleiben soll.

Es sei angenommen, daß der Angreifer die Möglichkeit hat, eine Million speziell zum Angriff entworfene VLSI-Chips einzusetzen, die jeweils 500 Millionen Schlüssel pro

[8] Es mag derzeit noch technologisch weit hergeholt erscheinen, aber es muß durchaus in Betracht gezogen werden, daß gerade ein Verbot bestimmter Nachrichten somit letztlich sogar Synthesizer für eben diese Nachrichten hervorbringt, die mit beliebigen Zufallsdaten gefüttert werden können, und damit kontraproduktiv ist.

Sekunde testen können. Mit einer solchen Maschine lassen sich $2^{10} \cdot 2^{19} = 2^{29}$ Schlüssel *pro Sekunde* testen. In Tabelle 5.1 sind die vollständigen Suchzeiten für verschiedene Schlüssellängen aufgelistet (siehe auch [138, 135, 34]). Unberücksichtigt ist dabei die Detektion des Erfolges, die am einfachsten bei einer Known Plaintext-Attacke durch einfachen Vergleich zu erreichen ist.

Zeit	Bit (ca.)	Beispiel
1 ms	39	Amerik. Exportbeschränkung 40 Bit
1 Sekunde	49	
1 Minute	55	DES: 56 Bit
1 Stunde	61	
1 Tag	65	
1 Woche	68	
1 Monat	70	
1 Jahr	74	
10 Jahre	77	Skipjack: 80 Bit
$3 \cdot 10^{11}$ Jahre	112	3DES: 112 Bit
$2 \cdot 10^{16}$ Jahre	128	IDEA: 128 Bit
$7 \cdot 10^{54}$ Jahre	256	GOST: 256 Bit

Tabelle 5.1: Die Zeit, die 1 Million Prozessoren bei einer Rechenleistung von je $500 \cdot 10^6$ Schlüsseln pro Sekunde zum vollständigen Durchsuchen des Schlüsselraums benötigen. Die mittlere Rechenzeit hängt davon ab, wie viele Schlüssel gleichzeitig gebrochen werden sollen.

5.4.1 Informationstheoretische Betrachtungen

Wie aus den Bemerkungen 5.14, 5.15 und 5.16 hervorgeht, kann ein Angreifer, der über die Möglichkeit der vollständigen Durchsuchung des Schlüsselraumes verfügt, und die Wahrscheinlichkeitsverteilungen von Klartext und Schlüssel kennt, die Wahrscheinlichkeiten berechnen, daß zu einem gegebenen Chiffrat y ein Schlüssel k oder ein Klartext x gehören:

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x)}{p_{\mathcal{C}}(y)} \cdot p_{\mathcal{C}}(y|x) = p_{\mathcal{P}}(x) \cdot \frac{\sum\limits_{k \in \mathcal{K}: y = E_k(x)} p_{\mathcal{K}}(k)}{\sum\limits_{k \in \mathcal{K}} p_{\mathcal{K}}(k) \cdot p_{\mathcal{P}}(D_k(y))}$$

$$p_{\mathcal{K}}(k|y) = \frac{p_{\mathcal{K}}(k)}{p_{\mathcal{C}}(y)} \cdot p_{\mathcal{C}}(y|k) = p_{\mathcal{K}}(k) \cdot \frac{p_{\mathcal{P}}(D_k(y))}{\sum\limits_{k' \in \mathcal{K}} p_{\mathcal{K}}(k') \cdot p_{\mathcal{P}}(D_{k'}(y))}$$

bzw.

$$H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{K}) + H_a(\mathcal{P}) - H_a(\mathcal{C})$$

und

$$H_a(\mathcal{P}|\mathcal{C}) = H_a(\mathcal{K}|\mathcal{C}) - H_a(\mathcal{K}|(\mathcal{C}\mathcal{P}))$$

Ziel des Verteidigers ist es, daß der Angreifer aus dem Chiffrat möglichst wenig Information gewinnen kann, also $H_a(\mathcal{K}|\mathcal{C})$ und damit $H_a(\mathcal{P}|\mathcal{C})$ möglichst hoch zu treiben.

5.4.1.1 Entfernung der Schlüsselredundanz

Der naheliegendste Weg, $H_a(\mathcal{K}|\mathcal{C})$ hochzutreiben ist die Erhöhung von $H_a(\mathcal{K})$. Dummerweise ist $H_a(\mathcal{K})$ aber gerade durch die Begrenzung der Schlüssellänge nach oben beschränkt. Gerade wegen der kurzen Schlüssellänge ist es aber wichtig, diese Länge vollständig auszunutzen, $H_a(\mathcal{K})$ also möglichst nahe an diese Schranke zu bringen.

Dazu ist es notwendig, sehr gute Zufallszahlengeneratoren zu verwenden oder bei Abbildungen auf Paßworte auf ausreichende Länge zu achten.

Bei natürlichsprachlichen Paßworten und Phrasen kann ein Informationsgehalt von ca. 1 - 2 bit pro Zeichen angesetzt werden. Selbst bei einem äußerst kurzen Schlüssel von nur 40 Bit sollte deshalb (mit Sicherheitsreserve) ein Paßwort von ca. 40 bis 60 Zeichen gewählt werden.

5.4.1.2 Entfernung der Klartextredundanz

Ein anderer Weg $H_a(\mathcal{K}|\mathcal{C})$ hochzutreiben ist die Erhöhung von $H_a(\mathcal{P})$ und damit die Entfernung der Klartextredundanz durch geeignete Codierung, Kompression, Wahl von Protokollen usw.

Die Klartextentropie $H_a(\mathcal{P})$ ist dann optimal, wenn für jedes $x \in \mathcal{P}$ gilt: $p_{\mathcal{P}}(x) = \frac{1}{|P|}$

5.4.1.3 Unterschreiten der Unizitätslänge

Wie gezeigt wurde gilt

$$H_a(\mathcal{P}|\mathcal{C}) = H_a(\mathcal{K}) + H_a(\mathcal{P}) - H_a(\mathcal{C}) - H_a(\mathcal{K}|(\mathcal{C}\mathcal{P}))$$

Der Angreifer kann den Klartext anhand des Chiffrats im Mittel dann eindeutig bestimmen, wenn $H_a(\mathcal{P}|\mathcal{C}) = 0$, also

$$H_a(\mathcal{K}) + H_a(\mathcal{P}) = H_a(\mathcal{C}) + H_a(\mathcal{K}|(\mathcal{C}\mathcal{P})).$$

$H_a(\mathcal{K})$ und $H_a(\mathcal{K}|(\mathcal{CP}))$ sind in der Regel durch die Wahl der Chiffre festgelegt. Daher muß der Verteidiger Sorge tragen, daß

$$H_a(\mathcal{P}) \gg H_a(\mathcal{C}) + (H_a(\mathcal{K}|(\mathcal{CP})) - H_a(\mathcal{K})).$$

Das ist allerdings mit steigender Länge des Klartextes kaum durchzuhalten. Während $H_a(\mathcal{C})$ mit jedem Bit gnadenlos mitwächst, schleicht sich in $H_a(\mathcal{P})$ zwangsläufig Redundanz ein, sofern nicht gerade der seltene Fall vorliegt, daß eine perfekte Codierung gefunden wurde.

Die Länge des Quelltextes, bei der $H_a(\mathcal{P}|\mathcal{C}) = 0$ erreicht wird, wird als *Unizitätslänge* bezeichnet. Besteht der Klartext z. B. aus ASCII-codiertem natürlichsprachlichem Text, ist von einer Entropie von nur ca. 1 - 1,5 bit pro Byte auszugehen. Bei einer Schlüssellänge von 40 Bit wäre die Unizitätslänge schon nach etwa 7 Zeichen erreicht.

Wenn die Schlüssellänge gesetzlich beschränkt, aber keine Mindestredundanz im Klartext vorgeschrieben ist, können die Nachrichten in entsprechend viele kleine Teilklartexte aufgespalten werden.

5.4.1.4 Perfekte Sicherheit

Der Angreifer kann mit dem Chiffrat überhaupt nichts anfangen, wenn es ihm nichts über den Klartext oder den Schlüssel verrät, wenn nämlich $H_a(\mathcal{P}|\mathcal{C}) = H_a(\mathcal{P})$ und $H_a(\mathcal{K}|\mathcal{C}) = H_a(\mathcal{K})$.

Daraus ergibt sich für die Sicherheit des Klartextes

$$0 = H_a(K) - H_a(C) - H_a(\mathcal{K}|(\mathcal{CP}))$$

bzw. für die Sicherheit des Schlüssels

$$0 = H_a(P) - H_a(C)$$

Daraus lassen sich zwei Anforderungen ablesen:

- Zur Sicherheit des Schlüssels muß $H_a(P) = H_a(C)$ gelten, d. h. der Klartext kann zwar nicht mehr Information enthalten als das Chiffrat, weil sonst die Chiffre verlustbehaftet wäre, er darf aber auch nicht weniger Information enthalten (vgl. Beweis 5.18).
- Zur Sicherheit des Klartextes muß $H_a(K) - H_a(\mathcal{K}|(\mathcal{CP})) = H_a(C)$ gelten, der Schlüssel[9] muß also *mindestens* so lange sein wie das Chiffrat. Ist durch einen beliebigen Klartext und ein beliebiges Chiffrat nicht eindeutig ein Schlüssel festgelegt, muß er sogar *länger* sein!

Auch hier ist bei einer Beschränkung der Schlüssellänge wieder die Unterteilung der Nachricht in kleine Einzelnachrichten in Betracht zu ziehen.

[9] Es wird unterstellt, daß die Schlüsselentropie gleich der Schlüssellänge ist.

5.4.1.5 Phantomredundanz

Ein Angreifer, der eine vollständige Suche durchführt, wird normalerweise alle die $x' \in \mathcal{P}$ als möglichen Klartext in Betracht ziehen und weiterer Prüfung unterziehen, für die

$$p_{\mathcal{P}}(x'|y) \approx \max_{x \in \mathcal{P}} p_{\mathcal{P}}(x|y)$$

gilt.

Der Verteidiger kann nun eine „falsche Fährte“ legen, indem er seinen Klartext $x \in \mathcal{P}$ so konstruiert und mit einem Schlüssel $k \in \mathcal{K}$ chiffriert, daß es zum Chiffrat $y \in \mathcal{C}$ eine zweiten Schlüssel $k' \in \mathcal{K}$ gibt mit

$$p_{\mathcal{P}}(D_{k'}(y)|y) \gg p_{\mathcal{P}}(x|y), \quad D_{k'}(y) \neq x.$$

Der Angreifer wird dann den Phantomtext $x' := D_{k'}(y)$ für den Klartext halten, sofern er seinem $p_{\mathcal{P}}$ vertraut und x' nicht auffällig viel Rauschen enthält.

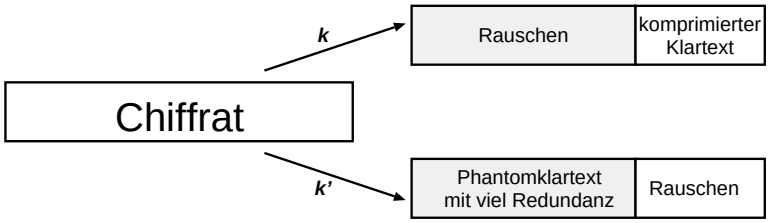


Abbildung 5.3: Durch den Phantomklartext mit hoher Redundanz wird der Angreifer zu einem falschen Schlüssel k' gelockt. Mit dem echten Schlüssel k findet er praktisch keine Redundanz und hält dies für einen Fehlversuch.

5.4.1.6 Blendungsentropie

Der Angreifer, der eine vollständige Suche durchführt, wird nicht in jedem Fall gleichzeitig eine Tabelle führen können, in der er für alle versuchten Schlüssel die im damit erhaltenen Dechiffrat gefundene Redundanz zu notieren und seine Auswahl zu skalieren.

Er wird im Normalfall eine gewisse Vorstellung davon haben, welche Werte von $p_{\mathcal{P}}$ als „Treffer“ anzusehen sind und nach solchen Werten suchen. Gelingt dem Verteidiger aus irgendwelchen Gründen keine Kompression, kann er die Redundanz seines Klartextes verrauschen. Da das naheliegenderweise verlustfrei geschehen soll, muß die Kapazität – und damit die Länge des Chiffrats – so hoch sein, daß Rauschen und Klartextentropie übertragen werden können. Damit sinkt der Anteil der Redundanz an der Gesamtnachricht und die Wahrscheinlichkeit, als „Treffer“ detektiert zu werden.

Bemerkung 5.24:
$H_a(\mathcal{C}|(\mathcal{KP})) \neq 0$

In Bemerkung 5.15 wurde angenommen, daß das Chiffrierverfahren eindeutig ist und das Chiffrat durch Klartext und Schlüssel festgelegt ist, also $H_a(\mathcal{C}|(\mathcal{KP})) = 0$ ist.

Bei der in diesem und dem vorhergehenden Abschnitt erwähnten Blendungsentropie und der Phantomredundanz ist dies nicht mehr der Fall. Solange der Angreifer das genaue Dechiffrierverfahren nicht kennt, sind die von dieser Annahme abgeleiteten Gleichungen nicht mehr zutreffend.

5.4.2 Schlüssellose Chiffren

Der Zweck einer gesetzlichen Beschränkung der Schlüssellänge ist es, die vollständige Suche mit vertretbarem Aufwand möglich zu machen.

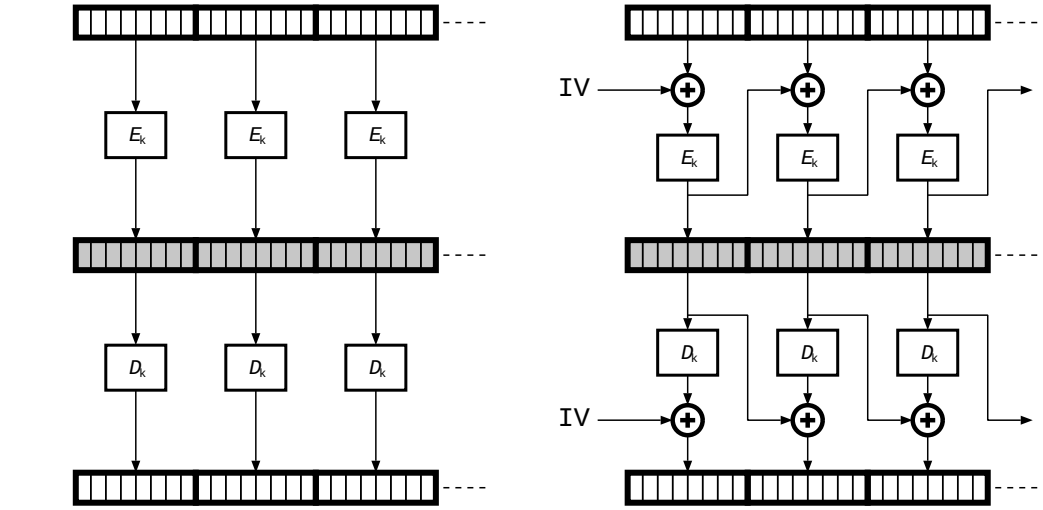
Bei der vollständigen Suche werden normalerweise aber nicht mit jedem Durchlauf ganze Nachrichten entschlüsselt, sondern nur Teilabschnitte der Nachricht, die oft nur das etwa 1 bis 3-fache der Blockgröße betragen, und zu denen Vermutungen über den möglichen Klartext bestehen. Daraus ergibt sich ein enormer Geschwindigkeitsvorteil gerade für den Angreifer, der mit den Mitteln staatlicher Nachrichtendienste angreift, und der nicht mehr mit einer flexiblen und programmierbaren, aber langsamen und teuren Maschine angreifen muß, sondern stattdessen mit speziellen, auf das Problem zugeschnittenen Rechenwerken in Form von programmierten FPGAs oder eigens angefertigten Integrierten Schaltungen arbeiten kann. Damit wird die Rechenleistung immens erhöht bzw. der Preis für das Brechen einer Chiffre drastisch gesenkt[10] (vgl. Tabelle 5.1 und [135, 138, 34, 89]). Die wirksamste Maßnahme gegen einen solchen „Brute Force-Angriff“ ist die Erhöhung der Schlüsselentropie, was aber bei gesetztlich beschränkter Schlüssellänge illegal wäre. Es gibt aber auch andere Wege, den effizienten Angriff über spezifische Rechenwerke zu erschweren.

Die bislang üblichen vier Betriebsarten „Electronic Codebook“ (ECB), „Cipher Block Chaining“ (CBC), „Output Feedback“ (OFB) und „Cipher Feedback“ (CFB), die in Abbildung 5.4 dargestellt werden, sind nicht sonderlich geeignet, einen Angriff wie den beschriebenen abzuwehren.

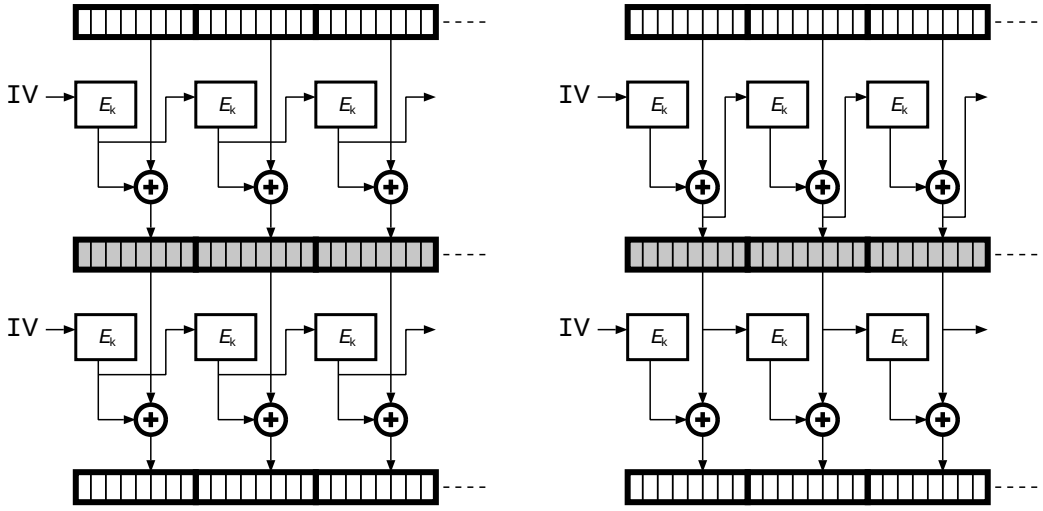
Alle vier Betriebsarten weisen bestimmte, konstruktionsbedingte Eigenschaften auf, die in diesem Kontext als Schwäche angesehen werden können.

Eine dieser Eigenschaften ist, daß mit den Betriebssarten eine Stromchiffre nachgebildet wird und die Nachricht schon teilweise fertig chiffriert werden kann, bevor die ganze Nachricht in der Chiffriereinrichtung angelangt ist. Die Chiffrierung jedes Datenblockes ist von den nachfolgenden Datenblöcken völlig unabhängig. Eine „Known

[10] Dabei wird angenommen, daß die Anlagen ausgelastet und nicht nur einmalig verwendet werden



(a) ECB (b) CBC



(c) OFB (d) CFB

Abbildung 5.4: Die vier üblichen Betriebsarten für Blockchiffren: Electronic Codebook (a), Cipher Block Chaining (b), Output Feedback (c) und Cipher Feedback (d). Die obere Hälfte der Grafiken stellt die *Verschlüsselung* dar, die untere die *Entschlüsselung*. Die weiß unterlegten Kästchen symbolisieren die Zeichengruppen des *Klartextes*, die grauen die des *Chiffrats*. E_K steht für die Verschlüsselung durch die Chiffre, D_K für die Entschlüsselung und K für den Schlüssel (OFB und CFB verwenden die Chiffre nur in Verschlüsselungsrichtung). Das Plus-Zeichen steht für eine XOR-Verknüpfung, IV ist ein Initialisierungswert.

Plaintext“-Attacke, bei der der Anfang des Klartextes bekannt ist, kann mit dem Anfang des Chiffrats durchgeführt werden, ohne den Rest des Klartextes oder des Chiffrats zu beachten.

Eine zweite (sehr ähnliche) Eigenschaft ist, daß der Zustand der Chiffriereinrichtung bei den meisten Betriebsarten nur vom Schlüssel und z. T. vom bereits erzeugten Chiffrat abhängen, was dem Angreifer bekannt ist. Auch hier ist die Folge eine Kontextunabhängigkeit, die dazu führt, daß eine „Brute Force“-Attacke auch gegen einen kleinen Teil des Chiffrats ausgeführt werden kann:

- In der Betriebsart ECB ist die Verschlüsselung völlig kontextunabhängig und hängt nur vom Schlüssel ab. Der Angreifer braucht nicht einmal die benachbarten Chiffrat-Blöcke zu betrachten.
- Bei CBC und CFB hängt die Verschlüsselung vom Schlüssel und dem unmittelbar zuvor übertragenen Chiffratblock ab, der dem Angreifer bekannt ist (es sei denn, es handelt sich um den ersten Block und der Initialisierungsvektor ist geheim, was hier aber im Rahmen der gesetzlichen Schlüssellängenbegrenzung ausgeschlossen wird).
- Beim OFB hängt der Zustand der Chiffriereinrichtung vom Schlüssel und von der Zahl der Blockdurchläufe ab, damit also von der Position des Blockes innerhalb der Nachricht, nicht aber von der Nachrichtenentropie selbst.

  Weil der Angreifer hier nur beim ersten Block der Nachricht die Eingabe der Verschlüsselungsfunktion kennt, muß er bei der Suche im Schlüsselraum für jeden Schlüssel die Verschlüsselungsfunktion mehrfach aufrufen, und zwar in Abhängigkeit von der Position des Blockes in der Nachricht.

  Der Angreifer muß jedoch keinen Speicheraufwand betreiben, denn er braucht auch hier nur eine konstante und von der Länge unabhängige Zahl von Registern (und natürlich einen ausreichend langen Zähler).

Eine Verbesserung besteht offensichtlich darin, die Nachricht so zu bearbeiten, daß sie nicht mehr ausschnittsweise, sondern nur noch in ihrer gesamten Länge dechiffriert werden kann. Damit bleibt zwar der Schlüsselraum konstant, denn bei einer Beschränkung auf n Bit gibt es zu einem gegebenen Chiffrat noch immer nur 2^n potentielle Klartexte. Aber der Aufwand zur Erfolgdetektion hängt nun auch von der Nachrichtengröße ab.

Um dies zu erreichen bieten sich zwei Wege an: Geänderte Betriebsarten und ein von der eigentlichen Verschlüsselung getrennter Arbeitsschritt. Es wird zunächst der separate Arbeitsschritt betrachtet. Damit der Angreifer diesen Arbeitsschritt nicht nur einmal, sondern für jeden versuchten Schlüssel rückgängig zu machen hat, muß der Sender ihn *vor* der Verschlüsselung vornehmen. An diesen Arbeitsschritt können im Prinzip die gleichen Anforderungen wie an eine Chiffre gestellt werden; der Unterschied liegt im Fehlen eines Schlüssels.

Definition 5.25:
„Schlüssellose Chiffre“
Eine Abbildung $f : \{0,1\}^* \rightarrow \{0,1\}^*$ (oder auf einem anderen Alphabet) heißt „Schlüssellose Chiffre“, wenn sie folgende Bedingungen erfüllt:

- Es gibt eine inverse Abbildung f^{-1}, die mindestens die gleiche Komplexität wie f aufweist.
- $f(x)$ und $f^{-1}(x)$ sind berechenbar für jedes x endlicher Länge.
- f ist längenerhaltend, d. h.
  $\forall x \in \{0,1\}^* : x \in \{0,1\}^n \Leftrightarrow f(x) \in \{0,1\}^n$.
  Aus Gründen der Implementierung sei aber erleichternd erlaubt, daß f nur für eine bestimmte Blockgröße definiert ist, d. h. $n \in k\mathbb{N} + q$, sofern es eine weitere, invertierbare Abbildung gibt, die jedes x beliebiger Länge auf ein x' geeigneter Blocklänge transformiert und dabei dem Angreifer über die Struktur des x' die Erfolgsdetektion nicht ermöglicht.
- f weist den sog. „Lawineneffekt“ auf, d. h. wenn man an einem beliebigen x ein beliebiges Bit ändert, dann ändert sich in $f(x)$ und $f^{-1}(x)$ jedes Bit mit einer Wahrscheinlichkeit von je 50%. Das bedeutet, daß in f und f^{-1} jedes Ausgangsbit von jedem Eingangsbit abhängt.

Beispiel 5.26:
Eine schlüssellose Chiffre
Zur Veranschaulichung wird eine etwas grobschlächtige Funktion betrachtet. Abbildung 5.5 zeigt die ersten zwei Arbeitsschritte der Funktion.

Die Nachricht wird in Blöcke unterteilt. Der Reihe nach wird jeder Block (ähnlich ECB) verschlüsselt. Dabei dient eine kryptographische Hash-Summe der anderen Blöcke jeweils als Schlüssel. Die verwendete Chiffre sollte eine Schlüssellänge aufweisen, die der Länge des Hash-Wertes nahekommt; sie kann die gesetzliche Höchstlänge weit überschreiten, weil hier keine geheime Schlüsselentropie verwendet wird.

Wie man leicht sieht, hängt nach einem solchen Arbeitsschritt der verschlüsselte Block von jedem Bit aller anderen Blöcke ab, denn jedes Bit des Hash-Wertes hängt von jedem dieser Bits ab und bei Verwendung einer geeigneten Chiffre hängt jedes Bit des Chiffrats von jedem Bit des Schlüssels ab. Da er bei einer guten Chiffre außerdem von jedem Bit des Klartextes abhängt, hängt jedes Bit des Ergebnisses auch von jedem Bit des eigenen Blockes ab.

Wird als Verschlüsselungsfunktion jedoch nur eine sehr schwache Funktion gewählt (z. B. Exklusives Oder), dann kann eine starke Durchmischung

durch mehrfaches Anwenden der Funktion erreicht werden. Nach dem ersten Durchlauf hängt dann jedes Bit nur von den Bits aller anderen Blöcke ab, dadurch aber nach dem zweiten Durchlauf aber auch von allen Bits des eigenen Blockes.

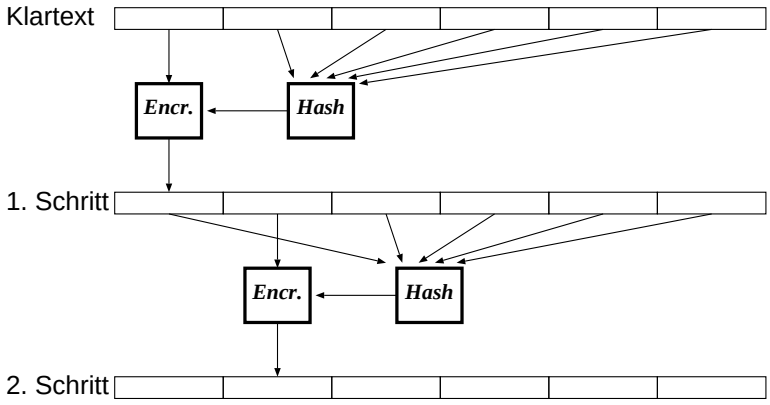


Abbildung 5.5: Ein Beispiel für eine „Schlüssellose Chiffre“. Gezeigt werden die ersten zwei Schritte. Jeder Block der Nachricht wird der Reihe nach verschlüsselt, wobei jeweils der Hash-Wert aller anderen Blöcke als Schlüssel dient. Die Schlüssellänge der verwendeten Chiffre kann weit über dem gesetzlichen Gebot liegen, weil keine geheime Schlüsselentropie verwendet wird.

Bemerkung 5.27:
Wirkung „schlüsselloser Chiffren“
Die Verwendung einer solchen Funktion kann und soll den Schlüsselraum für die gesamte Nachricht nicht vergrößern.

Wird aber statt der gesamten Nachricht mit n Bit nur ein Teil der Nachricht mit k Bit betrachtet, dann dann wirkt sich der Rest der Nachricht wie eine zusätzliche Portion Schlüsselentropie aus, d. h. der Schlüsselraum wächst aus der Sicht des Angreifers auf das bis zu 2^{n-k}-fache an.

Wie stark dieser Anstieg tatsächlich verläuft, hängt von der Qualität der Funktion ab. Im in Abbildung 5.5 gezeigten Beispiel kann die zusätliche Entropie bei der Betrachtung eines einzelnen Blockes nur die Länge des Schlüssels der zur Durchmischung eingesetzten Chiffre betragen, auch wenn der Rest der Nachricht deutlich länger ist.

Bemerkung 5.28:
Qualitative Unterscheidung vom längeren Schlüssel
Wird durch die Nachrichtengröße und die Durchmischung der Aufwand gegenüber dem Testen eines einzelnen Blocks z. B. vertausendfacht, kann

dies durchaus mit einem Gewinn von 10 Bit Schlüsselentropie verglichen werden.

Es wäre aber ein Trugschluß, dies mit der Sicherheit zu vergleichen, die ein tatsächlich längerer Schlüssel bietet.

Zwar steigt der Aufwand des Angreifers, aber in genau dem gleichen Maß steigt auch der Aufwand für Sender und Empfänger. Die befugten Parteien haben also keinen *komplexitätstheoretischen* Vorsprung gegenüber dem Angreifer erzielt. Der Angreifer muß nach wie vor genau einmal den Schlüsselraum durchlaufen, dessen Größe unverändert ist.

Der vorgestellte Vorgehensweise ist damit nicht als *kryptographisch* anzusehen, denn es fehlt am Geheimnis und es fehlt am komplexitätstheoretischen Vorsprung. Genau das ist aber auch unerwünscht, denn gerade das wäre ja ein Verstoß gegen ein Verbot (und außerdem mit einer stärkeren Chiffre leichter zu erreichen).

Das Verfahren nimmt dem Angreifer aber einen gewissen *technologischen* Vorsprung, indem es den Einsatz einfacher, billiger und schneller Schaltungen erschwert oder verhindert. Die Vorgehensweise ist deshalb als *Verschleierung* (s. Abschnitt 3.9) anzusehen.

Bemerkung 5.29: Abgrenzung zum Shared Secret-Schema

Schlüssellose Chiffren und Shared Secret-Schemen weisen auf den ersten Blick gewisse Ähnlichkeit auf: Beide haben zum Ziel, eine Nachricht so zu verteilen, daß ein Angreifer mit kleinen bzw. zu wenigen Teilen nichts oder nur wenig anfangen kann.

Es bestehen aber erhebliche Unterschiede:

- Shared Secret-Schemen sind Schwellwert-Verfahren, es gilt alles oder nichts.

  Für Schlüssellose Chiffren gilt: Je weniger man hat, desto mehr fehlt einem.

- Bei Shared Secret-Schemen sollte jeder Teil die gleiche Länge (Entropie) wie der Klartext haben, die Größe aller bestehenden oder benötigten Teile ist also ein Vielfaches.

  Schlüssellose Chiffren sind längenerhaltend.

- Shared Secret-Schemen sind auf eine bestimmte Aufteilung festgelegt, die der Verteidiger vornehmen muß.

  Schlüssellose Chiffren sind unabhängig von der konkreten Aufteilung, wirken also auch bei einer beliebigen Aufteilung durch den Angreifer.

- Die Sicherheit von Shared Secret-Schemen hängt davon ab, *wieviele Teile* der Angreifer angreift, nicht aber wieviel Information er insgesamt erhalten hat. Hat er bei einem n-aus-m-Schema von n Teilen je ein Bit in Erfahrung gebracht, dann könnte er im Prinzip[11] daraus ein Bit des Klartextes gewinnen.
- Zur Erzeugung von Shared Secret-Teilen ist eine Entropiequelle notwendig (Zufallszahlengenerator). Schlüssellose Chiffren benötigen diese gerade nicht.

Schlüssellose Chiffre und Shared Secret-Schema sind also funktional nicht deckungsgleich. Sie können sich aber sehr gut ergänzen: Wird die Nachricht mit der Schlüssellosen Chiffre „grundiert“, dann hält das Shared Secret-Schema besser (s.o.).

Die Durchmischung muß nicht notwendigerweise völlig von der Verschlüsselung getrennt werden, sondern kann mit dieser verschmelzen.

So kann die Verschlüsselung in die Durchmischung eingefügt werden. Bei dem in Beispiel 5.26 gezeigten Verfahren könnte etwa der Hash-Wert zusätzlich zu den übrigen Blöcken auch den Schlüssel umfassen[12] („Key seeded hash value“); ein getrennter Verschlüsselungsschritt wäre dann nicht mehr nötig.

Bemerkung 5.30:
Hash-Verfahren als Chiffre
Damit ist indirekt auch gezeigt, daß jedes qualitativ hochwertige Verfahren zur Berechnung von Hash-Werten als symmetrische Chiffre genutzt werden kann.

Umgekehrt kann eine Durchmischung aber auch als Teil der Verschlüsselung durchgeführt werden, sofern in Abweichung von den üblichen Betriebsarten eine Durchmischung der gesamten Nachricht gewährleistet wird.

Beispiel 5.31:
CBC mit vollständiger Durchmischung
Abbildung 5.6 zeigt eine Abwandlung der CBC-Betriebsart: Statt nur auf den nachfolgenden Block wird das Ergebnis einer Blockverschlüsselung auf alle anderen Blöcke aufaddiert.

Zunächst erscheint das nicht hilfreich. Die Additionen „links unter der E-Diagonalen“ lassen sich trivial abstreifen. Mit den so erhaltenen Werten ist

[11] Ob, wann und wie er dies kann, hängt vom Verfahren ab. Kann er dies nicht, dann ist das eine Eigenschaft des speziellen Verfahrens, nicht des Shared Secret-Prinzips selbst.

[12] Es gibt auch Hash-Verfahren, die einen Schlüssel verwenden, z. B. die in GOST R34.11-94 [108] definierte Betriebsart.

die vollständige Suche praktisch ebenso einfach durchzuführen wie bei einem normalen CBC. Der Grund liegt darin, daß der Angreifer das Chiffrat und damit die in der Abbildung unten liegenden Blöcke kennt.

Wird dieser Schritt aber mehrfach angewandt oder durch einen zusätzlichen ECB-Schritt abgeschlossen, dann kennt der Angreifer die in der Abbildung unten liegenden Blöcke nicht mehr, denn sie sehen für jeden möglichen Schlüssel anders aus.

Da der Angreifer für die vollständige Suche mindestens einen Block vom Chiffrat zum Quelltext durchprobieren muß und zu dessen Dechiffrierung alle anderen Blöcke benötigt werden, muß der Angreifer für jeden Schlüssel die Nachricht in der gesamten Breite bearbeiten.

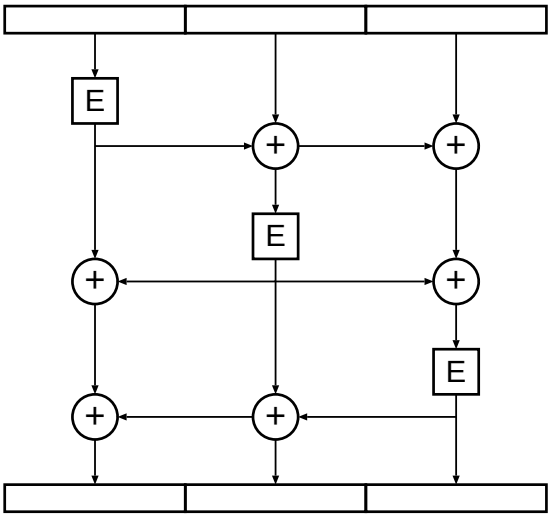


Abbildung 5.6: Eine Variation des CBC mit verstärkter Durchmischung. Gezeigt wird ein Durchlauf des Verfahrens am Beispiel einer Nachricht, deren Länge der dreifachen Blocklänge entspricht. Wie bei CBC auch wird der Reihe nach jeder Block verschlüsselt, das Blockchiffrat jedoch nicht nur auf den nachfolgenden, sondern auf alle anderen Blöcke bitweise aufaddiert.
Der gezeigte Einzelschritt bringt so noch keinen Sicherheitsvorteil: Die Summen links unter der „E-Diagonalen“ lassen sich trivial abstreifen, die oberhalb der Diagonalen stellen keine Behinderung der vollständigen Suche dar. Die Stärke liegt in der Kaskadierung des Verfahrens.

Bemerkung 5.32:
Aufwandsbetrachtung zu Schlüssellosen Chiffren
Bei den in den Abbildungen 5.5 und 5.6 gezeigten Verfahren wurde Wert

auf die einfache Darstellung der zugrundeliegenden Idee gelegt, nicht auf die Effizienz des Verfahrens. Beide Verfahren haben offensichtlich einen Aufwand von $O(n^2)$, was bei der Anwendung auf lange Nachrichten zu einem zu hohem Aufwand führt. Auf den ersten Blick könnte man dem entgegenhalten, daß auch dem Angreifer ein entsprechender Aufwand entsteht; dieses Argument ist aber nicht haltbar.

Der Angreifer hat die Möglichkeit, äquivalente Verfahren mit niedrigerem Aufwand zu suchen. Deshalb muß auch der Verteidiger danach suchen.

Außerdem verfügt der Angreifer regelmäßig über eine sehr hohe Rechenleistung. Das Mittel, den Wert dieser Rechenleistung durch Erhöhung des Aufwandes zu senken, ist die (verbotene) Steigerung der Schlüssellänge.

Ziel der Schlüssellosen Chiffren ist es, den *Speicheraufwand* und die *Komplexität der Maschine* des Angreifers hochzutreiben und Angriffe auf Ausschnitte der Nachricht zu erschweren. Daher stellt es keine Schwächung dar, den Aufwand zu verbessern.

Der Algorithmus einer Schlüssellosen Chiffre muß so beschaffen sein, daß jedes Bit des Eingangs auf jedes Bit des Ausgangs einwirken kann (vgl. Definition 5.25). Da die Breite der Register der hier in Betracht kommenden Rechenmaschinen von fest begrenzter Länge ist, die Nachrichten aber beliebig lange sein können, ist von einer wie auch immer gearteten Iteration über die Zeichen der Nachricht auszugehen. Damit beträgt der Aufwand mindestens $O(n)$.

Zu berücksichtigen ist aber, daß mit einer solchen einfachen Iteration eine Schlüssellose Chiffre nicht implementiert werden kann, weil dabei die Bits des Ausgangs nur von den zeitlich früher bearbeiteten Daten, nicht aber von den später zu bearbeitenden Daten abhängen können. Der Aufwand muß daher größer als $O(n)$ sein.

Es wird beispielhaft das in Abbildung 5.6 dargestellte Verfahren betrachtet. Der Aufwand des Verfahrens soll durch Rekursion verbessert werden. Wie leicht zu sehen ist, gibt es eine „Diagonale“ aus Verschlüsselungsschritten mit fester Blockgröße und die Addition der Ergebnisse rechts oberhalb dieser Diagonalen und links unterhalb derselben. Das Verfahren soll rekursiv in zwei Schritte unterteilt werden, was in Abbildung 5.7 dargestellt wird. Das Verfahren aus Abbildung 5.6 wird dabei durch einen diagonalen Strich dargestellt.

In einem ersten Schritt wird die erste Hälfte der Nachricht vollständig bearbeitet. Im zweiten Schritt werden die akkumulierten Summanden als konstanter Wert auf die zweite Hälfte der Nachricht addiert (mit linearem Aufwand). Im dritten Schritt wird die zweite Hälfte der Nachricht bearbeitet und im vierten Schritt werden die Summanden aus dem dritten Schritt nunmehr auf die erste Hälfte der Nachricht addiert.

Daraus ergibt sich $O(2n) = 2O(n) + 2n$ und damit $O(n) = n \log n$.

Grundsätzlich bieten sich für die Schlüssellosen Chiffren alle Butterfly-ähnlichen Strukturen an, womit sich ein Aufwand von $O(n) = n \log n$ als erreichbare untere Schranke für Schlüssellose Chiffren abschätzen läßt.

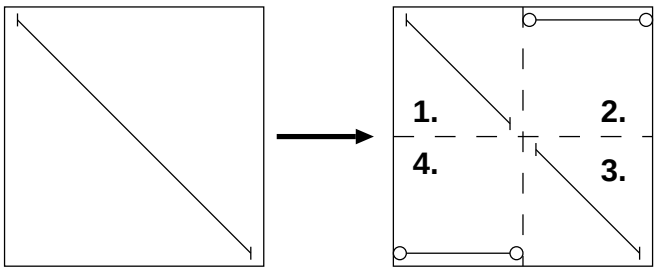


Abbildung 5.7: Rekursive Zerlegung des Verfahrens aus Abbildung 5.6. Der Aufwand wird in Bemerkung 5.32 erörtert.

5.4.3 Verkürzung der Schlüssellänge ohne Kenntnis des Senders

In den beiden vorhergehenden Abschnitten wurde der Fall einer allgemein bekannten (gesetzlichen) Beschränkung der Schlüssellänge betrachtet.

Es sind auch verdeckte Methoden der Schlüsselverkürzung denkbar:

Reduktion der Schlüsselentropie

Schlüssel*länge* ist nicht gleich Schlüssel*entropie*. Zur Erzeugung des Schlüssels wird eine Entropiequelle – sprich: Zufallszahlengenerator – hoher Qualität benötigt. Gelingt es dem Angreifer, dem Verteidiger eine schlechte Entropiequelle unterzuschieben, wird die Schlüsselkapazität nicht voll ausgenutzt. Der Verteidiger glaubt, einen Schlüssel mit einer der Länge entsprechenden Entropie zu benutzen, der in Wirklichkeit eine geringere Entropie hat.

Reduktion der Schlüsselrelevanz

Ist dem Verteidiger der genaue Aufbau des Chiffrierverfahrens nicht bekannt, kann er nicht unmittelbar beurteilen, in welcher Weise die Schlüsselentropie in den Chiffriervorgang einfließt. Das ist insbesondere bei allen „Black Box“-Verfahren der Fall.

Der Verteidiger kann hier nur in geringem Umfang Versuche anstellen, beispielsweise ob bei festem Klartext jedes Chiffratbit mit einer Wahrscheinlichkeit von 50% kippt, wenn ein beliebiges Bit des Schlüssels geändert wird.

Während der Schlüsselaufbereitungsphase kann aber problemlos ein großer Teil der Entropie so entfernt werden, daß dies nur mit großem Aufwand nachgewiesen werden kann.

Wird in der „Black Box“ zunächst eine (einfache) kryptographische Hashsumme des Schlüssels gebildet und von dieser nur eine kleiner Teil verwendet, zeigt die Box nach außen hin die Eigenschaften eines mangelfreien Systems. Der Benutzer kann mit einfachen Tests keine Fehlfunktion feststellen und insbesondere die Schlüsseläquivalenzklassen nicht feststellen.

Der Angreifer, dem eine Version der Box ohne die Schlüsselaufbereitung zur Verfügung steht, kann eine vollständige Suche direkt über den Äquivalenzklassen ausführen.

5.5 Protokolle mit Schlüsseloffenlegung

Ein wichtiger Ansatzpunkt staatlicher Kommunikationsüberwachung sind die symmetrischen Chiffren, weil diese beim derzeitigen Stand der Technik zum Verschlüsselung der eigentlich für den Staat interessanten Informationen verwendet werden. Der Staat kann also ein erhebliches Interesse daran haben, daß nur solche Chiffren Verwendung finden, die ihn beim Zugriff auf die Daten nicht allzu sehr behindern.

Wenn der Staat nun die Verwendung solcher Chiffren durchsetzen will, dann muß er auch verhindern, daß der unwillige Bürger die Schwächung wieder entfernt oder eine „kompatible“ starke Version baut, oder daß er die Schwächung überhaupt erst erkennt. Das ist praktisch – von der Ausnahme der freiwilligen Kooperation der Bürger abgesehen – nur realisierbar, wenn der Verschlüsselungsalgorithmus der Chiffre geheim ist und die Chiffriereinrichtung als fest verschlossene „Black Box“ bereitgestellt wird.

Die Publikation einer geschwächten Chiffre, deren Schwäche auch fachkundigen Bürgern mit hoher Wahrscheinlichkeit verborgen bleiben soll, würde einen erheblichen wissenschaftlichen Vorsprung des Staates gegenüber der Öffentlichkeit voraussetzen[13].

5.5.1 Offenlegung des Schlüssels mit Kenntnis des Senders

Der einfachste Fall liegt vor, wenn die Tatsache einer Schlüsseloffenlegung nicht verheimlicht werden muß, weil dann das Verfahren die Anzeichen einer Schlüsseloffenlegung offen tragen kann und auf die in den beiden nachfolgenden Abschnitten dargestellten Kunstgriffe verzichtet werden kann. Stattdessen wird „offiziell“ ein Kanal

[13] Womit ausdrücklich nicht gesagt wird, daß es keine Staaten gäbe, die diesen Vorsprung haben könnten.

geringer Bandbreite zum Staat hergestellt und auf diesem der Schlüssel (oder ein Teil dessen) dem Staat mitgeteilt.

Als einfaches Beispiel kann hier die in den Export-Versionen mancher kommerzieller amerikanischer Produkte verwendete Offenlegung dienen: Dabei wird z. B. eine Chiffre mit einer Schlüssellänge von 64 Bit verwendet. An jede verschlüsselte Nachricht bzw. jede Datei wird ein Feld angehängt, das 24 Bit dieses Schlüssels enthält, und zwar wiederum verschlüsselt mit dem öffentlichen Schlüssel des Staates. So muß der gemeine Angreifer 64 Bit brechen, während der Staat nur noch 40 Bit brechen muß, was mit modernen Mitteln kaum ein Hindernis mehr darstellt.

Ein etwas komplizierteres Beispiel ist der „Clipper Chip“, mit dem die amerikanische Regierung versuchte, ein Verschlüsselungsverfahren mit Offenlegung des Sitzungsschlüssels zu etablieren. Eine genaue Beschreibung ist z. B. in [65] zu finden.

Dieser Chip stellt zunächst die Implementierung einer gewöhnlichen – aber geheimgehaltenen – Blockchiffre mit einer Schlüssellänge von 80 Bit dar (der sog. „Skipjack“-Algorithmus). Jeder Chip hat eine eindeutige 32 Bit Seriennummer und einen individuellen „Unit Key“, der unauslesbar im Chip untergebracht und sonst nur dem Staat bekannt ist. Außerdem enthält er einen weiteren Schlüssel, den sog. „Family Key“, der ebenfalls unauslesbar ist und nur dem Staat bekannt ist, der aber bei allen Chips, die in einem Land verkauft werden, gleich ist.

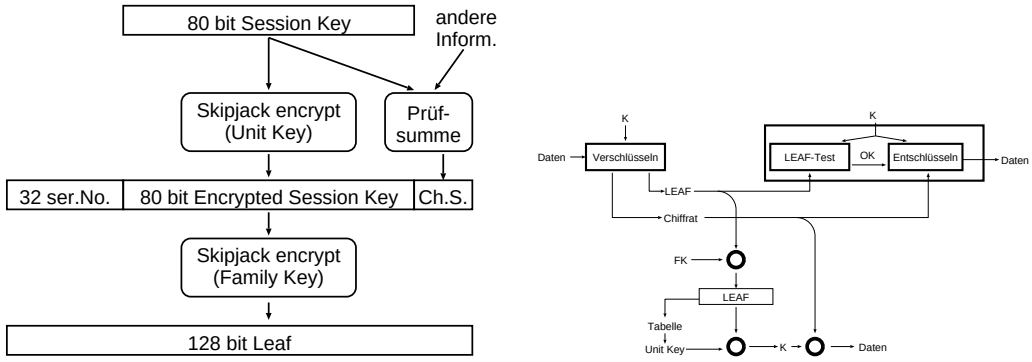
Nachdem der Sender den Sitzungsschlüssel in den Chip geladen hat, erzeugt der Chip ein sog. LEAF (Law Enforcement Access Field) wie in Abbildung 5.8a. Der Schlüssel wird mit dem „Unit Key“ verschlüsselt und mit der Seriennummer und einer Prüfsumme versehen. Dieser Block wird dann mit dem „Family Key“ erneut verschlüsselt. Der Sender soll nun zusätzlich zu den verschlüsselten Daten dieses LEAF übertragen.

Damit er dieses LEAF auch wirklich versendet, ist der Empfänger so gebaut, daß er erst dann arbeitet, wenn außer dem Sitzungsschlüssel auch das LEAF geladen wurde. Mit dem „Family Key“ kann der Empfänger das LEAF entschlüsseln und gelangt so an die Prüfsumme. Diese wird auf Konsistenz mit dem Sitzungsschlüssel geprüft, damit der Empfänger kein falsches LEAF angeben kann. Stimmt die Prüfsumme, wird die Nachricht entschlüsselt.

Der Staat, der die Übertragung abhört, kann das LEAF mit dem „Family Key“ entschlüsseln und gelangt so an die Seriennummer, anhand der er in seiner Datenbank den „Unit Key“ finden kann. Damit kann er den Sitzungsschlüssel entschlüsseln und mit diesem die ganze Nachricht (Abbildung 5.8b).

Es stellte sich aber schnell heraus, daß es mehrere leichte Wege gibt, den staatlichen Zugriff auszuhebeln:

- Der Sender kann vor oder nach der Clipper-Verschlüsselung ein weiteres, anderes Verfahren anwenden. Selbst wenn dieses Verfahren minderwertig ist und nur eine geringe Schlüssellänge hat, ist die Erfolgsdetektion schwierig.



(a) Erzeugung des LEAF-Feldes innerhalb des Clipper Chips

(b) Zugriff des Staates auf den Sitzungsschlüssel

Abbildung 5.8: Aufbau und Funktionsweise des „Clipper Chip“: Der Chip stellt eine normale Blockchiffre mit einem Schlüssel von 80 Bit zur Verfügung („Skipjack“-Algorithmus). Zu jeder Nachricht wird außerdem ein sog. „LEAF“ (Law Enforcement Access Field) generiert.

- Das LEAF kann durchaus auf einem anderen, sicheren Kanal mit geringer Kapazität und akausal übertragen werden, etwa durch ein Public-Key-Verfahren.
- Wie zuerst Mat Blaze (u. a. in [65]) zeigte, kann der Sender wegen der kurzen Prüfsumme von nur 16 Bit auch ohne Kenntnis des „Family Key“ mit durchschnittlich $2^{16} = 65536$ Versuchen ein falsches und aus Zufallsdaten bestehendes LEAF erraten, das zwar den Empfänger freischaltet, dem Staat aber den Zugriff nicht ermöglicht.

5.5.2 Offenlegung des Schlüssels ohne Kenntnis des Senders

Deutlich schwieriger ist die Offenlegung des Schlüssels ohne die Kenntnis und damit auch ohne das Einverständnis und gegen den Willen des Senders der chiffrierten Daten.

Ein mit der Kryptographie vertrauter Sender wird die verwendeten Protokolle und die Chiffren hinreichend prüfen und ggf. entsprechende Gegenmaßnahmen ergreifen, wie sich z. B. im oben beschriebenen Fall des „Clipper“ gezeigt hat.

Die bekannten neueren und für die EDV entworfenen Strom- und Blockchiffren weisen eine wichtige Eigenschaft auf: Die Zeichen des Chiffrats entstammen dem gleichen Alphabet wie der Klartext und das Chiffrat hat die gleiche Zahl von Zeichen. Chiffrat und Klartext können prinzipiell die gleiche Menge an Information tragen. Ein sorgsamer Sender wird deshalb auf jeden Fall mißtrauisch werden, wenn die Länge des Chiffrats von der Länge des Klartextes abweicht oder ein anderes Alphabet verwendet.

Eine Offenlegung des Schlüssels ohne Kenntnis des Senders setzt also bereits voraus, daß auf ein äußeres, dem Sender nicht ersichtliches Protokoll verzichtet wird und die Schwächung innerhalb der Chiffre selbst stattfindet. Sie setzt weiterhin voraus, daß dem Sender der Chiffrieralgorithmus nicht bekannt ist, weil er sonst den Algorithmus untersuchen und die Offenlegung finden bzw. durch Simulation die Abweichung einer Chiffriermaschine vom veröffentlichten Algorithmus entdecken kann. Es ist deshalb eine „Black Box“ notwendig. Die notwendigen Eigenschaften einer solchen „Black Box“ sollen nun betrachtet werden.

Der Schutz vor Entdeckung setzt voraus, daß das Chiffrat immer die gleiche Länge wie der Klartext hat. Es kann also keinen „zusätzlichen“ verdeckten Kanal für die Schlüsselentropie geben; die Schlüsselentropie muß über den normalen Kanal an den Zensor übermittelt werden. Das bedeutet notwendigerweise, daß Teile des Klartextes nicht übertragen werden können. Dabei sind in Abhängigkeit von der Art der Daten – d. h. von deren Interpretation – drei Fälle zu unterscheiden:

Irrelevanz
: Irrelevante Informationen können vor der Absendung entfernt und ohne weiteres beim Empfang synthetisiert werden. Dabei treten notwendigerweise Übertragungsfehler auf, falls der Informationsgehalt der irrelevanten Informationen größer als Null ist.

Redundanz
: Redundante Informationen können vor der Absendung durch Kompression entfernt und beim Empfang aus den übertragenen Daten durch Dekompression wieder erzeugt werden. Die übliche Unterscheidung zwischen verlustfreien und verlustbehafteten Kompressionsverfahren findet sich hier in der Unterscheidung zwischen Irrelevanz und Redundanz. Deshalb wird angenommen, daß die Redundanz beim Empfänger verlustfrei wieder hergestellt werden kann.

Klartextentropie
: Schließlich kann auch ein Teil der Klartextentropie entfernt werden, was aber auf jeden Fall zu einem Übertragungsfehler führt.

Der erfolgversprechendste Platz für die Übertragung der Schlüsselentropie liegt daher in der *Redundanz* des Klartextes. Abbildung 5.9 zeigt das Grundprinzip der Übertragung zwischen Sender und Empfänger mit der eingebetteten Übertragung der Schlüsselentropie. Der Angreifer, der den Datenstrom abhört, kann sich so Zugang zum Sitzungsschlüssel verschaffen.

Durch entsprechenden Aufbau der „Black Box“ kann die Schlüsselentropie, die der Sender vorgibt, in den freien Platz, der durch die Kompression erreicht wird, portionsweise eingeschoben werden und mit einem nur dem Zensor bekannten zweiten Schlüssel K' verschlüsselt werden (Abbildung 5.10).

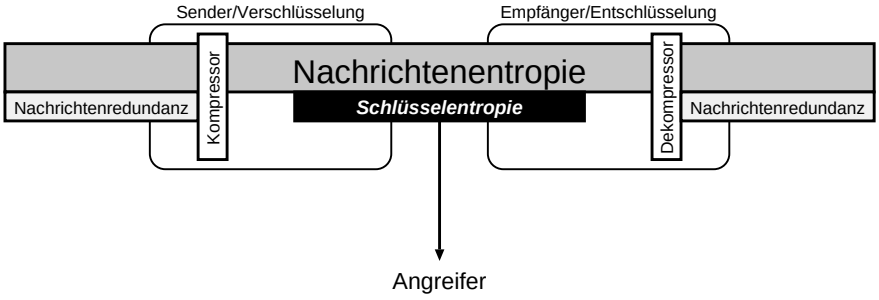


Abbildung 5.9: Eine „Black Box“-Chiffriereinrichtung könnte die übertragenen Daten komprimieren und in der so freigewordenen Kanalkapazität die Schlüsselentropie mitübertragen. Ein Angreifer, der den Kanal abhört, könnte sich so Zugang zum Sitzungsschlüssel verschaffen.

Das Grundproblem dabei ist, daß der Kompressor immer nur für ein bestimmtes statistisches Modell der Daten ausgelegt ist und deshalb auf einer Annahme des Angreifers über die Eigenschaften der übertragenen Daten beruht. Stimmt diese nicht, kommt es zwangsläufig zu Übertragungsfehlern. Abbildung 5.10 zeigt deshalb nur ein vereinfachtes Bild. Ein ernsthafterer Aufbau würde verschiedene Phasen der Übertragung unterscheiden:

Adaption

In der Adaptionsphase werden die Daten unverändert übertragen, es kann deshalb nicht zu Übertragungsfehlern kommen.

Sender und Empfänger untersuchen aber die übertragenen Daten und adaptieren ihr Kompressionsverfahren, z. B. indem sie Codebücher, Häufigkeitstabellen oder Synthesefilter generieren.

Da beide Seiten auf den gleichen Daten arbeiten, kommen sie zum gleichen Ergebnis.

Prognose

Auch in dieser Phase werden die Daten unverändert übertragen.

Es besteht aber das Problem, daß sich beide Seiten darüber einigen müssen, ob, wann und in welchem Umfang sie auf eine Kompression umschalten. Dabei ist zu berücksichtigen, daß zu diesem Zeitpunkt noch keine Übertragungskapazität für diese Information zur Verfügung steht. Beide Seiten müssen unabhängig von einander und ohne explizite Kommunikation anhand der bereits übertragenen Daten entscheiden, ob, wann und wie die Schlüsselentropie „geschmuggelt“ wird.

Dazu erstellen sie eine *Prognose*: Das (adaptierte) Kompressionsverfahren wird testweise auf die übertragenen Daten angewandt. Erlaubt das Ergebnis die Vermutung, daß auch die nächsten zu übertragenden Daten so gut zu komprimieren

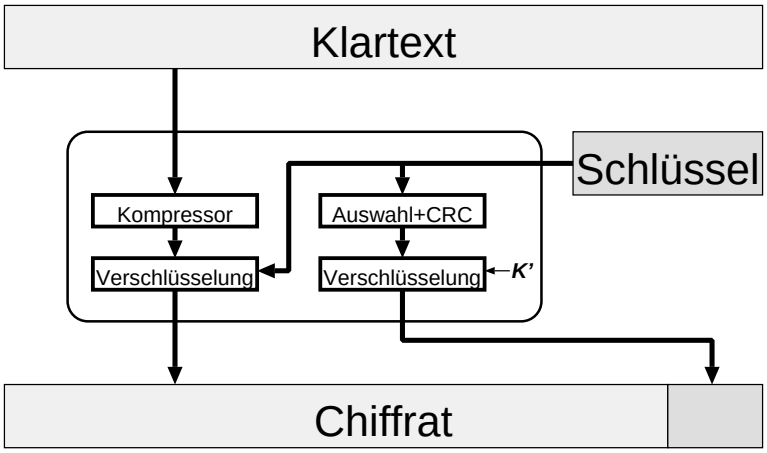


Abbildung 5.10: Vereinfachter Aufbau einer „Black Box“-Chiffriereinrichtung mit verdecktem Kanal zur Übertragung der Schlüsselentropie an den Angreifer. Zum Schutz vor Entdeckung und Ausnutzung durch andere Angreifer wird die Übertragung des Schlüssels zusätzlich mit einem zweiten Schlüssel K' verschlüsselt, der nur dem Angreifer bekannt ist.

sind, daß die Schlüsselentropie versteckt werden kann, so wird die nächste Phase der Kompromittierung durchgeführt.

Während der Sender hier eine a posteriori-Messung vornehmen könnte, kann der Empfänger nur eine a priori-Abschätzung vornehmen. Da beide aber unbedingt zum gleichen Ergebnis kommen müssen, muß sich auch der Sender auf die a priori-Abschätzung beschränken.

Kompromittierung

Ist die Prognose günstig, so schalten Sender und Empfänger synchron auf die Kompression bzw. Dekompression um und übertragen zusätzlich die Schlüsselentropie.

Weil beide Seiten die Entscheidung, ob und wie eine Kompromittierung erfolgt, auf eine a priori-Abschätzung stützen müssen, ist es durchaus möglich, daß die Prognose fehlerhaft ist und das adaptierte Kompressionsverfahren ein falsches Ergebnis liefert oder die Daten nicht verkürzt. Da die Entscheidung nicht revidierbar ist, kommt es zu Störungen in der Übertragung, wenn die Entropie nicht der Prognose entspricht.

Das ist dann das vom Zensor verursachte Rauschen aus Beweis 5.18.

Normalbetrieb

Ist die Prognose ungünstig oder Schlüssel übertragen worden, wird der Normalbetrieb aufgenommen.

Der Angreifer, der das Chiffrat abhört, kann zunächst nicht sicher entscheiden, ob der

Schlüssel mit übertragen wurde oder nicht, denn darin würde bereits 1 Bit Information liegen und die Anhebung der Übertragungskapazität erzwingen. Er kann aber annehmen, daß die Prognose günstig war, da suchen, wo der Schlüssel liegen würde, und diesen Schlüssel versuchen. Je nach Anwendungsgebiet könnte damit ein großer Teil der Übertragungen leicht mitgelesen werden.

Eine einfachere Variante wäre, den Schlüssel einfach ohne jede Rücksicht auf Übertragungsfehler zu übertragen und darauf zu hoffen, daß der Fehler unbemerkt bleibt oder auf Fehler im Kanal zurückgeführt wird.

Beispiel 5.33:
Telefonverschlüsselung
Eine solche „Black Box“ soll zur Verschlüsselung von Telefongesprächen entworfen werden.

Telefongespräche haben im Normalfall einen hohen Anteil an Redundanz und Irrelevanz, die durch die Sprache, das Hörvermögen, die Eigenschaften des Kehlkopfs, der beschränkten Qualität von Mikrofonen, Lautsprechern und Verstärkern etc. bedingt ist.

Eine einfache Methode wäre es etwa, einen 80-Bit-Schlüssel einfach irgendwann zu übertragen und mit einem charakteristischen 48-Bit-Header zu versehen, der dem Angreifer das Auffinden erleichtert. Bei einem Gespräch in ISDN-Qualität (8000 Samples pro Sekunde zu je 8 Bit) würden damit 16 Samples gestört, was ein sehr kurzes Knacken von 2 ms zur Folge hätte, falls sie am Block übertragen werden. Würden sie jedoch „flach“ in das unterste Bit gelegt, würde die Übertragung 16 ms dauern, der Übertragungsfehler aber vom menschlichen Ohr nicht wahrgenommen werden.

Größere Datenmengen können übermittelt werden, wenn die Stimme des Sprechers analysiert wird und eine Sprachkompression (z. B. CELP oder GSM) durch Aufbau von Codebüchern vorbereitet wird.

Folgt dann ein eindeutiger Zischlaut, ein klarer Vokal oder eine Sprechpause, kann kurzfristig auf die Kompression umgeschaltet werden, weil der Synthesizer diese Laute für kurze Zeit selbst so „singen“ kann, daß dies nicht auffällt.

Das Beispiel ist analog auch auf andere Bereiche anwendbar, etwa die Verschlüsselung von Datenpaketen im Netzwerkbereich.

5.5.2.1 Erkennung der Schlüsseloffenlegung durch Tests

Tests können prinzipiell nicht die Abwesenheit eines Fehlers (= Abweichung von der Spezifikation) belegen, sondern nur dessen Anwesenheit. Es wäre deshalb trügerisch, die Sicherheit einer „Black Box“ mit dem Bestehen von Tests beründen zu wollen.

Jedoch kann man Tests so gestalten, daß die Konstruktion einer Einrichtung, die diese Tests besteht und trotzdem Schlüsselentropie offenbart, erheblich erschwert wird.

Prinzipiell sind alle vorgestellten Tests auf den Nachweis einer manchmal niedrigeren Übertragungskapazität als der nominellen ausgerichtet, weil von der nominellen Übertragungskapazität im Fall der Kompromittierung ein kleiner Teil für die Schlüsselentropie verbraucht wird.

Abgesehen von Stromverbrauch und Rechenleistung unterscheidet sich die Chiffriereinrichtung „mit Hintertür“ nur in der Kompromittierungsphase von einer „ohne Hintertür“. Da die Struktur der Chiffre nicht bekannt ist, muß die Beurteilung anhand des Ur-Klartextes und des Dechiffrates erfolgen. Dabei ist nun mit Tests zu versuchen, einen Übertragungsfehler zu provozieren und so den Verlust von Nachrichtenentropie nachzuweisen. Übertragungsfehler können bei einfachen Verfahren schon im Normalbetrieb auftreten, bei Verwendung einer Prognosefunktion dann, wenn diese zum falschen Ergebnis führt.

Ein erster Schritt ist die Suche nach Übertragungsfehlern im Normalbetrieb. Dabei wird gewährleistet, daß es nicht zu Fehlern auf dem Kanal selbst kommen kann. Falls es schon hier zu Übertragungsfehlern kommt, ist bereits der Nachweis der „fehlerhaften“ Funktion erbracht.

Ist die Chiffriereinrichtung für einen bestimmten Zweck entworfen, der mit einem gewissen statistischen Modell der zu übertragenden Daten verbunden werden kann, ist zu versuchen, eine Synthese von Irrelevanz oder Reproduktion von Redundanz zu erkennen. Dazu sind Veränderungen in der Irrelevanz oder der Redundanz der übertragenen Daten zu erzeugen, die mit dem anzunehmenden statistischen Modell unverträglich sind. Ziel des Versuches ist, die Dekompression zu einer erkennbar fehlerhaften Arbeitsweise zu bringen.

Ebenso könnte es versucht werden, die Prognosefunktion zu einem erkennbaren Fehler zu provozieren, indem versucht wird, durch starke Schwankungen in der Entropie der Daten eine Fehlprognose bzw. eine zum Fehler führende Adaption herbeizuführen.

5.5.3 Triviale Umgehungen der Offenlegung

Eine Schlüsseloffenlegung, die dem Sender bekannt ist, kann er natürlich auf verschiedene triviale Weisen umgehen, wie auch das Beispiel „Clipper Chip“ zeigte. Ist die Offenlegung gesetzlich vorgeschrieben, liegt in der Umgehung freilich ein Gesetzesverstoß. Trotzdem sollen hier kurz einige Methoden exemplarisch aufgezählt werden:

- Der Sender verwendet das Verfahren oder die Offenlegung überhaupt nicht, sondern nutzt ein anderes Verfahren.
- Der Sender neutralisiert die Offenlegung, indem er das Protokoll verändert und die für die Offenlegung wesentlichen Schritte nicht oder anders ausführt.

- Der Sender unternimmt eine *Unterverschlüsselung*, d. h. er verschlüsselt den Klartext mit einem anderen Verfahren und wendet darauf das vorgeschriebene Verfahren an.

  Trotz eines Gesetzesverstoßes muß der Staat zur Strafverfolgung zunächst nachweisen bzw. erklären, woher er überhaupt von der Unterverschlüsselung weiß, was dem Zweck der Überwachung zuwiderläuft.

- Der Sender kann *Überverschlüsseln* und die gesamte Nachricht oder nur die zur Offenlegung wesentlichen Teile geschützt übertragen, wenn dies zur Funktion des Verfahrens notwendig ist (z. B. Clipper).

  Verallgemeinert kann der Sender die für die Offenlegung relevanten Teile auch über einen anderen, sicheren Kanal übertragen, der sich vom überwachten Kanal zeitlich oder räumlich unterscheidet.

5.5.4 „Legale“ Umgehungen der Offenlegung

Sehr viel interessanter ist es, eine Offenlegung mit „legalen“ Mitteln zu umgehen, also das Protokoll bestimmungsgemäß anzuwenden und trotzdem die Offenlegung zu verhindern.

Das bedeutet:

- Keine versteckten Kanäle
- Keine Manipulation des Protokolls
- Der Empfänger kann durch ausschließliche Verwendung der „Black Box“ in bestimmungsmäßiger Weise und ohne zusätzliche Geheimnisse die Nachricht im Klartext erfahren.
- Der Empfänger verfügt daher auch nicht über eine eigene Entropiequelle, d. h. keinen Zufallszahlengenerator.
- Der Angreifer kennt die „Software“ des Empfängers und deren Anwendung. Es handelt sich dabei nicht um eine Klasse von Programmen, d. h. es wird keine versteckte Entropie durch die Wahl der Verfahren eingeschleppt.
- Auch der Angreifer bzw. Zensor verhält sich „legal“.

Somit erscheint es zunächst ausgeschlossen, eine Offenlegung zu umgehen, weil nämlich der Zensor *die Position des Empfängers übernommen hat und von diesem technisch nicht mehr unterscheidbar ist*.

Die Möglichkeit einer technischen Unterscheidung kann aber dann gegeben sein, wenn sich der Angreifer durch andere Rahmenbedingungen technisch vom Empfänger unterscheiden muß.

Beispiel 5.34:
Zeitliche Beschränkung des Zensors

Es ist aus Gründen der Akzeptanz und aus juristischen Überlegungen zu mißbilligen, wenn Kommunikation willkürlich belauscht wird. Es soll dazu einer Genehmigung von dritter – richterlicher – Seite bedürfen, die in beide Richtungen zeitlich abgeschlossen ist: Sie soll nicht rückwirkend gelten und sie soll nicht unbegrenzt gelten, also auf eine bestimmte Dauer beschränkt werden.

Ein Protokoll, das dieses gewährleistet, wird in [16] vorgestellt.

Damit kann der Zensor zeitlich nicht mehr die volle Position des Empfängers einnehmen. Zensor und Empfänger werden technisch unterscheidbar und der Empfänger einzeln adressierbar.

Zur Umgehung des Protokolls kann daher die zeitliche Beschränkung des Zensors ausgenutzt werden. Die Übertragung muß auf verschiedene Zeitpunkte verteilt werden, wie weiter als die maximale Überwachungsdauer auseinanderliegen.

Dabei sind zu unterscheiden:

Akausale erste Kommunikation

muß stattfinden, wenn der Sender die Nachricht zum ersten Übertragungszeitpunkt noch nicht kennt.

Er übermittelt dem Empfänger einen normalen symmetrischen Schlüssel, der extra groß und auffällig als solcher gekennzeichnet ist, sowie eine ausführliche Bedienungsanleitung nebst Dechiffrierprogramm. Die Übertragung wird nur durch die „Black Box“ gesichert.

In der zweiten, späteren Übertragung versendet er die Nachricht, die mit dem bereits mitgeteilten Schlüssel unterverschlüsselt wurde. Außerdem fügt er im Klartext einen deutlichen Hinweis hinzu, wie der Empfänger die Nachricht zu dechiffrieren habe.

Der Zensor kann nur eine der beiden Übertragungen abhören. Beide sind aber legal, weil sie den oben aufgestellten Anforderungen genügen. Der Empfänger ist unter Verwendung nur der Box schon in der Lage, den Klartext eindeutig zu bestimmen. Es liegt daher keine verbotene Übertragung vor.

Kausale erste Kommunikation

Kennt der Sender zum Zeitpunkt der ersten Übertragung bereits die Nachricht, kann er sie natürlich auch mit einem Shared Secret-Schema aufteilen oder mit einer Schlüssellosen Chiffre bearbeiten und in zwei Hälften transportieren.

Auch dabei weist er bei der Übertragung ausdrücklich darauf hin, was der Empfänger zu tun habe, um sich nicht dem Vorwurf versteckter Absprachen auszusetzen.

5.6 Nachträgliche Verpflichtung zur Offenlegung

Eine oft sehr schwierige Form des Angriffs ist der Angriff auf die Position des Verteidigers, also der Versuch des Angreifers, diesen völlig zu übernehmen (Abbildung 2.3e auf Seite 48). Gelingt dieser Angriff, dann versagen alle technischen Sicherungsmaßnahmen, weil Verteidiger und Angreifer technisch nicht mehr unterscheidbar sind. Eine solche Übernahme ist auch die *„bedingungslose Kapitulation“* des Verteidigers.

Einige typische Methoden staatlicher Kommunikationsüberwachung müssen als ein solcher Angriff mit dem Ziel der Übernahme der Position des Verteidigers angesehen werden. Dazu gehören u. a.

- „Lauschangriffe“, bei denen entschlüsselte Nachrichten abgehört werden, also der Territorialschutz des Verteidigers umgangen wird,
- „Lauschangriffe“, bei denen durch Abhörmaßnahmen vor allem Schlüsselgeheimnisse ausgespäht werden, also die technische Unterscheidbarkeit von Verteidiger und Angreifer durch Kenntnis von Geheimnissen untergraben wird und kryptographische Methoden unwirksam gemacht werden,
- „Zwangsmaßnahmen“, wie Strafandrohung oder Beugehaft, mit der die Aufgabe der Sicherungsmaßnahmen erzwungen wird und
- „Gewaltmaßnahmen“, wie Beschlagnahme und Hausdurchsuchungen, mit denen der Territorialschutz auf Schicht 1 gebrochen wird.

Die staatliche Kommunikationsüberwachung kann deshalb als prototypisches Beispiel für den Angriff auf die Position des Verteidigers angesehen werden.

5.6.1 Schutzobjekt eigene Identität

Die Übernahme der Position einer Partei wird in den allermeisten Fällen gezielt versucht werden. Der Angreifer hat vor dem Angriff eine genaue Vorstellung von der Identität des Verteidigers bzw. muß sich im Rahmen der Angriffsvorbereitung Kenntnis von der Identität des Verteidigers verschaffen.

Eine Maßnahme gegen den Angriff ist daher das Verbergen der eigenen Identität. Im Zusammenhang mit der Kommunikationssicherheit bedeutet dies natürlich zunächst, daß die Vertraulichkeit aller Nutzlasten gesichert werden muß.

Wichtiger sind hier aber die Hilfslasten, gerade weil sie so gebaut sind, daß sie technisch leicht und damit automatisiert ausgewertet werden können und weil sie zweckbedingt auch dem Routing dienen und damit die Feststellung der räumlichen oder zeitlichen Position einer Partei erleichtern.

Zur Abwehr sind daher alle Sicherungsmaßnahmen heranzuziehen, die die Hilfslasten der verschiedenen Schichten schützen.

5.6.2 Eigenpartitionierung

Die Übernahme der eigenen Partei bezieht sich dann auf die gesamte Partei, wenn die Partei unteilbar ist (was sie per Definition 2.1 ist).

Kann die Partei sich selbst aber bezüglich ihrer Interessenlage weiter differenzieren und sich in Bestandteile unterschiedlicher Interessenlage teilen, oder betrachtet sie sich selbst als zukünftigen Angreifer, dann kann sie sich selbst räumlich oder zeitlich in mehrere „Unterparteien“ aufspalten und eine Objektentkopplung vornehmen. Diese Unterparteien werden dann selbst Kommunikationsparteien. Der Angreifer, der solche Unterparteien übernommen hat, rutscht gegenüber den anderen Teilen in die Position aus Abbildung 2.3d ab und kann mit bekannten Mitteln abgewehrt werden.

5.6.2.1 Räumliche Unterteilung

Eine besonders gegen Angriffe auf Schicht 1 – also auch gewaltsame Angriffe – wirksame Maßnahme ist die räumliche Unterteilung der eigenen Partei. Das bedeutet, daß verschiedene Interessenaspekte mit verschiedenen, gegeneinander abgesicherten Orten und technischen Einrichtungen korrespondieren müssen. Im einfachsten Fall bedeutet das, daß thematisch unterschiedliche Daten auf verschiedenen Rechnern oder unter verschiedenen Benutzeridentitäten gespeichert werden. Eine stärkere Sicherung wäre die Sicherung der Datenspeicherung über Shared Secret-Verfahren und die Speicherung einzelner Teile in verschiedenen Ländern mit unterschiedlichen Rechtsnormen.

Die Wirksamkeit der räumlichen Unterteilung hängt davon ab, daß die einzelnen Teile gegeneinander auf Grundlage einer Bedrohungsannahme abgesichert werden, in der jeweils alle anderen Teile als feindlich angesehen werden. Die Konsequenz daraus ist, daß die Teile nicht nur bezüglich der Nutzlast gegeneinander abgesichert werden, sondern auch bezüglich der Hilfslasten. Im Idealfall kann der Angreifer auf den Teilen, die er übernommen hat, weder erkennen noch beweisen, daß es weitere Teile gibt.

5.6.2.2 Zeitliche Unterteilung

Die räumliche Unterteilung kann durch eine Kapitulation ihre Wirkung verlieren. Die Folge ist, daß der Verteidiger sich selbst als potentiellen Angreifer in der Zukunft an-

sehen muß. Eine Trennung von Angreifer und Verteidiger setzt dabei die zeitliche Unterteilung voraus, was jedoch schwierig ist, weil der zeitlichen Übertragung die Eigenschaft des Sende- und Empfangsfensters fehlt (vgl. Abbildung 2.2 auf Seite 40).

Dabei gibt es prinzipiell zwei Methoden der organisatorischen Abgrenzung, nämlich die zeitliche Positionierung der befugten Partei *vor* dem Angreifer, was bedeutet, daß etwas ab einem bestimmten Zeitpunkt nicht mehr möglich ist, und *nach* dem Angreifer, was bedeutet, daß etwas vor einem bestimmten Zeitpunkt noch nicht möglich ist. Die beiden Varianten werden nachfolgend untersucht.

5.6.3 Verteidiger *vor* Angreifer – Unwiederholbarkeit

In der ersten Variante der zeitlichen Eigenpartitionierung liegt der Verteidiger zeitlich *vor* dem Angreifer. Die eigene Partei soll also *jetzt* etwas können, was sie *zukünftig* nicht mehr kann.

Es wird weiterhin gefordert, daß sich die Zeit, in der die eigene Partei noch als Verteidiger anzusehen ist, mit dem Angriff zeitlich nicht überlappt. Würden die Verteidigungsmaßnahmen erst nach dem Angriff ergriffen, gäbe es einen ungeschützten Zeitraum, der zum Angriff oder zur Blockierung ausreichen kann. Bei einer Kapitulation besteht dann auch gar nicht mehr der Wille zur Verteidigung[14].

Die Abgrenzung muß also *prophylaktisch* erfolgen.

Im Normalfall wird es keine vorgegebenen und geeigneten technischen Unterscheidungsmerkmale der eigenen Partei zu verschiedenen Zeitpunkten geben. Der von technischem Gegebenheiten unabhängige Weg, zwei Parteien künstlich unterscheidbar zu machen, ist der kryptographische, nämlich durch Kenntnis eines Geheimnisses. Die zeitliche Abgrenzung erfolgt dann durch *Vernichtung* des Geheimnisses.

Zur Vernichtung bieten sich zwei Wege an:

1. Vernichtung des *Geheimnisinhaltes* durch Löschen der Daten.
2. Vernichtung der *Geheimniseigenschaft* durch Veröffentlichung der Daten.

Beide Wege werden nachfolgend betrachtet.

In der Literatur [91, 59, 47] wird einem Protokoll in diesem Zusammenhang die Eigenschaft „perfect forward secrecy“ zugeschrieben, wenn die Kompromittierung der Langzeitschlüssel nicht zu einer Kompromottierung der Kurzzeitschlüssel führt. Dies wird nachfolgend näher untersucht.

[14] Die Situation ist einem Banküberfall vergleichbar: Steht der Tresor noch offen, fehlt womöglich die Zeit, ihn bei einem Überfall zu schließen. Ist er verschlossen, kann seine Öffnung durch Gewaltandrohung erzwungen werden. Hat er aber ein Zeitschloß, wird die Sache interessant.

5.6.3.1 Der triviale Fall: Vertraulichkeit zeitlicher Übertragungen

Ist das Schutzobjekt die Erhaltung der Vertraulichkeit von nur zeitlich im Bereich des Verteidigers übertragenen Daten, also einer kontinuierlichen Übertragung der Partei an sich selbst, liegt der triviale Fall vor, daß die Übertragung nicht geschützt werden muß, sondern einfach vom Verteidiger selbst abgebrochen werden kann (z. B. durch Löschung der Datenträger). Dieser Fall muß daher bei den nachfolgenden Überlegungen nicht mehr berücksichtigt werden.

5.6.3.2 Interaktion

Der triviale Fall ist nicht mehr gegeben, wenn die Daten auch an anderer Stelle zeitlich übertragen werden, wenn sie etwa der Sender fehlerkausal oder -akausel erneut überträgt oder der Angreifer die Kommunikation abgehört hat. Hat der Angreifer eine unchiffrierte Kommunikation abgehört, dann war der Angriff bereits erfolgreich und eine Prophylaxe ist nicht mehr sinnvoll. Daher wird der Fall betrachtet, daß der Angreifer ein Chiffrat aufgefangen hat und den Verteidiger auf der Suche nach dem Schlüssel angreift.

Schutzobjekt ist damit der *Kurzzeitschlüssel*, der prophylaktisch vernichtet werden muß. Die Vernichtung ist aber dann nicht möglich, wenn der Verteidiger diesen Schlüssel wiedergewinnen kann, nämlich deterministisch aus dem übertragenen und vom Angreifer aufgefangenen Chiffrat gewonnen (z. B. wenn der Sitzungsschlüssel Public Key-verschlüsselt übertragen wurde und der dazu passende geheime Schlüssel nicht gelöscht werden darf) oder anderweitig wiederhergestellt werden kann (z. B. aufgrund Schlüsselhinterlegung). Tritt der Verteidiger als rein passiver Empfänger auf, dann ist der Empfangsvorgang durch erneute Zusendung jederzeit wiederholbar, weil der Empfang ja eindeutig sein muß und das Empfangsverfahren bei erneuter Anwendung zum gleichen Ergebnis – dem Klartext – führen muß.

Der Empfänger kann also nicht passiv bleiben, sondern muß seinerseits auch *senden*, also Entropie abgeben. Der eigentliche Sender wiederrum darf sich nicht „taub stellen“, denn sonst könnte der Angreifer den Sender durch erneutes Abspielen der Nachricht simulieren und so den Vorgang nachstellen. Der Sender muß die zugesandte Entropie verarbeiten, sie dazu erst empfangen und dann seine Sendung davon abhängig machen.

Der Angreifer könnte aber auch diese vorhergehende Übertragung in Gegenrichtung aufzeichnen. Sie muß also kryptographisch geschützt sein. Der Angreifer wird deshalb versuchen, auch den Sender zu übernehmen und ihn zur Wiederholung zu zwingen. Damit besteht wieder genau das gleiche Problem wie zuvor, nur einen Protokollschritt früher und mit vertauschten Seiten!

Auch hier stellt sich wieder das Problem, daß es einen passiven und deterministisch ablaufenden Empfänger gibt, der nachträglich durch Wiederholung der empfangenen (chiffrierten) Daten simuliert werden kann.

Deshalb soll gefordert werden:

- Kein potentieller Empfänger (wozu je nach Eigenschaften der Chiffre und verwendetem Protokoll auch der Absender gehören kann) darf rein determiniert funktionieren, also durch Langzeitschlüssel und die empfangenen Daten festgelegt sein. Er muß eine eigene Entropiequelle verwenden.
- Der Empfang darf nur unter Verwendung eines aus der Entropiequelle gewonnenen Kurzzeitschlüssels möglich sein.

  Das bedeutet, daß das Chiffrat vom Kurzzeitschlüssel nicht unabhängig sein darf.

  Folglich muß vor der Übertragung des Chiffrats, aber nach Bildung des Kurzzeitschlüssels eine von diesem abhängige Übertragung vom potentiellen Empfänger zum Sender stattfinden, damit der Sender darauf reagieren kann.
- Diese Übertragung darf den Kurzzeitschlüssel nicht gefährden.
- Nach Abarbeitung des Übertragungsprotokolls müssen die Kurzzeitschlüssel vernichtet werden.

Definition 5.35:
„kryptographisch interaktiv“
Ein Protokoll, daß die beiden ersten der oben genannten Bedingungen erfüllt, heißt „kryptographisch interaktiv“.

Die letzten beiden Bedingungen ergeben sich zwangsläufig aus naheliegenden – und wie sogleich gezeigt wird, aus weniger naheliegenden – Gründen.

Als Beispiel wird das in Abschnitt 5.7.1 dargestellte Protokoll betrachtet. Beide Seiten nutzen eine Entropiequelle (zur Bildung von k). Beide Seiten senden auch eine von der Entropiequelle abhängige Information (die Signatur). Diese Signaturen gefährden weder k, noch den Signierschlüssel. Nach Abarbeitung „vernichten“ beide Seiten ihr k. Trotzdem ist das Protokoll nicht gegen nachträgliche Übernahme sicher, denn das k ist aus der Signatur, der Nachricht und dem Langzeitschlüssel zu rekonstruieren.

Die Kompromittierung des Langzeitschlüssels alleine, wie sie in der oben beschriebenen Definition von „perfect forward secrecy“ genannt wird, reicht hier nicht aus. *Deshalb wird zusätzlich angenommen, daß der Angreifer die gesamte Kommunikation aufgezeichnet hat und darüberhinaus alle beteiligten Parteien nachträglich – also nach der Schlüsselvernichtung – übernommen hat.*

Bemerkung 5.36:
Unvernichtbarkeit der Signierinformation
Im Gegensatz zum RSA-Verfahren, das völlig determiniert abläuft, wird zur Erzeugung von ElGamal- und ähnlichen Signaturen Entropie benötigt. Sie kann aber nicht mehr unabhängig vom Langzeitschlüssel vernichtet werden (siehe auch Abschnitt 5.7.3).

Zu fordern ist also weiterhin, daß der Verteidiger nach Vernichtung des Kurzzeitschlüssels die gleiche Position einnimmt, die der Angreifer zu diesem Zeitpunkt hat und gegen die das Protokoll primär ausgelegt ist.

Ein Beispiel für ein solches Protokoll ist das Diffie-Hellman-Protokoll. Besteht noch kein geeigneter Sitzungsschlüssel, kann durch diesen Zusatzschritt ein bestehendes Protokoll abgesichert werden.

5.6.3.3 Pseudointeraktion

Nicht in jedem Fall besteht die Möglichkeit einer direkten Interaktion zwischen Sender und Empfänger. Das ist gerade dann der Fall, wenn die zu sichernde Kommunikation nicht interaktiv ist, beispielsweise E-Mail (abgesehen von interaktiven Protokollen tieferer Schichten wie SMTP oder TCP). Die Erzwingung der Interaktion würde einen weitreichenden Eingriff in das Protokoll und die Anforderungen an die Parteien bedeuten.

In diesem Fall bietet sich eine „Pseudointeraktivität“ an, bei der der wesentliche Schritt der entropieabhängigen Übertragung vom individuellen Kommunikationspartner und vom einzelnen Übertragungsvorgang abstrahiert wird und sich nur noch auf die zeitliche Begrenzung bezieht.

Beispiel 5.37:
Pseudointeraktiver Schlüsseltausch
Der Verteidiger erzeugt in regelmäßigen Abständen ein neues Public Key-Schlüsselpaar, nimmt eine Eigenzertifizierung vor und macht den öffentlichen Teil allgemein zugänglich. Er gibt dabei an, daß dieser Schlüssel nur für das nächste Zeitinterval gültig ist. Nach Ablauf des Intervals vernichtet er den geheimen Teil. Nachrichten, die mit diesem Schlüssel chiffriert wurden, kann er nur innerhalb dieses Intervals dechiffrieren. Eine nachträgliche Offenlegung ist nicht möglich.

5.6.3.4 Schlüsselabwurf

Eine andere Problemstellung ergibt sich, wenn nicht *Vertraulichkeit*, sondern die zeitliche Begrenzung der Authentizität bzw. die *Unbeweisbarkeit* das Ziel ist. Will der Angreifer beweisen, daß der Verteidiger sein Geheimnis in irgendeiner Weise verwendet hat, z. B. indem er ihm eine Signatur entgegenhält, beruht der Beweis auf der Annahme, daß nur der Verteidiger das Geheimnis kennt. Kann der Verteidiger nichts gegen den Beweis unternehmen, daß das Geheimnis überhaupt verwendet wurde (die dem Angreifer vorliegende Signatur paßt zum öffentlich zertifizierten Schlüssel), dann kann er das Geheimnis *abwerfen*, d. h. so veröffentlichen, daß jeder es hätte verwenden können. Der Verteidiger ist damit nicht mehr technisch von der Umwelt unterscheidbar und einzeln adressierbar.

Zu unterscheiden ist dabei zwischen dem Angriffs*kausalen* und dem prophylaktischen Abwurf.

Beispiel 5.38:
Signaturen mit Schlüsselabwurf
Eine Nachricht soll versandt werden. Zur Gewährleistung der Authentizität gegenüber den befugten Empfängern soll sie eine Signatur tragen. Der Angreifer soll die Authentizität aber nicht nachweisen können.

Der Sender erzeugt dazu ein Signaturschlüsselpaar und nimmt eine Eigenzertifizierung vor, signiert also mit seinem dauerhaften und öffentlich zertifizierten Schlüssel den neu erzeugten öffentlichen Schlüssel. Mit dem neuen geheimen Schlüssel signiert er seine Nachrichten und versendet diese zusammen mit der Signatur und dem eigenzertifizierten öffentlichen Schlüssel.

Nach gewisser Zeit veröffentlicht er auch den geheimen Schlüssel. In der Zwischenzeit können sich die befugten Empfänger von der Echtheit der Nachricht überzeugen. Ein Angreifer kann die Authentizität jedoch nur nachweisen, wenn er beweisen kann, daß die Signatur vor dem ersten Schlüsselabwurf erzeugt wurde.

5.6.4 Verteidiger *nach* Angreifer – Zeitfenster

Die schwierigere Variante ist die Positionierung des Verteidigers *nach* dem Angreifer, also die Gewährleistung dessen, daß man *später* etwas kann, was man *jetzt* noch nicht kann. Es ist Gegenstand der Kryptographie, *Wissen* zu schützen, aber es gehört bislang nicht zu ihren Aufgaben, *eigene Unwissenheit* zu erhalten. Deshalb ist eine gewisse Kreativität notwendig.

5.6.4.1 Kryptographische Problemstellungen

Ein möglicher Weg führt über eine Abschätzung der eigenen Rechenleistung. Der Verteidiger setzt sich selbst in die Position des Angreifers und verteidigt sich so gegen sich selbst, daß er den Angriffsaufwand abschätzen kann. Er könnte beispielsweise eine Zufallszahl ziehen, diese als öffentlichen Schlüssel eines Public Key-Verfahrens verwenden, die Nachricht damit verschlüsseln, den Klartext vernichten und sich sodann an das Brechen des Schlüssels machen. Stimmt die Schätzung hinreichend, ist er erst nach Ablauf einer gewissen Zeit in der Lage, die Nachricht zu lesen.

Um die Gefahr eines Zufallstreffers zu minimieren oder eine besonders schwere Suche zu vermeiden kann es zweckmäßig sein, die Nachricht über ein Shared Secret-Schema aufzuteilen und alle Teile getrennt zu schützen. Statistische Ausreißer werden so abgedämpft.

Die Sicherheit dessen wird erheblich geschwächt, wenn der Angreifer nicht nur die Position des Verteidigers übernimmt, sondern auch noch eigene Rechenleistung mitbringt.

5.6.4.2 Der Zeit-Notar

Ein anderer Weg führt über die Einbindung einer (oder mehrerer) vertrauenswürdiger Dritter, die den Zeitablauf herstellen.

Beispiel 5.39:
Der Zeit-Notar
Ein Notar erzeugt ein Public Key-Schlüsselpaar und zertifiziert dieses. Er veröffentlicht den öffentlichen Schlüssel mit der Ankündigung, den geheimen Schlüssel 10 Jahre später ebenfalls zu veröffentlichen.

Der Verteidiger kann die Nachricht verschlüsseln und das Chiffrat selbst lagern. Gibt der Notar nach 10 Jahren den geheimen Schlüssel frei, kann die Nachricht wieder dechiffriert werden.

5.6.4.3 Organisatorische Trennung

Ein dritter Weg wäre die Lagerung an einem über den Zeitraum unzugänglichen Ort. Beispiele hierfür sind:

- Innerhalb einer Briefsendung, die der Verteidiger an sich selbst verschickt und einerseits auf die Zuverlässigkeit, andererseits auf die Langsamkeit der Post vertraut.
- Innerhalb einer Briefsendung, die der Verteidiger an eine zufällig erdachte Adresse in einem fernen Land verschickt und darauf hofft, daß es die Adresse nicht gibt und der Brief an den Absender zurückgeht.
- Innerhalb einer Raumsonde, die auf einer Bahn in den Weltraum geschossen wird, die sie nach gewisser Zeit wieder zur Erde bringt.
- Innerhalb einer Raumsonde, die nach Ablauf gewisser Zeit die Daten zurückfunkt.

5.7 Konflikte mit der Signatursicherheit

Eine staatliche Kommunikationskontrolle wird erst dann wirksam, wenn der Gebrauch von Chiffren, die der Staat nicht brechen oder auf sonst eine Art entfernen kann, verhindert wird, was naheliegenderweise durch ein Verbot geschehen wird. Gleichzeitig haben die meisten Staaten aber aus wirtschaftlichen und Wettbewerbsüberlegungen

heraus ein Interesse, digitale Signaturen zu etablieren, um Geschäfte im Internet möglich zu machen, Dokumente elektronisch speichern und transportieren zu können usw. Eine derartige Situation liegt zur Zeit auch in Deutschland vor bzw. wird von manchen angestrebt.

Beide Forderungen widersprechen sich jedoch. Ein Kryptographieverbot ist erst dann als wirksam anzusehen, wenn dem einzelnen Bürger der Besitz eines nur ihm bekannten kryptographischen Geheimnisses untersagt oder unmöglich ist und wenn er insbesondere den zur Kommunikation mit anderen notwendigen Schlüsseltausch jedenfalls nicht ohne (vom Staat feststellbares) persönliches Zusammentreffen mit dem Kommunikationspartner durchführen kann. Es darf also keine Zertifizierungsinfrastruktur entstehen.

Eine sichere und beweiskräftige Signatur setzt aber gerade das voraus, nämlich daß der Bürger ein eigenes Geheimnis zur Erstellung von Signaturen hat und weiterhin Zugriff auf eine vertrauenswürdige Zertifizierungsinfrastruktur, um fremde Signaturen prüfen zu können.

Hierin liegt aber ein Widerspruch, denn

- jedes Signiergeheimnis kann unmittelbar oder mittelbar auch als Chiffriergeheimnis verwendet werden und
- jede Zertifizierungsinfrastruktur kann unmittelbar oder mittelbar auch zur Prüfung der Authentizität eines Schlüsseltauschs für Chiffren benutzt werden.

Es wird angenommen, daß normale symmetrische Chiffren allgemein bekannt sind und Software verfügbar ist. Für den überwachenden Staat ist es wichtig, den Schlüsseltausch zwischen verschiedenen Personen, deren Zusammenhang für ihn nicht erkennbar ist, zu verhindern, also das Zustandekommen eines ihm nicht bekannten Sitzungsschlüssels zu verhindern und die Identität der Parteien (z. B. durch Abhören der Datenübertragungen) festzustellen.

Nachfolgend werden ein spezieller und der allgemeine Fall betrachtet.

5.7.1 Impliziter Schlüsseltausch durch DLP-Signaturen

Hierzu wird zunächst das *ElGamal*-Signaturschema [56] betrachtet, das auf dem Problem des Diskreten Logarithmus aufsetzt:

1. Gegeben seien eine große Primzahl p und ein Generator g in $\mathbb{Z}_p^*$.
2. Eine Partei A bildet ihren öffentlichen und geheimen Schlüssel:

   Gewählt wird eine Zufallszahl x_A, $1 < x_A < p - 1$.

   $y_A := g^{x_A} \bmod p$.

   Der öffentliche Schlüssel ist das Tupel (p, g, y_A),
   der geheime Schlüssel ist (p, g, x_A).

3. Eine Nachricht M $(M < p-1)$ wird signiert:

   Gewählt wird eine Zufallszahl k_M, $1 < k_M < p-1$, ggt$(k_M, p-1) = 1$, d. h. k_M^{-1} mod $p-1$ existiert.

   $r_M := g^{k_M}$ mod p.

   $s_M := k_M^{-1} \cdot (M - x_A r_M)$ mod $p-1$.

   Die Signatur für M ist (r_M, s_M).

   Damit gilt[15]: $M = s_M k_M + x_A r_M$ mod $p-1$

4. Die Signatur wird verifiziert:

   Es wird geprüft ob

   $g^M = r_M^{s_M} \cdot y_A^{r_M}$ mod p

   ist, was bei Echtheit der Signatur durch Konstruktion gegeben ist.

Damit enthält *jede* Signatur eine Zahl r_M, deren diskreter Logithmus k_M nur dem Erzeuger der Signatur bekannt ist. Typischerweise werden p und g nicht nur für ein einzelnes Schlüsselpaar, sondern für mehrere Schlüsselpaare oder eine ganze Infrastruktur verwendet.

Damit wird aber mit je einer signierten Nachricht zweier Absender sofort ein impliziter Diffie-Hellman-Schlüsseltausch zwischen den beiden Absendern erzeugt:

A sendet M_A mit der Signatur (r_{M_A}, s_{M_A}),
B sendet M_B mit der Signatur (r_{M_B}, s_{M_B}).

Damit ist ein gemeinsamer Schlüssel $g^{k_{M_A} \cdot k_{M_B}}$ mod p gegeben, den jede der beiden Parteien aus dem eigenen k und dem gegnerischen r errechnen kann: $g^{k_{M_A} \cdot k_{M_B}} = r_{M_A}^{k_{M_B}} = r_{M_B}^{k_{M_A}}$ mod p.

Beispiel 5.40:
Waschmaschine und Käsekuchen

Alice sendet eine signierte Nachricht in eine Usenet-Newsgruppe, in der sie eine gebrauchte Waschmaschine sucht. Zwei Wochen später gibt Bob in einer anderen Newsgruppe ein ebenfalls signiertes innovatives Rezept für Käsekuchen zum besten. Beide Nachrichten werden weltweit verbreitet.

Beide haben sich völlig legal, bestimmungsgemäß und unverdächtig verhalten. Es besteht keinerlei erkennbarer Zusammenhang zwischen beiden Nachrichten.

[15] Genau genommen ist die Gleichung so nicht richtig, denn M, x, s und k sind Elemente aus $\mathbb{Z}_{p-1}$, während y und r Elemente aus $\mathbb{Z}_p^*$ sind. Es wird aber stillschweigend eine Abbildung $\mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$ unterstellt, die alle Elemente außer $p-1$ „identisch“ abbildet. x ist kleiner als $p-1$ zu wählen.

Trotzdem existiert nun zwischen beiden ein gemeinsamer Schlüssel. Beide können sich über die Signaturen der Nachrichten von der Identität des anderen überzeugen.

Sendet Alice nun über ein Broadcast-Medium (z. B. das Usenet) eine mit diesem Schlüssel chiffrierte Nachricht, kann kein Dritter erkennen, wer der Empfänger dieser Nachricht ist. Ein Zusammenhang zwischen Alice und Bob ist für Dritte nicht erkennbar.

Die Parteien brauchen sich k_M übrigens nicht zu merken, da dieses jederzeit aus der Nachricht M, der Signatur (r_M, s_M) und dem geheimen Schlüssel (p, g, x_A) wieder errechnet[16] werden kann (vgl. Abschnitt 5.7.3). Damit kann allerdings auch ein Angreifer nach Übernahme des geheimen Schlüssels (p, g, x_A) einer der beiden Parteien den gemeinsamen Schlüssel ermitteln; das Verfahren ist also nicht sicher gegen eine nachträgliche Übernahme einer Partei. Es empfiehlt sich daher die Objektentkopplung durch Zwischenschaltung eines Interaktivitäts- oder Pseudointeraktivitätsschrittes (siehe Abschnitt 5.6.3.2), z. B. eines weiteren Diffie-Hellman-Schlüsseltauschs mit frei gewählten Zufallszahlen, wobei die öffentlichen Schlüssel mit dem durch die Signaturen indizierten gemeinsamen Schlüssel chiffriert und damit indirekt auf Authentizität geprüft werden. Wenn die dafür gewählten Zufallszahlen und der so erzeugte Schlüssel nach Beendigung der Kommunikation vernichtet werden, kann auch eine nachträgliche Übernahme des geheimen Schlüssels (p, g, x_A) nicht mehr zu einer nachträglichen Dechiffrierung der Kommunikation führen.

5.7.2 Expliziter Schlüsseltausch durch Eigenzertifizierung

Im vorhergehenden Abschnitt wurde gezeigt, wie durch Verwendung des auf dem Diskreten Logarithmus beruhenden ElGamal-Signaturschemas ein authentischer Schlüsseltausch verdeckt und ohne von der normalen Signatur abweichende Arbeitsschritte durchgeführt werden kann.

Auch unabhängig vom Funktionsprinzip eines Signaturschemas oder des diesem zugrundegelegten Problems könne Signaturen zur zum authentischen Schlüsseltausch „mißbraucht“ werden, wenn auch nur mit einem expliziten Arbeitsschritt und somit nicht mehr verdeckt.

Zwei Parteien, die einen Schlüsseltausch durchführen wollen, können dazu problemlos einen Diffie-Hellman-Schlüsseltausch unternehmen:

1. Die Parteien A und B einigen sich auf eine große Primzahl p und einen Generator g in $\mathbb{Z}_p^*$.

[16] Im Beispiel 5.40 wären Nachricht und Signatur jederzeit in öffentlich zugänglichen News-Archiven zu finden.

2. Beide Parteien erzeugen je eine Zufallszahl x, $1 < x < p - 1$. Die Zahlen x_A und x_B bleiben geheim und werden nach der letzten Nutzung des ausgehandelten Schlüssels vernichtet.
3. Die Parteien errechnen jeweils $y := g^x \bmod p$ und senden sich gegenseitig diese y_A und y_B.
4. Die Parteien errechnen den ausgehandelten Sitzungsschlüssel:
   $g^{x_A x_B} = y_A^{x_B} = y_B^{x_A} \bmod p$

Damit haben die Parteien einen gemeinsamen Sitzungsschlüssel, der Dritten nicht bekannt wird, ausgehandelt. Kritisch ist jedoch der Austausch von y_A und y_B in Schritt 3. Hier wird nämlich ein vertrauenswürdiger Kanal benötigt, der die Authentizität und die Integrität gewährleistet. Es besteht sonst die Gefahr, daß sich ein Angreifer zwischen die Parteien schaltet, mit beiden Seiten je einen Schlüssel aushandelt und sich so transparent zwischen die Parteien setzt oder sich ganz einfach als eine der Parteien ohne deren Mitwirkung ausgibt. Es existieren zwar verschiedene Interlock-Protokolle, aber sie gewährleisten Authentizität und Integrität nur unter gewissen Randbedingungen.

Mit einem allgemein anerkannten Signaturschema und einer vertrauenswürdigen Zertifizierungsinfrastruktur ist aber genau der fehlende sichere Kanal gegeben, der Authentizität und Integrität gewährleistet. So kann sich jede Partei problemlos und jederzeit ein x und ein y heraussuchen und das y mit ihrem Namen versehen und signieren, damit also *eigenzertifizieren*. Der Kommunikationspartner kann die Signatur prüfen und sich bei Erfolg auf den Schlüsseltausch einlassen.

Bemerkung 5.41:
Signaturen und Chiffrierschlüssel
Damit ist auf einfache Weise gezeigt, daß mit einer bestehenden Infrastruktur für Signaturen immer auch eine Infrastruktur für den authentischen Schlüsseltausch geschaffen wird, deren Sicherheit als das Minimum aus der Sicherheit der Signaturinfrastruktur und des Schlüsseltauschverfahrens (hier Diffie-Hellman) anzusehen ist.

Die politische Forderung, einerseits vertrauenswürdige und gute Signaturen haben zu haben, andererseits aber starke Verschlüsselungsverfahren und insbesondere Schlüsselzertifizierungen und Schlüsseltauschverfahren verbieten und eindämmen zu wollen, läßt sich also nicht durchsetzen. Man muß sich zwischen Signaturen und einem Kryptoverbot entscheiden.

5.7.3 Signaturen als Nachrichtenkanäle

Wie Gus Simmons zeigte [114, 115, 116, 113, 117], können ElGamal-Signaturen auch als „Subliminal Channel“, also zur verdeckten Übertragung von Informationen genutzt werden.

Kennt nämlich der Empfänger einer Nachricht M mit der ElGamal-Signatur (r_M, s_M) (siehe Abschnitt 5.7.1) das geheime x des Absenders, dann kann er die Gleichung $M = s_M k_M + x r_M \bmod p-1$ nach k_M auflösen und so die für andere nicht erkennbare Zahl k_M feststellen, damit also eine verdeckte Nachricht empfangen.

Dieses Problem besteht grundsätzlich bei allen kryptographischen Protokollschritten, bei denen ein Zufallszahlengenerator – und damit eine zusätzliche Entropie – verwendet wird.

Diese verdeckten Kanäle sind dabei nach mehreren Kriterien zu unterscheiden bzw. zu klassifizieren:

Sender-Empfänger oder Empfänger-Empfänger

Im Falle der hier gezeigten Übertragung des k_M kann der Absender die übertragene Nachricht (nahezu) frei festlegen, er kann damit *echte* Nachrichten übertragen.

Im in Abschnitt 5.7.1 beschriebenen Protokoll wird zwar zwischen beiden Parteien ein gemeinsamer Schlüssel vereinbart, den zwar jede der Parteien durch ihre Wahl beeinflußt, den aber deshalb auch keine der Parteien alleine bestimmen und deshalb auch keine echte Nachricht darin unterbringen kann. Beide Parteien sind als *Empfänger* des ausgehandelten Schlüssels anzusehen.

Gemeinsames Geheimnis

Die hier gezeigte Übertragung des k_M funktioniert nur, solange es zwischen Sender und Empfänger ein gemeinsames Geheimnis x gibt. Es muß also zuvor auf andere Weise ein gemeinsames Geheimnis vereinbart worden sein.

Im Gegensatz dazu ist im in Abschnitt 5.7.1 beschriebene Protokoll ein gemeinsames Geheimnis nicht notwendig.

Gus Simmons hat außerdem gezeigt, daß nur Verfahren, die ein gemeinsames Geheimnis voraussetzen, eine hohe Kanalkapazität ermöglichen können.

Bemerkung 5.42:
Kombination beider Verfahren

Die beiden beschriebenen Verfahren unterscheiden sich in ihren Anforderungen und den Eigenschaften des erzeugten Kanals.

Sie lassen sich aber durchaus kombinieren, indem zunächst ein gemeinsamer Schlüssel erzeugt und aus diesem dann ein beiden Seiten bekanntes x abgeleitet wird, mit dessen Hilfe nunmehr echte Nachrichten übertragen werden können.

6 Zusammenfassung und Einordnung

In der vorliegenden Arbeit wurden wichtige Arbeitsschritte zum Entwurf und zur Erstellung sicherer Kommunikationssysteme vorgestellt. Der Inhalt der Arbeit geht dabei über die bisher in der Informatik übliche Sichtweise der System- und Kommunikationssicherheit, die rein auf die mathematischen Aspekte der Kryptographie beschränkt war, hinaus und zeigt auf, wie diese Verfahren ausgewählt und zu einem funktionierenden und den Anforderungen genügenden System zusammengesetzt werden können und wie ein bestehendes System zu untersuchen ist.

Die Thematik ist jedoch nicht mit der Algorithmentechnik oder der Programmverifikation zu verwechseln. Beide setzen nämlich das Bestehen einer Spezifikation voraus, während die in dieser Arbeit vorgestellten Kriterien und Methoden erst der Erstellung der Spezifikation dienen. Die Arbeit stellt somit ein Bindeglied zwischen reiner Kryptographie einerseits, und der Softwaretechnik und Programmverifikation und -validierung andererseits dar, das bisher in der Informatik vernachlässigt wurde.

Die vorliegende Arbeit ist damit nicht völlig abstrakt, sondern zielt klar auf die tatsächliche Erstellung realer Systeme ab. Sie kann daher die harte – und bisweilen äußerst unwissenschaftliche – reale Welt nicht völlig außer Acht lassen, sondern muß auch nichttechnische Rahmenbedingungen insoweit berücksichtigen, als sie für den Entwurf von Kommunikationssystemen von erheblicher Bedeutung sind. Sie muß sich auch aus und gerade wegen wissenschaftlicher Sichtweise mit Rahmenbedingungen befassen, die wissenschaftlichen Erkenntnissen geradewegs entgegenläuft. Deshalb wurde auch im Rahmen des Themas eine Betrachtung staatlicher Kommunikationskontrolle unternommen. Diese Arbeit wurde in einer Zeit angefertigt, in der dieser staatliche Eingriff aktuelles Thema war.

Die Ergebnisse dieser Arbeit bildeten die Grundlage eines für den Deutschen Bundestag angefertigten Gutachtens über Anforderungen an die Kommunikationssicherheit in der Medizin[44].

Literaturverzeichnis

[1] *Urteil des AG Frankfurt a. M. v. 31.10.1997 – 30 C 1299/97-47*. NJW 1998, 687.

[2] *Urteil des AG Osnabrück v. 24.10.97 – 47 C 335/97*. NJW 1998, 688.

[3] ALBITZ, PAUL und CRICKET LIU: *DNS and BIND*. O'Reilly & Associates, 1997.

[4] ALTMANN, RALPH: *Vorsicht: Konto in Gefahr*. c't 4/96, Seite 66, 1996.

[5] BALZERT, HELMUT: *Die Entwicklung von Software-Systemen*, Band Band 34 der Reihe *Reihe Informatik*. Bibliographisches Institut, 1982.

[6] BAUER, FRIEDRICH L.: *Kryptologie — Methoden und Maximen*. Springer, 2. Auflage, 1994.

[7] BAUER, FRIEDRICH L. und MARTIN WIRSING: *Elementare Aussagenlogik*. Springer-Verlag, 1991.

[8] BAUSPIESS, F., P. HORSTER und ST. STEMPEL: *Netzwerksicherheit durch selektiven Pakettransport*. In: *Tagungsband Verläßliche Informationssysteme VIS '93*, Springer Informatikberichte, 1993.

[9] BECK, MICHAEL und OTHERS: *Linux-Kernel-Programmierung*. Addison-Wesley, 2. Auflage, 1994.

[10] BELL, D. E. und L. J. LAPADULA: *Secure Computer Systems: Unified Exposition and Multics Interpretation*. Technischer BerichtESD-TR-75-306, MTR 2997 Rev. 1, The MITRE Corporation, March 1976.

[11] BELLOVIN, STEVEN M.: *Security Problems in the TCP/IP Protocol Suite*. Computer Communication Review, 19(2):32–48, April 1989. `http://www.rootshell.com/docs/tcpip_problems_bellovin.ps.gz`.

[12] BELLOVIN, STEVEN M.: *Packets Found on an Internet*. Computer Communications Review, 23(3):26–31, July 1993. `http://www.rootshell.com/docs/packets_found_bellovin.ps.gz`.

[13] BERNERS-LEE, T., R. FIELDING und H. NIELSEN: *RFC1945: Hypertext Transfer Protocol – HTTP/1.0*. `ftp://ds.internic.net/rfc/`, 1996.

[14] BETH, GOLLMANN, HORSTER, SCHÄFER und WICHMANN: *Leitfaden zur PC-Sicherheit*. E.I.S.S.-Report 1991/4, E.I.S.S., 1991.

[15] BETH, TH., F. BAUSPIESS, H.-J. KNOBLOCH und ST. STEMPEL: *TESS - A Security System Based On Discrete Exponentiation*. Computer and Communications, 17(7):466–475, 1994.

[16] BETH, TH., H. J. KNOBLOCH, M. OTTEN, G. J. SIMMONS und P. WICHMANN: *Towards Acceptable Key Escrow Systems*. In: *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, Seiten 51–58, New York, 1994. ACM Press.

[17] BETH, TH., H.-J. KNOBLOCH und ST. STEMPEL: *Authentifikationsdienst SELANE - Modularisierung und Einsatz*. E.I.S.S.-Report 3/1994.

[18] BIRKELBACH, JÖRG: *Safer Banking*. c't 12/96, Seiten 104–108, 1996.

[19] BI-WISS.-VERL., LEKTORAT D. (Herausgeber): *Duden Informatik*. Bibliographisches Institut, Mannheim, 1993.

[20] BLAZE, MATT: *NFS Tracing By Passive Network Monitoring*. `http://www.rootshell.com/docs/nfs_trace.txt`.

[21] BORENSTEIN, N. und N. FREED: *RFC1521: MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies*. `ftp://ds.internic.net/rfc/`, 1993.

[22] BREWER, D. F. C. und M. J. NASH: *The Chinese Wall Security Policy*. In: *Proceedings of the IEEE Symposium on Security and Privacy*, Seiten 206–214, Oakland, 1989.

[23] BÄR, SIEGFRIED: *Forschen auf Deutsch: Der Machiavelli für Forscher und solche, die es noch werden wollen*. Verlag Harri Deutsch, 1996.

[24] *Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz – BSIG) vom 17. Dezember 1990*. Bundesgesetzblatt 1990, Teil I, 2834.

[25] *Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung – BSIZertV).* Bundesgesetzblatt 1992, Teil I, 1230.

[26] *Vierter Zwischenbericht der Enquete-Kommission „Zukuft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ des Deutschen Bundestages*. Bundestagsdrucksache 13/11002.

[27] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *IT-Sicherheitshandbuch, Handbuch für die sichere Anwendung der Informationstechnik*, März 1992.

[28] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Gefährdungen und Sicherheitsmaßnahmen beim Betrieb von digitalen Telekommunikationsanlagen*, April 1994.

[29] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *IT-Grundschutzhandbuch, Maßnahmenempfehlungen für den mittleren Schutzbedarf*, 1995.

[30] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *IT-Grundschutzhandbuch, Maßnahmenempfehlungen für den mittleren Schutzbedarf*, 1997.

[31] *CERT Advisory CA-95:10: ghostscript Vulnerability*. `ftp://info.cert.org/pub/cert_advisories/`, 1995.

[32] *CERT Advisory CA-96.05: Java Implementations Can Allow Connections to an Arbitrary Host.* `ftp://info.cert.org/pub/cert_advisories/`, 1996.

[33] *CERT Advisory CA-96.07: Weaknesses in Java Bytecode Verifier*. `ftp://info.cert.org/pub/cert_advisories/`, 1996.

[34] *Cracking DES.* O'Reilly & Associates, 1998.

[35] CHAPMAN, D. BRENT: *Network (In)Security Through IP Packet Filtering*. In: *Proceedings of the Third USENIX Security Symposium*, Baltimore, MD, September 1992.

[36] CLARK, DAVID D. und DAVID R. WILSON: *A Comparison of Commercial and Military Computer Security Policies*. In: *Proceedings of the IEEE Symposium on Security and Privacy*, Seiten 184–194, Oakland, 1987.

[37] COMMISSION OF THE EUROPEAN COMMUNITIES: *INFOSEC '93, Security Investigations, The Security of Information Systems*, 1993.

[38] COMMISSION OF THE EUROPEAN COMMUNITIES: *INFOSEC '94, Security Investigations, The Security of Information Systems*, 1994.

[39] COSTALES, BRYAN und ERIC ALLMAN: *sendmail*. O'Reilly & Associates, 1997.

[40] CREIFELDS, CARL: *Rechtswörterbuch*. C. H. Beck, München, 13. Auflage, 1996.

[41] CROCKER, D.: *RFC822: Standard for the format of ARPA Internet text messages*. `ftp://ds.internic.net/rfc/`, 1982.

[42] CURRY, DAVID A.: *Improving the Security of your Unix System*. http://file:/Z/www.rootshell.com/docs/ improving_security_sri.ps.gz, April 1990.

[43] DANISCH, HADMUT: *RFC1824: The Exponential Security System TESS: An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange*. `ftp://ds.internic.net/rfc/`, 1995.

[44] DANISCH, HADMUT: *Gutachten über Künftige Anforderungen an die Kommunikationssicherheit in der Medizin, angefertigt für die Enquete-Kommission „Zukuft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft" des Deutschen Bundestages*. Technischer Bericht Europäisches Institut für Systemsicherheit, 1998.

[45] DEICIDE: *The Neophyte's Guide to Hacking*. `http://www.rootshell.com/docs/hacking_guide.txt`, August 1993.

[46] DIFFIE, W. und M. E. HELLMAN: *New Directions in Cryptography*. IEEE Transactions on Information Theory, IT-22(6):644–654, November 1976.

[47] DIFFIE, W., P. C. VAN OORSCHOT und M. J WIENER: *Designs, Codes and Cryptography*, Band 2, Kapitel Authentication and authenticated key exchanges, Seiten 107–125. 1992.

[48] *Allgemeine Kriterien für Stellen, die Produkte zertifizieren*. Deutsche Norm DIN EN 45 011.

[49] DUDENRED., WISSENSCHAFTLICHER RAT D. (Herausgeber): *Duden Herkunftswörterbuch*. Bibliographisches Institut, Mannheim, 1963.

[50] DUDENRED., WISSENSCHAFTLICHER RAT D. (Herausgeber): *Duden Fremdwörterbuch*. Bibliographisches Institut, Mannheim, 1982.

[51] EICHING, M. W. und J. A. ROCHLIS: *With Microscope and Tweezers. An Analysis of the Internet Virus of November 1988*. In: *Proceedings of IEEE Symposium on Research in Security and Privacy*, Seiten 326–345, 1989.

[52] ENGLER, TOBIAS: *Der gläserne Web-User*. c't 12/96, Seiten 94–99, 1996.

[53] EUROPEAN COMMUNITIES, COMMISSION OF THE: *Information Technology Security Evaluation Manual (ITSEM)*, 1993.

[54] FAUST, HARALD: *Datenschutz und Arbeitsplatzrechner*. Sicherheit in der Informationstechnik. Oldenbourg, 1991.

[55] FRIES, O., A. FRITSCH, V. KESSLER und B. KLEIN (Herausgeber): *Sicherheitsmechanismen*, Sicherheit in der Informationstechnik. Oldenbourg, 1993.

[56] GAMAL, T. EL: *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Transactinos of Information Theory, IT-31(4):469–72, July 1985.

[57] GEMOLL, WILHELM: *Griechisch-Deutsches Schul- und Handwörterbuch*. G. Freytag Verlag, 1965.

[58] GERHARDT, WALTRAUD: *Zugriffskontrolle bei Datenbanken*. Sicherheit in der Informationstechnik. Oldenbourg, 1993.

[59] GÜNTHER, C. G.: *An identity-based key-exchange protocol*. In: *Advances in Cryptology – Eurocrypt '89*, Nummer 434 in *Lecture Notes in Computer Science*, Seiten 29–37. Springer, 1990.

[60] GOLLMANN, DIETER: *Rambling about Security Protocols*. Vortrag an der Universität Karlsruhe am 24.4.1998.

[61] GRASSL, MARKUS: *Authentication as a By-Product of Error Correction in Communication Systems with Stream Ciphers*. Unveröffentlichter Aufsatz.

[62] HEISE, WERNER und PASQUALE QUATTROCCHI: *Informations- und Codierungstheorie*. Springer Verlag, 3 Auflage, 1995.

[63] HERDA, SIEGFRIED, SIBYLLE MUND und ANGELIKA STEINACKER (Herausgeber): *Szenarien zru Sicherheit informationstechnischer System*, Sicherheit in der Informationstechnik. Oldenbourg, 1993.

[64] HINSLEY, F. H. und ALAN STRIPP (Herausgeber): *Code Breakers – The Inside Story of Blechtley Park*. Oxford University Press, 1993.

[65] HOFFMAN, LANCE J. (Herausgeber): *Building in Big Brother*. Springer, 1995.

[66] HOWARD, JOHN D.: *An Analysis Of Security Incidents On The ???* Dissertation, Cernegie Mellon University, Pittsburgh, Pennsylvania 15213 USA, 1997. `http://www.info-sec.com/internet/howard/index.html`.

[67] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO/IEC Norm 7498-1:1994: Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*, 2. Auflage, 1994.

[68] *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)*. u. a. in Gemeinsames Ministerialblatt 1992, 546 und über die Kommission der Europäischen Gemeinschaften.

[69] *IT-Sicherheitskritierien*. u. a. in Gemeinsames Ministerialblatt 1989, 278.

[70] *Informations- und Kommunikationsdienste-Gesetz*. Gesetzblatt irgendwo, 1997. `http://www.iid.de/rahmen/iukdgbt.html`.

[71] JOHNS, M. ST.: *RFC1413: Identification Protocol*. `ftp://ds.internic.net/rfc/`, 1993.

[72] JONCHERAY, LAURENT: *A Simple Active Attack Against TCP*. `http://www.rootshell.com/docs/tcp_attack.ps.gz`, April 1995.

[73] KAHN, DAVID: *The Codebreakers*. Scribner, New York, 1996.

[74] KAUFMAN, CHARLIE, RADIA PERLMAN und MIKE SPECINER: *Network Security — Private Communication in a Public World*. Prentice-Hall, 1995.

[75] KERSTEN, HEINRICH: *Einführung in die Computersicherheit*. Sicherheit in der Informationstechnik. Oldenbourg, 1991.

[76] KERSTEN, HEINRICH: *Sicherheit in der Informationstechnik*. Oldenbourg, 1995.

[77] KLEIN, BIRGIT: *Authentifikationsdienste für sichere Informationssysteme*. Dissertation, Universität Karlsruhe, 1993.

[78] KOZACZUK, WLADYSLAW: *Geheimoperation WICHER – Polnische Mathematiker knacken den deutschen Funkschlüssel*. Bernard & Graefe Verlag, 1989.

[79] KUNZE, MICHAEL: *Netz-Razzia – Scientology bedrängt das Internet*. c't 7/1995, Seite 22.

[80] KUNZE, MICHAEL: *Privatsphäre im Datennebel*. c't 12/96, Seiten 100–102, 1996.

[81] LANDWEHR, CARL E.: *Formal Models for Computer Security*. ACM Computing Surveys, 13(3):247–278, September 1981.

[82] LANDWEHR, CARL E., ALAN R. BULL, JOHN P. MCDERMOTT und WILLIAM S. CHOI: *A Taxonomy of Computer Program Security Flaws, with Examples*. ACM Computing Surveys, 26(3), 1994. `http://www.itd.nrl.navy.mil/ITD/5540 /publications/CHACS/LANDWEHRindex.html`.

[83] LANDWEHR, C. E., C. L. HEITMEYER und J. MCLEAN: *A Security Model for Military Message Systems*. ACM Transactions on Computer Systems, 2(3):193–222, August 1984.

[84] *Langenscheidts Taschenwörterbuch Altgriechisch*, 1985.

[85] *Langenscheidts Universal-Wörterbuch Griechisch*, 1994.

[86] *Urteil des LG Frankfurt a. M. v. 22.4.1998 – 2/1 S 391/97*. NJW 1998, 3785.

[87] *Urteil des LG Hannover v. 16.3.1998 – 20 S 97/97*. NJW-CoR 1998, 304.

[88] LUCKHARDT, NORBERT: *Makro infiziert WinWord*. c't 10/95, Seite 57, 1995.

[89] MATSUI, MITSURU: *Linear Cryptanalysis of DES Cipher (III)*. In: *The 1994 Symposium on Cryptography and Information Security*, Biwako, Japan, 27. - 29. Januar 1994.

[90] MCLEAN, JOHN: *The Algebra of Security*. In: *IEEE Symposium on Security and Privacy*, 1988.

[91] MENEZES, ALFRED J., PAUL C. VAN OORSCHOT und SCOTT A. VANSTONE: *Handbook of Applied Cryptography*. CRC Press, 1997.

[92] MUI, LINDA und ERIC PEARCE: *X Protocol Reference Manual*, Band 8 der Reihe *The Definitive Guides to the X Window System*. O'Reilly & Associates, 1992.

[93] MYERS, J. und M. ROSE: *RFC1939: Post Office Protocol - Version 3*. `ftp://ds.internic.net/rfc/`, 1996.

[94] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. Department of Commerce: *An Introduction to Computer Security: The NIST Handbook*, Draft Auflage, 1994.

[95] NIST: *A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)*. Fed. Register, 56(169):42980–2, Aug. 1991.

[96] NYE, ADRIAN (Herausgeber): *X Protocol Reference Manual*, Band 0 der Reihe *The Definitive Guides to the X Window System*. O'Reilly & Associates, 1995.

[97] *Urteil des OLG Hamm zum EC-Kartenmißbrauch vom 17.3.1997 – 31 U 72/96*. NJW 1997, 1711.

[98] *Department of Defense Standard, DoD 5200.28-STD, „The Orange Book"*. `http://www.disa.mil/MLS`, December 1985.

[99] ORWELL, GEORGE: *1984*. Harcourt Brace Jovanovich, 1949.

[100] *Plenarprotokoll 13/170 des Deutschen Bundestages vom 18.4.1997*. `http://www.bundestag.de/ftp/13170a.zip`, 1997.

[101] PETERSON, FRANK: *Zensur oder Urheberschutz? – Scientology im Internet*. c't 3/1996, Seite 50.

[102] POHL, HARTMUT und GERHARD WECK (Herausgeber): *Einführung in die Informationssicherheit*, Sicherheit in der Informationstechnik. Oldenbourg, 1993.

[103] POSTEL, J.: *RFC821: Simple Mail Transfer Protocol*. `ftp://ds.internic.net/rfc/`, 1982.

[104] POSTEL, J.: *RFC1591: Domain Name System Structure and Delegation*. `ftp://ds.internic.net/rfc/`, 1994.

[105] RANUM, MARCUS J.: *Thinking About Firewalls*. `http://www.rootshell.com/docs/ firewalls_ranum.ps.gz`.

[106] REIF, HOLGER: *Word verseucht DOS*. c't 11/95, 1995.

[107] *Signale, Codes und Chiffren II*. Vorlesungsscript, Karlsruhe, 1993. Institut für Algorithmen und Kognitive Systeme.

[108] SCHNEIER, BRUCE: *Applied Cryptography*. John Wiley & Sons, Inc., 2. Auflage, 1996.

[109] SCHÖNING, UWE: *Logik für Informatiker*, Band Band 56 der Reihe *Reihe Informatik*. Bibliographisches Institut, 1987.

[110] SCHNURER, GEORG: *Eingehämmert – Wie Intels Marketing-Maschine funktioniert*. c't 13/1997, Seite 142.

[111] SHANNON, CLAUDE: *Communication Theory of Secrecy Systems*. Bell Systems Technical Journal, 1949.

[112] SILBERT, O., P. A. PORRAS und R. LINDELL: *The Intel 80x86 Processor Architecture: Pitfalls for Secure Systems*. In: *Proceedings of the IEEE Symposium on Security and Privacy*, Seiten 211–222, Oakland, 1995.

[113] SIMMONS, G. J.: *Subliminal Channels; Past and Present*. Working Copy.

[114] SIMMONS, G. J.: *The Prisoners' Problem and the Subliminal Channel*. In: CHAUM, D. (Herausgeber): *Crypto '83, Santa Barbara, CA, Aug. 21-14, 1983*, Advances in Cryptology, New York, 1984. Plenum Press.

[115] SIMMONS, G. J.: *The Subliminal Channel and Digital Signatures*. In: BETH, T. (Herausgeber): *Eurocrypt '84, Paris, France, April 9-11, 1984*, Advances in Cryptology, Seiten 364–378, Berlin, 1985. Springer Verlag.

[116] SIMMONS, G. J.: *A Secure Subliminal Channel (?)*. In: WILLIAMS, H. C. (Herausgeber): *Crypto '85, Santa Barbara, CA, Aug. 18-22, 1985*, Advances in Cryptology, Seiten 33–41, Berlin, 1986. Springer Verlag.

[117] SIMMONS, G. J.: *Contemporary Cryptology, The Science of Information Integrity*. IEEE Press, 1992.

[118] SIR HACKALOT: *UNIX: A Hacking Tutorial*. `http://www.rootshell.com/docs/Unixhack.txt`.

[119] SPAFFORD, EUGENE H.: *The Internet Worm Program: An Analysis*. Computer Communication Review, 19(1):17–57, 1989.

[120] STANDARDS, NATIONAL BUREAU OF: *Data Encryption Standard*. FIPS Publication, (46):1–18, 1977.

[121] STEMPEL, STEFFEN: *Transparente Netzwerktrennung zur Erhöhung der Sicherheit*. Dissertation, Universität Karlsruhe, 1996.

[122] STEVENS, W. RICHARD: *TCP/IP Illustrated*, Band 1. Addison-Wesley, 1994.

[123] STEVENS, W. RICHARD: *TCP/IP Illustrated*, Band 2. Addison-Wesley, 1995.

[124] STILLER, ANDREAS: *Bug-Wahn – Pentium: Absturzloch*. c't 14/1997, Seite 24.

[125] STILLER, ANDREAS: *Prozessorgeflüster – Der Bug von Intels Flaggschiff*. c't 1/1995, Seite 20.

[126] STILLER, ANDREAS: *Waschzettel – Der Pentium und seine Fehler*. c't 7/1995, Seite 186.

[127] STINSON, DOUGLAS R.: *Cryptography, Theory and Practice*. CRC Press, 1995.

[128] STOLL, CLIFFORD: *The Cuckoo's Egg*. Pocket Books, 1990.

[129] STRACK, HERMANN: *Sicherheitsmodellierung und Zugriffskontrolle in verteilten Systemen*. Dissertation, Universität Karlsruhe, 1995.

[130] TANENBAUM, ANDREW S.: *Computer-Netzwerke*. Wolfram's Fachverlag, 2. Auflage, 1990.

[131] TANENBAUM, ANDREW S.: *Computer Networks*. Prentice-Hall, 3. Auflage, 1996.

[132] TERRY, PHIL und SIMON WISEMAN: *A 'New' Security Policy Model*. In: *Proceedings of the IEEE Symposium on Security and Privacy*, Seiten 215–228, Oakland, 1989.

[133] *True Stories*. `http://www.infosec.ch/faelle/fall00.htm`. ZBinden Infosec AG.

[134] WALLICH, PAUL: *Piraten im Datennetz*. Spektrum der Wissenschaft, Seite 64ff., Mai 1994.

[135] WAYNER, PETER: *Using Content-Adressable Search Engines To Encrypt and Break DES*.

[136] WAYNER, PETER: *Disappearing Cryptography*. Academic Press, 1996.

[137] WICHMANN, PEER: *Mir unbekannter Titel*. Dissertationsentwurf, Universität Karlsruhe, spätes 20. Jahrhundert.

[138] WIENER, MICHAEL J.: *Efficient DES Key Search*, August 1993.

[139] WRIGHT, STEVE: *An appraisal of technologies for political control*. European Parliament, Directorate General for Research, Directorate B, The STOA Programme, January 1998.

[140] *Sicherheitszertifikat BSI-ITSEC-0116-1997 X·PRESSO Security Package 1.1*. `http://www.bsi.bund.de/aufgaben/ii/zert/reporte/0116.PDF`, 1997.

[141] ZENTRALSTELLE FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK: *Kriterien für die Bewertung von Systemen der Informationstechnik – IT Sicherheitskriterien*.

[142] ZORN, WERNER: *Internet in Deutschland – ein Trauerspiel*. VDI Nachrichten, 11.7.1997.

Lebenslauf

Name:	Hadmut Werner Danisch
Geburt:	22. Juni 1966 in Mannheim
1972 - 1976	Goetheschule in Lampertheim (Hessen)
1976 - 1981	altsprachliches Rudi-Stephan-Gymnasium in Worms
1981 - 1985	altsprachliches Theodor-Heuss-Gymnasium in Ludwigshafen am Rhein
1985	Abitur
1985 - 1986	Grundwehrdienst in Lahnstein und Koblenz
1986 - 1994	Studium der Informatik an der Universität Karlsruhe
1994	Diplom in Informatik
1994 - 1998	Wissenschaftlicher Mitarbeiter am Europäischen Institut für Systemsicherheit (E.I.S.S.) an der Universität Karlsruhe
seit 1998	Spezialist für System- und Netzwerksicherheit bei der Xlink Internet Consulting GmbH und Xlink Internet Service GmbH in Karlsruhe