UNIVERSITÄT HAMBURG

Fachbereich Wirtschaftswissenschaften

Arbeitsbereich für Betriebswirtschaftliche Datenverarbeitung

Prof. Dr. D. B. Preßmar

Diplomarbeit zum Thema:

Sicherheitskonzepte für Informationsnetze

Vorgelegt von:

Sönke Volquartz

Fachrichtung Betriebswirtschaftslehre

Mat. Nr. : 43 54 147

Mühlenstraße 13

22049 Hamburg

Tel. 040 / 68 59 49

Abgabedatum: 26.02.1997

INHALTSVERZEICHNIS

SEITE

ABKÜRZUNGSVERZEICHNIS

a.a.O.	:= am angeführten Orte
Abb.	:= Abbildung
AC	:= Authentication Center
ACL	:= Access Control List
AFNOR	:= Association Française de Normalisation
ANSI	:= American National Standards Institute
API	:= Application Programmng Interface
ARPANET	:= Advanced Research Projects Agency Network
ASEs	:= Application Service Elements
Aufl.	:= Auflage
BSI	:= Bundesamt für Sicherheit in der Informationstechnik
BSS	:= Base Station System
bzw.	:= beziehungsweise
CAPI	:= Common Application Programming Interface
CBC	:= Cipher Block Chaining
CCITT	:= Comité Consultatif International Télégraphique et Téléphonique; Vereinigung der Post- und Fernmeldegesellschaften
CEPT	:= Comité Européen des Postes et des Télécommunications; Vereinigung europäischer Post- und Fernmeldeverwaltungen
CERT	:= Computer Emergency Response Team
CFB	:= Cipher FeedBack
CPU	:= Central Processing Unit
CSMA/CD	:= Carrier Sense Multiple Access with Collision Detection
DARPA	:= Defence Advanced Research Projects Agency
DCS	:= Digital Cellular System
DEC	:= Digital Equipment Corporation
DEK	:= Data Encrypting Key
DES	:= Data Encryption Standard
DFN	:= Deutsches Forschungs-Netz
DIN	:= Deutsches Institut für Normung
DoD	:= Department of Defense
DSS	:= Digital Signature Scheme
DuD	:= Zeitschrift für Datenschutz und Datensicherung

DV := Datenverarbeitung

ECB := Electronic Code Book

ECC := Elliptic Curve Cryptosystem

ECITC := European Commitee for Information Technology Testing and Certification

EDI := Electronic Data Interchange

EDIFACT := Electronic Data Interchange for Administration, Commerce and Transport

EEPROM := Electrically Erasable Programmable ROM

EIR := Equipment Identification Register

EIT := Enterprise Integration Technologies

et al. := et alii

etc. := et cetera

ETSI := European Telecommunication Standards Institute

FDDI := Fibre Distributed Data Interface

FTAM := File Transfer, Access and Management (OSI)

FTP := File Transfer Protocol

gez. := gezeichnet

GSM := Groupe Spécial Mobile

H. := Heft

HLR := Home Location Register

Hrsg. := Herausgeber

HTML := Hypertext Markup Language

HTTP := Hypertext Transfer Protocol

IAB := Internet Architecture Board

IBM := International Business Machines

ICC := Integrated Circuit Card

ICCB := Internet Configuration Control Board

IEEE := Institute of Electrical and Electronic Engineers

I / O := Input / Output

IMEI := International Mobile Equipment Identity

IMSI := International Mobile Subscriber Identity

IP := Internet Protocol

IRSG := Internet Research Steering Group

ISDN := Integrated Services Digital Network
ISO := International Standardization Organization
IT := Informationstechnik, informationstechnische
ITEH := IT-Evaluationshandbuch
ITG := Informationstechnische Gesellschaft im VDE
ITSEC := Information Technology Security Evaluation Criteria
ITSEM := Information Technology Security Evaluation Manual
ITSK := IT-Sicherheitskriterien
Jg. := Jahrgang
KEK := Key Encrypting Key
KES := Zeitschrift für Kommunikations- und EDV-Sicherheit
LA := Location Area
LAI := Location Area Identification
LAN := Local Area Network
MAN := Metropolitan Area Network
MD := Message Digest
ME := Mobile-Equipment
MIB := Management Information Base
MIC := Message Integrity Check
MOC := Managed Object Class
MS := Microsoft
MSC := Mobile Switching Center
NBS := National Bureau of Standards
NCSC := National Computer Security Center
NIST := National Institute of Standards and Technology
NLSP := Network Layer Security Protocol
Nr. := Nummer
NSA := National Security Agency
OFB := Output Feedback
OSF := Open Software Foundation
OSI := Open System Interconnection (ISO)
PDU := Protocol Data Unit
PCT := Private Communication Technology Protocol
PEM := Privacy Enhanced Mail

PGP := Pretty Good Privacy
PLMN := Public Land Mobile Network
RAM := Random Access Memory
RC := Ron’s Cipher
RFC := Request for Comments
RIPEM := Riordan’s Internet PEM
ROM := Read Only Memory
ROSE := Remote Operations Service Element (OSI)
RPC := Remote Procedure Call
RSA := Rivest, Shamir, Adleman
s. := siehe
s. o. := siehe oben
s. u. := siehe unten
S. := Seite
S. ... f := Seite und die folgende Seite
S. ... ff := Seite und mehrere folgende Seiten
SFE := Security-Front-End
SHA := Secure Hash Algorithm
SHS := Secure Hash Standard
S-HTTP := Secure Hypertext Transfer Protocol
SIM := Subcriber Identify Module
SMTP := Simple Mail Transfer Protocol
SNMP := Simple Network Management Protocol
sog. := sogenannter, sogenannte
SRES := Signed Response
SRT := Secure Request Technology
SSL := Secure Socket Layer
STE := Security Terminal Equipment
SVZ := Schlüsselvergabezentrum
TAN := Transaktionsnummer
TCP := Transmission Control Protocol (DARPA)
TCOS := Telesec Chipcard Operating System
TCSEC := Trusted Computer System Evaluation Criteria
TDMA := Time Division Multiple Access

TGS	:= Ticket Granting Server
TIS	:= Trusted Information Systems
TMSI	:= Temporary Mobile Subscriber Identity
TNI	:= Trusted Network Interpretation
TP	:= Transaction Processing
TÜV	:= Technischer Überwachungs-Verein
TVP	:= Time Variant Parameter
u.a.	:= unter anderem
UDP	:= User Datagram Protocol
URL	:= Uniform Resource Locator
VANS	:= Value Added Network Services; Mehrwertdienste
VDE	:= Verband Deutscher Elektrotechniker
VDMA	:= Verband Deutscher Maschinen- und Anlagenbau e.V.
vgl., Vgl.	:= Vergleiche
VLR	:= Visited Location Register
WAN	:= Wide Area Network
z.B.	:= zum Beispiel
ZKV	:= Zero-Knowledge-Verfahren
ZVEI	:= Zentralverband Elektrotechnik und Elektronikindustrie e.V.

ABBILDUNGSVERZEICHNIS

SEITE

TABELLENVERZEICHNIS

SEITE

1 Einleitung

1.1 Problemstellung

Zusätzlich zu den klassischen Produktionsfaktoren Boden, Arbeit und Kapital hat auch die Information im Produktionsprozeß an Bedeutung zugenommen. Und trotzdem es sich in den Gesellschaften der Industrienationen eingebürgert hat, wertvolle Gegenstände vor Unfall, Diebstahl und Mißbrauch zu schützen, scheint sich die Vorstellung, daß auch Information eines Schutzes bedarf, erst nach und nach durchzusetzen.[1]

Durch die zunehmende Internationalisierung der Handelsbeziehungen sowie dem Wandel vom Verkäufer- zum Käufermarkt hat sich in den letzten Jahren der Wettbewerbsdruck weltweit drastisch erhöht. Einer Sicherung der Wettbewerbsfähigkeit durch eine optimierte Gestaltung der Kommunikationsbeziehungen zu den Geschäftspartnern und modernen informationstechnischen (IT) Konzepten wie Client Server, Down Sizing, Right Sizing und Outsourcing folgen dabei eine erhöhte Flexibilität und kürzere Reaktionszeiten der Unternehmen – und auch eine größere Angreifbarkeit der Informationen.[2]

Aber auch die aktuellen Schlagworte wie „Information Highway“, „Electronic Cash“, „Telepräsenz“ oder „Cyberspace“, die uns eine problemlose Zukunft im Multimediazeitalter versprechen, stellen verstärkte und neue Angriffsflächen auf Informationen dar, was ein komplettes Überdenken der klassischen „Computersicherheit“ bedingt. Die Verwundbarkeit der modernen Informationssysteme trifft den zentralen Nerv unserer Wirtschaft und Gesellschaft als Einheit in einer globalen Wirtschaft mit weltweiten Infrastrukturen.[3] Damit stehen Wirtschaft und Gesellschaft vor einem schwierigen, aber unvermeidlichen Balanceakt zwischen „Öffnung“ und „Abschottung“, in dem auch ein Vermeiden der Entscheidung letztlich eine Entscheidung darstellt (jeder muß evtl. Konsequenzen, wie z. B. Verlust des Marktzugangs, selbst tragen).

Um eine Öffnung zu ermöglichen, müssen die Bedrohungspotentiale analysiert, wirksame Sicherheitsmaßnahmen entwickelt und adäquat den emergenten Informationssystemen in Form von Sicherheitskonzepten zugeordnet werden.

---

1 Vgl. Oppliger, Rolf: Computersicherheit: Eine Einführung, Braunschweig / Wiesbaden 1992, S. 1f.

2 Vgl. Strohmeyer, Rolf: Die strategische Bedeutung des elektronischen Datenaustausches, dargestellt am Beispiel von VEBA Wohnen, in: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, 44.Jg. (1992), H. 5, S. 462-475, hier S. 462f; **ebenso** Stiel, Hadi: Achillesferse Netzwerke, in: Datacom, 12. Jg. (1995), Heft 6, S. 44 - 48, hier S. 44.

3 Vgl. Becker, Lutz / Ehrhardt, Johannes: Die Datenautobahnen: Die Sicherheit der Highways, in: Datacom, 12. Jg. (1995), H. 4, S. 126 - 129, hier S. 126.

1.2 Gang der Untersuchung

Im zweiten Abschnitt dieser Arbeit wird zunächst der Begriff des Informationsnetzes eingegrenzt und anhand einer Bedrohungsanalyse ein Sollkonzept für die Sicherheit innerhalb eines solchen Informationsnetzes geschaffen, an dem die „Qualität“ des Sicherheitsbegriffes festgemacht wird. Diese konzeptuelle Grundlage wird dann kurz mit einem internationalen Standard für „offene Systeme“ abgeglichen, um mit Hilfe dieses Standards eine permanente Orientierungshilfe durch die nachfolgenden Abschnitte zu bilden.

Der dritte Abschnitt zeigt Hilfsmittel und Techniken, die als Einzelmechanismen zur Erfüllung der Sollkonzeption dienen können. Hierbei wird ein großes Gewicht auf den Bereich der Kryptographie gelegt, da dieser am leichtesten und günstigsten für „jedermann“ zu realisieren ist und die meisten „Dienste“ der Sollkonzeption erfüllt. Dieser Teil der Arbeit ist als Schwerpunkt zu sehen, da die aktuell vorhandenen und vor allem als sicher erachteten Bauteile für bestehende und potentielle Sicherheitskonzeptionen beschrieben werden und einen flächigen Überblick vermitteln.

Im vierten Abschnitt soll ein Überblick über die bestehenden Grundlagen für die sicherheitstechnische Beurteilung eines Sicherheitskonzeptes und einzelner Sicherheitskomponenten geschaffen werden, indem die gängigen drei Evaluationsmuster vorgestellt werden, die derzeit in Verwendung sind.

Ein Auszug der derzeit am Markt befindlichen Sicherheitskomponenten für Sicherheitskonzepte wird in Abschnitt fünf kurz vorgestellt, wobei die Komponenten größtenteils auf den im dritten Abschnitt vorgestellten Sicherheitsmechanismen aufbauen. Es werden Sicherheitskomponenten aufgezeigt, die in speziellen Diensten wie dem World Wide Web des Internet arbeiten, aber auch Komponenten für Übertragungsmedien und Übertragungsdienstleistungen sowie ein kurzer Einblick in Electronic-Cash-Anwendungen. Zudem soll am Beispiel eines Mobilfunknetzes ein Sicherheitskonzept in seiner Gesamtheit als mögliche Kombination am Markt befindlicher Sicherheitskomponenten exemplarisch vorgestellt werden.

Die Arbeit schließt mit einer kurzen zusammenfassenden Beurteilung der Ergebnisse ab, zu der eine prognostische Einschätzung der Entwicklung des Sicherheitsbedarfs und der Sicherheitstechnologien gewagt wird. Dabei wird auch kurz auf rechtliche Belange eingegangen, die auf die Effektivität bestimmter Sicherheitskomponenten einwirken.

2 Grundlagen Informationsnetze und -sicherheit

In diesem Abschnitt werden zunächst Grundlagen geschaffen, in dem die Begriffe „*Informationsnetz*“ und „*Sicherheitskonzept*“ in ihrem Umfeld dargestellt bzw. anhand eines Anforderungsprofils erarbeitet werden.

2.1 Informationsnetze

2.1.1 „Klassische“ Rechnernetze

Im Rahmen einer Klassifizierung von Rechnernetzen nach ihrer räumlichen Ausdehnung unterscheidet man traditionell lokale Netze (LAN, local area network) und Weitverkehrsnetze (WAN, wide area network).[1]

Ein *lokales Netz* liegt vor, wenn das Rechnernetz vollständig der Zuständigkeit eines Anwenders unterliegt und sich geographisch auf ein eng begrenztes Gebiet beschränkt, wie z.B. ein Gebäude oder ein Betriebsgelände.[2]

Weitverkehrsnetze sind Netze, bei denen geographisch entfernte, voneinander unabhängige Rechner über öffentliche oder private Netze (Trägernetze) miteinander verbunden sind. Zusätzlich bieten Betreiber von Trägernetzen neben der reinen Übertragungsleistung auch Dienste von selbst an das Netz angeschlossenen Rechnern an. In diesem Fall spricht man von *Mehrwertdiensten* (VANS, Value Added Network Services).[3]

Da heutzutage so gut wie alle Unternehmen, Regierungs- und akademische Organisationen ihre Datenverarbeitungssysteme (LAN’s und WAN’s) an eine Reihe von untereinander verbundenen Netzwerken anschließen, muß man dafür einen neuen Begriff bilden. Eine solche „Netzansammlung“ wird als *Internetzwerk*[4] bezeichnet.

2.1.2 Digitale Information

Das „*Informationsnetz*“ ist jedoch nicht nur auf den Bereich der Rechnernetze begrenzt, sondern umfaßt alle Bereiche *digitaler Kommunikation*, die in den letzten Jahren explosi-

---

[1] Vgl. Racke, Wilhelm F.: Netzarchitekturen, in: Lexikon der Wirtschaftsinformatik, Hrsg.: Mertens, Peter, 2. Aufl., Berlin, Heidelberg 1990, S. 292f.

[2] Vgl. Stahlknecht, P., Einführung in die Wirtschaftsinformatik, 7. Aufl., Berlin et al. 1995, S. 147f.

[3] Vgl. Ruland, Christoph: Sicherheit und Sicherheitsmanagement in offenen Kommunikationssystemen, in: Datacom, Netzwerkmanagement - Spezial -, 09/1990, S. 202-213, hier S. 203.

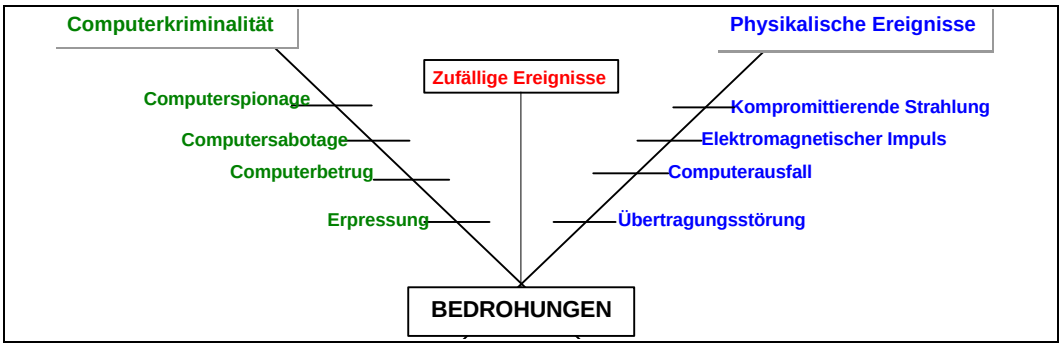
[4] Dies darf nicht mit dem Ausdruck *Internet* verwechselt werden. Das *Internet* bezieht sich auf einen bestimmten Zusammenschluß von Netzwerken, der zu einer Art globalem öffentlichen Netzwerk herangewachsen ist und eine der Einrichtungen sein kann, die eine Organisation zum Aufbau ihres Internetzwerkes nutzt. Vgl. Stallings, William: Network and Internetwork Security, Englewood Cliffs 1995, S. 2. (im folgenden zitiert als: Security)

onsartig gewachsen sind. Neben den Rechnernetzen werden auch Telefon- und Datenleitungen mit ihren Kommunikationsknoten (wie etwa ISDN-Nebenstellenanlagen), sowie zunehmend auch der Mobilfunk, als Trägernetz digitaler Information genutzt. Die digitalen Informationen stellen dabei elektronische Post, digitalisierte Sprache, digitalisierte Bilder oder gar digitalisierte Filme (Bewegtbilder) dar. Als Trägernetze seien hier das diensteintegrierende digitale Fernmeldenetz (ISDN), das für eine Zusammenfassung der Fernmeldedienste Fernsprechen, Fernkopieren (Telefax), Fernschreiben (Teletex / Telex) und Datenübertragung (wobei man sich hier wieder im Bereich WAN und Internetzwerk befindet) steht[1] und das GSM-Mobilfunknetz (GSM, Groupe Spécial Mobile), das für Fernsprechen, Telefax und im unteren Leistungsbereich auch für Datenübertragung steht, genannt.

2.2 Informationssicherheit

Ein Informationsnetz ist verschiedensten Bedrohungen[2] ausgesetzt, die seine Sicherheit einschränken. Inhalt dieser Arbeit ist nur ein Teil des Wortes Sicherheit, der sich in der deutschen Sprache schlecht herausarbeiten läßt – im Englischen wird zwischen *Security* (Sicherheit vor Datendiebstahl und -manipulation) und *Safety* (Sicherheit als Garantie der korrekten, permanenten Funktion) unterschieden.[3] Betrachtet man die Bedrohungspotentiale in Abbildung 1, so können wir Teile des rechten Astes als Repräsentanten des Information-Safety von der Behandlung ausschließen – nämlich den Computerausfall (z.B. durch Stromausfall, Wasser- od. Feuerschäden) und die Übertragungsstörung. Aber auch die restlichen physikalischen Ereignisse sollen vernachlässigt werden, da nur die

Abbildung 1: Bedrohungen für Informationsnetze



Quelle: Entworfen und gezeichnet: Verfasser, in Anlehnung an: Oppliger, Rolf, a.a.O., S. 15.

---

[1] Vgl. Ruland, Christoph: Sichere Kommunikation zwischen ISDN-Endgeräten, in: Datacom, 12. Jg. (1995), Heft 1, S. 108 - 116, hier S. 108.

[2] Eine *Bedrohung* ist eine mögliche Verletzung der Sicherheit eines Systems.

[3] Vgl. Kersten, H.: Sicherheit in der Informationstechnik, 2. Aufl., München 1995, S. 9ff; **ebenso** Thaller, Georg Erwin: Computersicherheit, DuD-Fachbeiträge 18, Braunschweig / Wiesbaden 1993, S. 10.

Information-Security analysiert wird, bei der die klassische Computersicherheit als technischer Sicherheitsaspekt (Abstrahlsicherheit und Schutz vor Elektromagnetischen Impulsen durch bauliche Maßnahmen) herausgelöst sein soll. Der verbleibende Teil der *Information-Security* wird auch als *Kommunikationssicherheit* (Communication-Secu-rity) bezeichnet.[1] Nachfolgend werden die „Zufälligen Ereignisse“ und die „Computer-kriminalität“ näher untersucht, wobei sich letztere in aktive und passive Angriffe aufteilt.

2.2.1 Zufällige Ereignisse

Zu den zufälligen oder unbewußten Bedrohungen gehören die Störungen, die bei jeder Datenübertragung auftreten können, also *Übertragungsfehler* wie z.B. durch Rauschen, Übersprechen von Nachbarkanälen, Wählgeräusche oder Leitungsunterbrechungen. Desweiteren kann es zu einem *Fehlrouting von Informationen* kommen, bei dem z. B. in den Zwischenknoten eines Vermittlungsnetzes die Information fehlgeleitet und an einen falschen Teilnehmer ausgeliefert wird, oder es gar zu einem Fehler beim Verbindungsaufbau kommt.[2] Zudem kommt die große Gruppe der *Fehler in Hard- und Software*, die heutzutage an der Tagesordnung sind. Das Gros der Software ist unverifiziert, so daß es durch die „normale“ Fehlermenge auf 100 Lines of Code zu situationsbedingtem Fehlverhalten kommen kann. Die Hardware kann durch defekte Bauteile (vor allem im Speicherbereich) und durch elektromagnetische Einflüsse aus der Umwelt zu falschem Verhalten führen.
Letztlich gibt es noch den „Schwachpunkt Mensch“, der für *Fehlbedienung* steht. Der Benutzer tätigt Zahlendreher bei der Eingabe von Rufnummern, löst versehentlich unbeabsichtigte Aktionen aus oder verwechselt zu versendende Dateien.[3] Nach Umfragen ist dies immer noch der prozentual größte Beeinträchtigungspunkt bei Netzwerken.[4]
Ein großes Problem ist es allerdings, die auftretenden Fehler einer der oben genannten „Zufälligkeiten“ zuzuschreiben oder den Verdacht auf einen der unten aufgeführten Angriffsformen zu lenken. Man kann die zufälligen Fehler nicht verhindern, muß aber versuchen, die Wirkung der durch sie ausgelösten Schäden zu minimieren.

---

[1] Vgl. Russell, Deborah / Gangemi, G.: Computer Security Basics, Sebastopol 1991, S. 17; **ebenso** vgl. Rihaczek, Karl: Datenschutz und Kommunikationssysteme, Braunschweig 1981, S. 5f.

[2] Vgl. Ruland, Christoph: Datenschutz in Kommunikationssystemen, Pulheim 1987, S. 16 (nachfolgend zitiert als: Datenschutz).

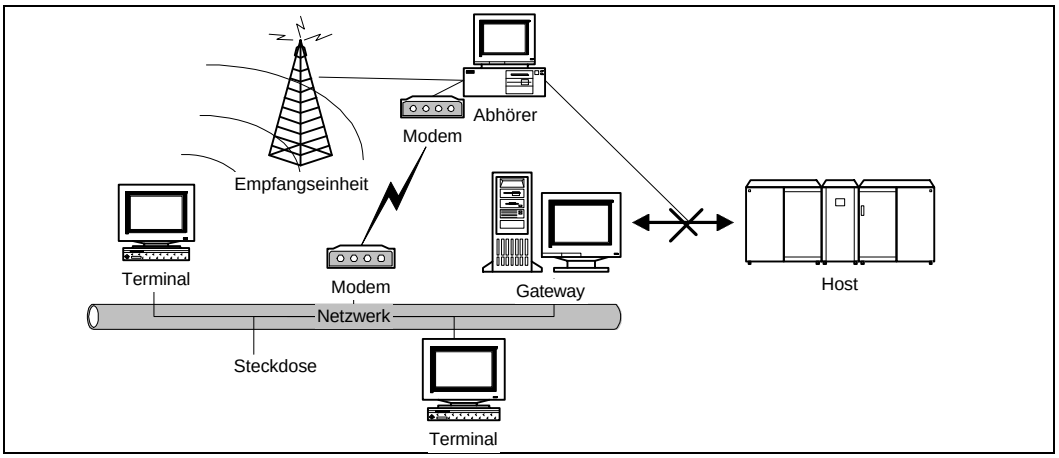
[3] Vgl. Ruland, Christoph: Informationssicherheit in Datennetzen (im folgenden zitiert als: Info.sicherheit), Bergheim 1993, S. 26ff.

[4] Vgl. Heinrich, Wilfried: Es lebe das Hoffnungsprinzip, in: Datacom, 13. Jg. (1996), Heft 1, S. 58 - 60, hier S. 59.

2.2.2 Passive Angriffe

Die passiven Angriffe sind bewußt und gezielt durchgeführte Bedrohungen der Datenkommunikation und bewirken keine Veränderung der übertragenen Information, sondern dienen nur der unerlaubten Informationsgewinnung. Sie sind dem Bereich Computerspionage und Erpressung (s. Abb. 1) zuzurechnen. Die Durchführung eines passiven Angriffs läßt sich in Abbildung 2 ablesen und geschieht durch Klemmen oder Induktionsschleifen an der Leitung, das Abfangen der elektromagnetischen Strahlung der Endgeräte (hier z. B. ein Terminal), die Nutzung freier „transparenter" Steckdosen mancher Netze (diese Flexibilität und Robustheit wird aus Sicht der Netzsicherheit zum Nachteil) und den Mißbrauch von Einwählpunkten via Modem.[1] Natürlich kann auch jedes unge-

Abbildung 2: Passive Angriffe durch Abhören



Quelle: Entworfen und gez.: Verfasser, in Anlehnung an: Ruland, Christoph: Info.sicherheit, a.a.O., S. 21.

schützte Terminal eines befugten Teilnehmers genutzt werden. Folgende passive Angriffe können unterschieden werden:[2]

1. **Abhören der Daten** – Hierbei werden einfach unerlaubt Informationen (z.B. Entwicklungsunterlagen, Paßwörter usw.) durch Abhören beschafft.
2. **Abhören der Teilnehmer-Identitäten** – Es wird in Erfahrung gebracht, welche Teilnehmer untereinander eine Verbindung aufbauen, wie groß die ausgetauschte Nachrichtenmenge ist, und welche Leistungsmerkmale angefordert werden (so lassen sich bei ISDN gewählte Gerätetypen und spezifische Dienste erkennen).

   Mit den gewonnenen Informationen sind oft Rückschlüsse auf den Inhalt der Nachricht oder das Verhalten der Teilnehmer möglich.

---

[1] Vgl. Moayeri, Behrooz: Netzwerk-Koppelelemente im Dienste der Sicherheit, in: Datacom, 13. Jg. (1996), Heft 1, S. 68 - 73, hier S. 69.

[2] Vgl. Pohlmann, Norbert: Durch die Maschen geschlüpft - Risiken im Netz, in: KES, 11. Jg. (1995), Heft 4, S. 13 - 21, hier S. 14ff.

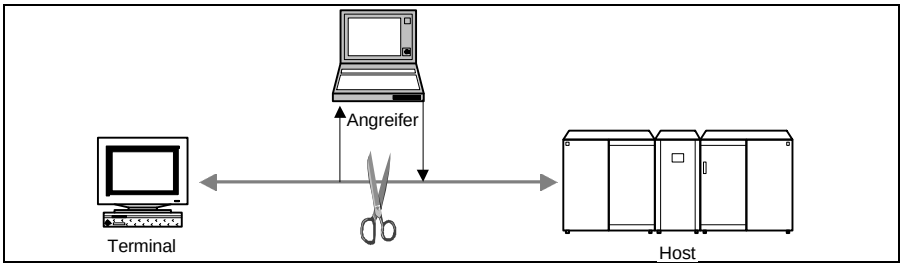
3. **Verkehrsflußanalyse** - Es ist möglich, das Abhören der Daten und Teilnehmeridentitäten wirksam zu verhindern (s. Kapitel 3). Es besteht dann aber immer noch die Gefahr der Verkehrsflußanalyse, bei der analysiert wird, zu welchem Zeitpunkt in welchem Umfang und mit welcher Struktur eine Kommunikation stattgefunden hat. Bei manchen Applikationen (z. B. Börse, Militär) lassen solche Informationen Rückschlüsse auf den Inhalt oder folgende Reaktionen zu.

Man kann abschließend allgemein zu den „Passiven Angriffen“ sagen, daß sie effektiv durch geeignete Maßnahmen verhinderbar sind.

2.2.3 Aktive Angriffe

Auch bei dieser Angriffsform sind die Bedrohungen bewußt durchgeführt, es kommt jedoch zu einer Verfälschung / Veränderung (= Manipulation) des Informationsstroms und / oder des Betriebs der Kommunikation, was ein falsches Verhalten des Empfängers veranlaßt. Damit werden die Delikte Computersabotage, Computerbetrug und auch Erpressung (s. Abb. 1) realisiert. Aktive Angriffe durch Dritte geschehen durch Auftrennen der Übertragungsstrecke und Dazwischenschaltung einer Station, die die Übertragungsprotokolle emuliert (s. Abb. 3). Es kann jedoch generell zwischen zwei Arten von Angreifern unterschieden werden – Kommunikationspartner und Dritte.[1]

Abbildung 3: Aktiver Angriff durch Auftrennen



Quelle: Pohlmann, N.: Sicherheitsdienste in Paket-Netzen, in: Sicherheit in netzgestützten Informationssystemen, SECUNET ’92, Hrsg.: Lippold, H. / Schmitz, P., Braunschweig 1992, S. 477.

2.2.3.1 Aktive Angriffe durch Kommunikationspartner

Hierbei kann es zu folgenden beiden Angriffsformen kommen:[2]

1. **Maskerade** – Der „legale“ Kommunikationspartner täuscht eine falsche Identität vor und erschleicht sich so Informationen und Benutzerrechte dieser „Identität“. Nach dem Vortäuschen einer falschen Identität können auch fremde Betriebsmittel unerlaubt oder in einer nicht zulässigen Weise genutzt werden.

---

[1] Vgl. Raubold, Eckart: Sicherheitsaspekte in der „offenen“ Telekommunikation, in: Entwicklungslinien der Telekommunikation, ITG Fachbericht 123, Hrsg.: ITG, Berlin 1993, S. 75 -81, hier S. 77.

[2] Vgl. Schläger, Uwe: Datenschutz in Netzen, in: DuD, Jg. 1995, Heft 5, S. 270 -275, hier S. 271.

2. **Leugnen von Kommunikationsbeziehungen** – Die Sendung bzw. der Empfang von Informationen wird durch den Partner geleugnet, was rechtsgültige geschäftliche Kommunikation (z.B. Bestellung von Waren und deren Bestätigung im Rahmen von Electronic Data Interchange (EDI)) problematisiert.

2.2.3.2 Aktive Angriffe durch Dritte

Bedrohungen durch Dritte sind:[1]

1. **Wiederholung oder Verzögerung einer Information** – Durch diese Angriffsform kann es zu einer Irritation und nachfolgender Fehlaktion des Empfängers kommen. Möglich ist z.B. auch die Wiederholung von Geldüberweisung oder einer abgefangenen Login-Prozedur. Auch durch eine Verzögerung können Sachverhalte verfälscht und Fehlentscheidungen ausgelöst werden.
2. **Modifizieren einer Information** – Bei der Modifikation muß man das Einfügen, Löschen und Ändern von Daten innerhalb der Nachrichten unterscheiden. Dadurch soll ebenfalls der Empfänger zu einer falschen Reaktion veranlaßt werden. Durch Einfügen oder Löschen von Worten wie „kein“ oder „nicht“ kann z.B. der Aussageninhalt der Nachricht umgekehrt werden. Das Ändern z.B. einer Kontonummer löst eine Fehlüberweisung aus. Unter dieser Angriffsform soll auch das Modifizieren von Rechten und Attributen gefaßt werden, bei dem sich der Angreifer einen Operatorstatus verschafft und damit weitere unerlaubte Modifikationen durchführen kann.
3. **Sabotieren des Kommunikationsnetzes** – Dieser Angriff zielt auf die Verfügbarkeit und Betriebssicherheit eines Systems. Das System (oder der Teilnehmer) wird durch ständige erneute Adressierung blockiert und dadurch letztendlich vom Rest des Kommunikationssytems isoliert. Dieses Vorgehen wird auch als „Denial of Service“ bezeichnet.

2.2.3.3 Aktive Angriffe durch bösartige Programme

Sowohl durch „maskierte“ Kommunikationspartner als auch durch Dritte kann es zum Einschleusen von Programmen kommen, die zu Computeranomalien führen. „*Computeranomalien gehören zur Gefahrenklasse der Manipulation. Sie stören die Ordnungsmäßigkeit der Datenverarbeitung, indem sie Daten und Programme verändern oder zerstören und zusätzliche Funktionen ausführen.*“ [2]

---

[1] Vgl. Pohlmann, Norbert: Vertrauliche Kommunikation über öffentliche Netze, in: Datacom, 11. Jg. (1994), Heft 8, S. 126 - 130, hier S. 127.

[2] Brobeil H.: Software-Angriffe auf PC’s und Netzwerke, Oldenbourg 1992, S. 41.

Nachfolgend sollen die drei Hauptkategorien von Anomalien kurz dargestellt werden:[1]

- **Trojanische Pferde** – Darunter versteht man Programme, die neben der geplanten Funktion zusätzlich (vom Programmierer beabsichtigte) Schadenfunktionen ausführen können (z.B. fiktive Login-Maske, um im Hintergrund die eingegebenen Paßwörter aufzuzeichnen und nach der Eingabe mit einer Meldung „falsches Paßwort“ an das richtige Login-Programm abzugeben). Man nennt solche „Trojanischen Pferde“ auch Spoofing-Programme. Ein „Trojanisches Pferd“ ist ein selbständiges Programm, das ortsfest ist und sich nicht vermehrt.
- **Würmer** – Hierbei handelt es sich um eigenständige, ortsunabhängige Programme, die sich durch Systemfehler oder Sicherheitslücken in Netzwerken fortpflanzen. Die Schadenfunktion kann im Transport eines „Trojanischen Pferdes“ oder im *Denial of Service* (also der Leitungsblockierung, s.o.) liegen.
- **Viren** – Ebenso wie Würmer sind auch Viren in der Lage, sich zu reproduzieren. Sie sind jedoch nicht eigenständig, sondern benötigen einen Wirt, was bedeutet: „*Ein Virus ist ein Programmstück, dessen Ausführung bewirkt, daß es sich als Ganzes oder eine modifizierte Version seiner selbst in ein anderes Programm kopiert.*“[2] Ein aktuelles Problem stellen die sogenannten *Daten-Viren* dar, die sich an MS-Word-Makros oder Postscriptsequenzen hängen und ganze Benutzerdatenbestände gefährden.

2.3 Sicherheitskriterien und -dienste

In den vorangegangenen Abschnitten wurden die potentiellen Bedrohungen für Informationsnetze dargestellt. Ausgehend von diesen Bedrohungen soll jetzt die Informations- / Kommunikationssicherheit konkret an Ersatzkriterien festgemacht werden, um daraus ableiten zu können, welche Dienste ein Informationsnetz bereitstellen muß, um als „sicher“ zu gelten. Die geforderten vier Sicherheitskriterien sind im einzelnen:[3]

- **Vertraulichkeit** ↫ Informationsvertraulichkeit
  ⇒ Schutz persönlicher oder geschäftswichtiger Daten
  ⇒ Anonymität der Nutz- und Vermittlungsdaten
- **Integrität** ↫ Partnergewißheit (Identifikation)
  ⇒ Zugangs-, Zugriffskontrolle

---

[1] Vgl. Kersten, Heinrich: Einführung in die Computersicherheit, München et al. 1991, S. 31ff.
[2] Brobeil H., a.a.O., S. 55.
[3] Vgl. Klein, Stefan: Informationssicherheit bei der Kommunikation von Versicherungen mit Dritten, in: Sicherheit in Informationssystemen, Proceedings des BIFOA-Kongresses SECUNET ’91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 169 - 183, hier S. 174f.

⇒ Integrität der gesendeten Daten

⇒ Sende- und Empfangsbeweis

- **Verfügbarkeit** ➧ Funktionalität

  ⇒ Betriebskontinuität

- **Authentität** ➧ Nachweisbarkeit der Urheberschaft

  ⇒ Nachweisbarkeit von Kommunikationsvorgängen

  ⇒ Rechtssicherheit der Kommunikation

  ⇒ Zertifizierung

Anhand dieser Sicherheitskriterien und ihrer Unterpunkte sollen nun die technologieunabhängigen Sicherheitsmaßnahmen, die *Sicherheitsdienste*, dargestellt werden. Jeder Dienst ist als *Modul* zu verstehen, der nach Bedarf einzeln oder in Kombination unter Verwendung der in Kapitel 3 dargestellten Technologien als *Sicherheitskonzept* zum Tragen kommt.[1] Das *Sicherheitskonzept* definiert dann die Grenzen akzeptablen Verhalten und die Reaktion auf Übertretungen bezüglich der Netzsicherheit. Folgende Sicherheitsdienste stehen zur Verfügung:[2]

1. **Vertraulichkeit** – Dieser wichtigste Dienst soll Schutz vor unbefugtem Lesen der übertragenen oder gespeicherten Informationen bieten und kann sich auf eine ganze Verbindung, einzelne Dateneinheiten oder nur auf bestimmte Felder von Dateneinheiten beziehen.
2. **Verhinderung einer Verkehrsflußanalyse** – Neben der Vertraulichkeit ein weiterer Dienst zur Verhinderung „Passiver Angriffe“, der Informationsgewinnung im Rahmen einer Verkehrsflußanalyse verhindern soll (s. o.).
3. **Erkennung der Datenunversehrtheit** – Dieser Dienst soll *Informationsmodifikation* durch „Aktive Angriffe“ oder Übertragungsfehler ausschließen und bei Bedarf ein *Recovery* (automatische Wiederholung der gestörten Dateneinheiten) auslösen. Dieser Dienst arbeitet auch verbindungsbezogen, für einzelne Dateneinheiten oder nur für Felder einzelner Dateneinheiten.
4. **Authentikation des Kommunikationspartners** – Mit diesem Dienst soll die Angriffsform „Maskerade“ abfangen werden. Man kann zwischen ein- und gegenseitiger Authentikation unterscheiden.

---

[1] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 33.

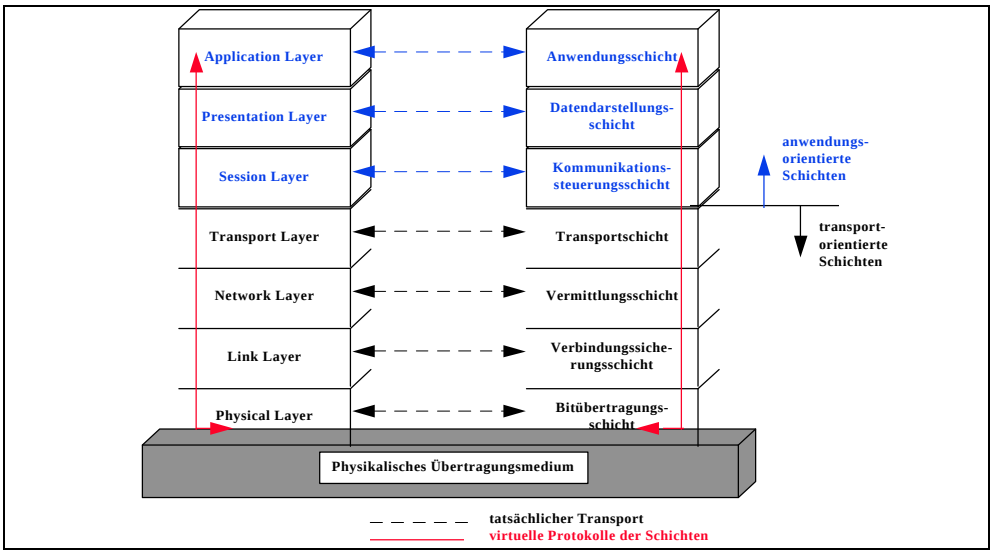
[2] Vgl. Stallings, William: Sicherheit im Datennetz, München, London, et al. 1995, S. 24ff; (im folgenden zitiert als: Datennetz); **ebenso** Weck, Gerhard: Sicherheit von Client/Server-Systemen, in: DuD, Jg. 1995, Heft 3 - 5, S. 156 - 163, 224 - 231 u. 276 - 283, hier S. 224ff.

5. **Authentikation des Datenursprungs** – Dieser Dienst ist weitgehender als der Letzte, bei dem ja nur der Partner geprüft wird, aber nicht die danach in der Folgephase ausgetauschten Informationen. Dieser Dienst schließt das „Einschleusen“ von Daten aus.
6. **Urhebernachweis** – Der Empfänger erhält eine rechtsgültige Sendebescheinigung, damit der Absender später die Nachricht nicht verleugnen kann.
7. **Empfängernachweis** – s. Punkt 6 mit rechtsgültiger Empfangsbescheinigung
8. **Zugangs- und Zugriffskontrolle** – Dieser Sicherheitsdienst schützt vor unbefugtem Nutzen von Betriebsmitteln und setzt eine erfolgreiche Authentikation des Kommunikationspartners und des Datenursprungs voraus.
9. **Aufrechterhaltung des Kommunikationsbetriebs** – Dieser Dienst soll ein „*Denial of Service*“ verhindern und einen unterbrechungsfreien Betrieb ermöglichen.

2.4 Die ISO-OSI Sicherheitsarchitektur

Das Modell, das sich durch diese Arbeit wie ein roter Faden zieht, ist die ISO-Sicherheitsarchitektur (ISO, International Standards Organization). Dieser „Faden“ muß allerdings manchmal unterbrochen werden, um zusätzliche Kapitel einzufügen – nämlich

Abbildung 4: Das ISO-OSI Referenzmodell



Quelle: Kauffels, F.-J.: Schwachstellen der Informationssicherheit in Netzen, in: DuD im Wandel der Informationstechnologien, Hrsg.: Spies, P. P., Berlin 1985, S. 51 - 69, hier S. 66.

die, die bestimmte Technologien beschreiben. Die ISO-Sicherheitsarchitektur beschreibt Sicherheitsaspekte in offenen Kommunikationssystemen. Es werden in allgemeiner Weise vierzehn *Sicherheitsdienste*[1] (Security-Services) und acht *Sicherheitsmechanismen*

[1] Zwei der neun in Abschnitt 2.3 genannten Sicherheitsdienste wurden von der ISO weiter aufgegliedert.

(Security Mechanisms) sowie die Beziehungen zwischen Diensten, Mechanismen und den Schichten des OSI-Referenzmodells (s.o. Abb. 4) als mögliche Maßnahmen der Kommunikationssicherheit dargestellt (OSI, Open Systems Interconnection).[1] Die „Security Architecture“ wurde 1989 als zweiter Teil [ISO 7498-2] dem OSI-Refe-renzmodell, das 1984 in der ISO-Norm 7498 veröffentlicht wurde, angehängt. Tabelle 1 zeigt dazu, auf welcher Schicht die Anordnung der Dienste laut der Sicherheitsarchitektur sinnvoll erscheint, und in welchen Bereichen bereits Normungsaktivitäten bestehen.[2]

Tabelle 1: Sicherheitsdienste in den OSI-Schichten

	OSI-Schichten						
Sicherheitsdienste	1	2	3	4	5	6	7
Authentikation des Kommunikationspartners			+	+			+
Authentikation des Datenursprungs			+	+			+
Zugangs-, Zugriffskontrolle			+	+			+
Vertraulichkeit b. verbindungsorientiertem Kommunikationsbetrieb	+	+	+	+		+	+
Vertraulichkeit bei verbindungslosem Kommunikationsbetrieb		+	+	+		+	+
Vertraulichkeit bei einzelnen Dateneinheiten						+	+
Verhinderung einer Verkehrsflußanalyse	+		+			+	+
Erkennung der Datenunversehrtheit mit Recovery				+			+
Erkennung der Datenunversehrtheit ohne Recovery			+	+			+
Verbindungsorientierte Datenunversehrtheit b. Datenfeldern							+
Verbindungslose Datenunversehrtheit			+	+			+
Verbindungslose Datenunversehrtheit bei Datenfeldern							+
Urhebernachweis							+
Empfängernachweis							+

\+ = Realisierung der Sicherheitsdienste = ISO-Normungsaktivitäten

Quelle: Fumy, Walter: Network Security, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 211 - 225, hier S. 214.

3 Mechanismen für Sicherheitskonzepte

Die oben technologieunabhängig vorgestellten Sicherheitsdienste sollen nun durch spezielle Technologien – oder *Sicherheitsmechanismen* – realisiert werden. In diesem Kapitel sollen alle aktuellen zur Verfügung stehenden Mechanismen dargestellt werden, wobei sich nicht auf die Sicherheitsmechanismen der OSI-Sicherheitsarchitektur beschränkt werden soll. Während die OSI-Sicherheitsmechanismen die Sicherheitsdienste in das Endsystem auf den einzelnen OSI-Schichten integrieren, werden andere Mechanismen als Hardwaresicherheitseinrichtung schnittstellenneutral zwischen das Endsystem und den Netzanschluß geschaltet. Darauf wird bei den einzelnen Mechanismen näher eingegangen.

---

[1] Vgl. Verschuren, Jan: ISO-OSI Security Architecture, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 179 - 192, hier S. 179f.

[2] Vgl. Hembach, Friedrich: IT-Sicherheitspolitik im Datex-P, in: BSI-Forum, 2. Jg. (1994), Heft 3, S. 56 - 58, hier S. 57; **ebenso** Mund, Sibylle / Rieß, H. P.: Kryptographische Protokolle für Sicherheit in Netzen, in: DuD, Jg. 1992, Heft 2, S. 72 - 80, hier S. 74.

3.1 Kryptographie

Kryptographie ist die Wissenschaft von den Methoden der Verschlüsselung und Entschlüsselung von Daten. Diese mathematischen Methoden werden aber nicht nur zur Verheimlichung von Informationen, sondern auch zur Erkennung der Datenunversehrtheit, zur Authentikation der Kommunikationspartner und des Datenursprungs sowie für Urheber- und Empfängernachweise eingesetzt – kurz: nach ISO 7498-2 können alle definierten Sicherheitsdienste außer der Zugriffskontrolle mit Hilfe von Verschlüsselungsverfahren und digitale Signatur realisiert werden.[1] Das Ziel jeder Verschlüsselung ist es aber grundsätzlich, Daten in einer solchen Weise einer mathematischen Transformation zu unterwerfen, daß es einem Angreifer, der die Daten oder eine Kopie in seinen Besitz bringt, nicht möglich ist, die Originaldaten (*Klartext*) aus den transformierten Daten zu rekonstruieren. Damit die verschlüsselten Daten (*Schlüsseltext*) für ihre legalen Nutzer noch verwendbar bleiben, muß es diesen möglich sein, durch Anwendung einer inversen Transformation (*Entschlüsselung*) wieder den Klartext zu erhalten.[2]

Dargestellt werden nur Methoden, die ausschließlich mit „unüberwindbarem“[3] Aufwand zu brechen sind, auf den Bereich der Kryptoanalyse (aktive Analyse, um die Krypto-verfahren zu brechen) wird nicht eingegangen.

3.1.1 Symmetrische Verschlüsselung

Bei Kryptosystemen mit symmetrischem Algorithmus wird nur *ein Schlüssel* verwendet, sowohl für die Ver- als auch die Entschlüsselung. Wer den Schlüssel hat, kann Klartext in Schlüsseltext und umgekehrt transformieren, so daß der Schlüssel unbedingt geheimgehalten werden muß. Daher nennt man dieses Verfahren auch *Private-Key-Verschlüs-selung*, dessen grober Ablauf vereinfacht in Abbildung 5 dargestellt ist. Großer Vorteil dieser Verfahren ist ihre unschlagbar hohe Geschwindigkeit, die später beschriebene Verfahren um Faktor 100 - 10.000 übertrifft. Der Einsatz eines Einzelschlüssels stellt jedoch den größten Nachteil dieser Verschlüsselungsart dar, denn das Schlüsselmanagement gestaltet sich schwierig. Bei N Kommunikationspartnern werden für eine paarweise sichere Kommunikation und ein *sicheres* Schlüsselmanagement (Verteilung / Zustellung (s.u. Abschnitt 3.1.5)) $\frac{N(N-1)}{2}$ Schlüssel benötigt.[1]

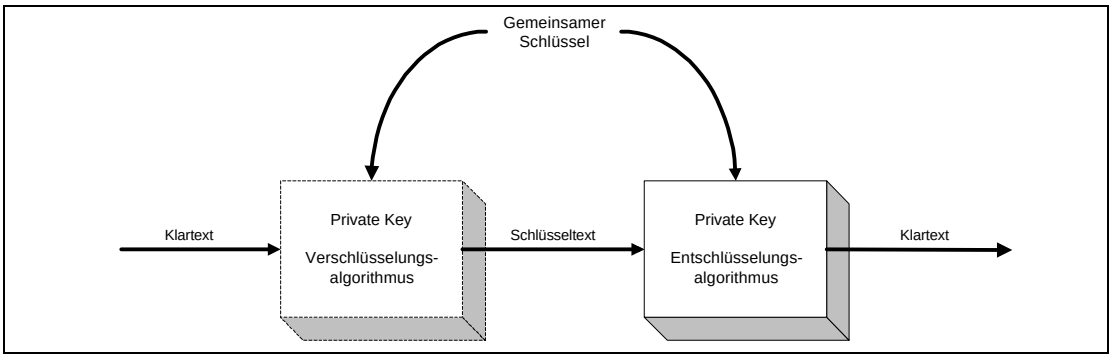
---

[1] Vgl. Papst, Markus: OSI und Security, in: Datacom, 10. Jg. (1993), Heft 3, S. 112 - 115, hier S. 112.

[2] Vgl. Hagemann, H. / Rieke, Andreas: Datenschlösser. Grundlagen der Kryptologie , in: c’t Magazin für Computertechnik, Jg. 1994, Heft 8, S. 230 - 238, hier S. 230f.

[3] Algorithmen, die keine oder nur unwesentliche Schwächen gegenüber Angriffen haben.

Abbildung 5: Vereinfachtes Modell der Private-Key-Verschlüsselung



Quelle: Stallings, William, Datennetz, a.a.O., S. 38.

Symmetrische Verfahren lassen sich wiederum in zwei Gruppen einteilen:[2]

1. **Stromchiffren** (Bit-Strom-Chiffrierung) – Hierbei wird der Klartext Bit für Bit verschlüsselt. Der geheime Schlüssel wird in einen *Pseudo-Zufallsgenerator*[3] eingegeben, der dann eine große Folge binärer Signale erzeugt. Die Periode der Folge muß dabei größer sein als die zu verschlüsselnde Nachricht. Diese Output-Folge wird dann mit dem Klartext (bzw. dem Schlüsseltext auf Entschlüsselungsseite) verknüpft, i.a. durch XOR (E**X**klusives **OR**, logische Antivalenz – mathematisches Zeichen: ⊻). Dadurch wird erreicht, daß gleiche Teile des Klartextes nicht identisch im Schlüsseltext auftauchen. Das *One-Time Pad* oder auch *Vernam-Verfahren*, das als einzige Verschlüsselung mit absoluter Sicherheit gilt, ist eine Stromchiffre. Es nutzt jeden Schlüssel allerdings nur einmal und die Klartextnachricht darf nicht länger als der Schlüssel sein – was einen praktischen Einsatz weitgehend ausschließt.
2. **Blockchiffren** – Bei dieser Technik wird der Klartext in Blöcke fester Länge (häufig 64 Bit) eingeteilt, die dann in einem Schritt transformiert werden. Ein Klartextblock wird dabei durch einen Schlüsseltextblock substituiert, in dem ein durch den Schlüssel festgelegter Algorithmus die Verschlüsselung der einzelnen Blöcke vornimmt. Für den Fall, daß die Länge des Klartextes kein Vielfaches der Blockgröße ist, muß der letzte Block aufgefüllt werden – dazu bedient man sich sog. Padding-Mechanismen, die bit- oder

---

[1] Vgl. Luckhard, Norbert: Kryptologische Begriffe und Verfahren, in: c't Magazin für Computertechnik, Jg. 1996, Heft 12, S.110 - 113, hier S. 112f.

[2] Vgl. Wähner, Gerd W.: Datensicherheit und Datenschutz, Düsseldorf 1993, S. 227ff; **ebenso** Ungerer, Bert: Knackfreundlich. Schnelle Online-Plattenverschlüsselung birgt Risiken, in: c't Magazin für Computertechnik, Jg. 1994, Heft 6, S. 184 - 190, hier S. 185ff.

[3] Computer sind nicht in der Lage, echte Zufallszahlen zu erzeugen, da sie mit festgelegten Verfahren arbeiten, die nur eine endliche Zahl von Zuständen annehmen können, was eine Periodizität der Zufallszahlen bedingt. Es werden spezielle Algorithmen eingesetzt, die Zufallszahlen „möglichst zufällig" erzeugen sollen – es sind allerdings nur Pseudo-Zufallszahlen.

oktettorientiert mit binären Werten auffüllen. Blockchiffren können in den folgenden vier Betriebsmodi betrieben werden:[1]

- **ECB** (Electronic Code Book) – In diesem Modus wird jeder Klartextblock mit dem vorhandenen Schlüssel auf die gleiche Methode verschlüsselt, was separate Entschlüsselung einzelner Blöcke für Angreifer möglich macht.
- **CBC** (Cipher Block Chaining) – Im Gegensatz zum ECB wird hier eine Verbindung zwischen den einzelnen Chiffreblöcken hergestellt, indem das Resultat einer Verschlüsselungsoperation dazu benutzt wird, den nächsten Block durch bitweise XOR-Verknüpfung zu modifizieren und so eine Einzelblockentschlüsselung zu unterbinden.
- **CFB** (Cipher FeedBack) – Hierbei werden jeweils x Bits ($1 \leq x \leq N$) einer Nachricht verschlüsselt. Bei $x = 1$ kommt es zu einer Stromverschlüsselung, bei $x = N$ zu einer verketteten Blockverschlüsselung (N entspricht der Blocklänge des Algorithmus). Für je x zu verschlüsselnde Bits ist eine komplette Blockchiffrierung nötig, so daß dieser Modus nicht so effizient wie ECB oder CBC ist.
- **OFB** (Output Feedback) – Dieser Modus arbeitet ähnlich wie der CFB, es werden jedoch die Outputvariablen der Verschlüsselungsoperation als Input für die nächste Verschlüsselungsoperation zurückgeführt.

In den nachfolgenden Unterabschnitten werden typische symmetrische Algorithmen vorgestellt, wobei der Data Encryption Standard einführend etwas ausführlicher dargestellt werden soll.

3.1.1.1 Data Encryption Standard (DES)

Der DES-Algorithmus wurde erstmals 1974 von der IBM veröffentlicht und ist als ANSI-Standard 1977 vom NBS (= National Bureau of Standards), dem heutigen National Institute of Standards and Technology (NIST), normiert (ANSI X3.92-1981).

Es handelt sich um eine Blockchiffre, welche 64 Bits Klartext in 64 Bits Schlüsseltext und umgekehrt überführt. Die Schlüssellänge beträgt ebenfalls 64 Bit, wobei jedoch nur 56 Bit hiervon signifikant sind, während die restlichen 8 Bits Paritätsbits sind.[2] Der prinzipielle Aufbau läßt sich in Abbildung 6 erkennen. Der Klartext wird mit Hilfe einer vom Schlüssel unabhängigen Permutation transformiert, um den semantischen Zusammenhang aufeinan-

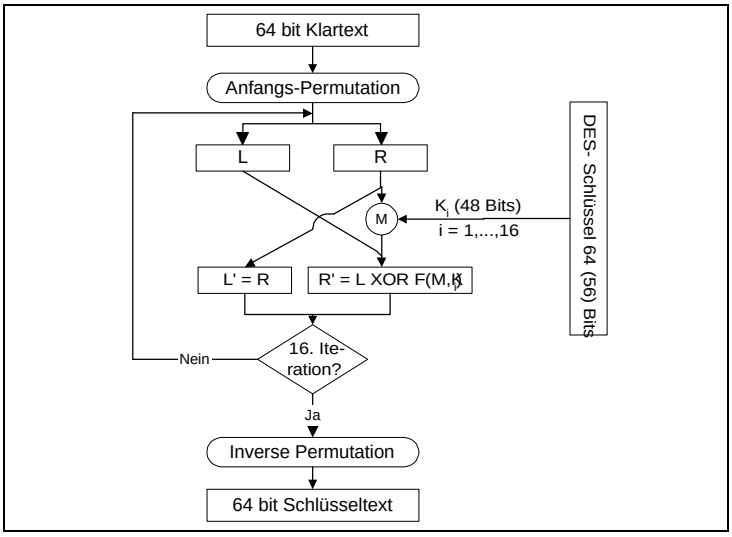
---

[1] Vgl. Weck, Gerhard: Datensicherheit, Stuttgart 1984, S. 291ff; **ebenso** Krallmann, Hermann: EDV-Sicherheitsmanagement, Berlin 1989, S. 292ff.

[2] Vgl. Universität-Gesamthochschule Siegen: Data Encryption Standard, Security Server, 17.11.1996 URL=http://www.uni-siegen.de/security/krypto/des.html

derfolgender Bits und Bytes zu beseitigen. Als nächstes beginnt eine Verarbeitung, die aus 16 Iterationsschritten besteht, in denen zuerst der 64-Bit-Klartext-block in eine linke (L) und eine rechte (R) Hälfte geteilt wird. Nach jedem Schritt wird die rechte Hälfte des teilweise verschlüsselten Blocks zur linken Hälfte des nächsten Schrittes. Die linke Hälfte wird dagegen nach jedem Schritt bitweise XOR mit dem Output einer aus nichtlinearen Substitutionen und Permutationen zusammengesetzten Funktion M verknüpft. Die Funktion M hängt von der rechten Hälfte des teilweise verschlüsselten Blockes und einem 48 Bit langen Arbeitsschlüssel K_i ab. K_i wird für jede Runde durch eine zusätzliche Schlüsselauswahlfunktion aus den 56 Bits des DES-Schlüssels abgeleitet. Das Ergebnis der XOR-Verknüpfung wird die rechte Hälfte des nächsten Schrittes. Nach der 16. Iteration werden noch einmal beide Hälften miteinander vertauscht und auf den resultierenden 64-Bit-String wird die zur Anfangs-Permutation inverse Permutation angewendet. Das Ergebnis bildet der 64-Bit-Schlüsseltextblock.[1]

Abbildung 6: Prinzipieller Aufbau des DES-Algorithmus



Quelle: Preneel, Bart: Computer Security and Industrial Cryptography, Berlin 1991, S. 87.

DES läßt sich sowohl hardwaremäßig, wie auch softwaremäßig implementieren. Bei den neuesten Hardware-Implementierungen liegen die Verschlüsselungsraten schon im Bereich GBit/s. Eingesetzt wird das DES-Verfahren insbesondere in Finanz-Applikationen und kann als Quasi-Standard bezeichnet werden, wenngleich es aufgrund steigender Rechnerperformance langsam angreifbar wird.[2]

---

[1] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 45f. **ebenso** Knobloch, H.-J. / Horster, Patrick: Eine Krypto-Toolbox für Smartcards, in: DuD , Jg. 1992, Heft 7, S. 353 - 361, hier S. 355.

[2] Vgl. Kyas, Othmar: Sicherheit im Internet: Risikoanalyse - Strategien - Firewalls, Bergheim 1996, S. 170.

3.1.1.2 Triple-DES (3DES)

Um die Schwäche des DES mit seiner Schlüssellänge von 56 signifikanten Bits bzw. 48 Bits bei den Arbeitsschlüsseln auszugleichen, wurde von Merkle und Hellman der 3DES entwickelt, der den Ursprungsalgorithmus – und somit die verfügbaren Software- und Hardwareimplementationen – beibehält, jedoch die Schlüssellänge erhöht. Der 3DES ist unter anderem Bestandteil der IBM „Common Cryptographic Architecture“ und es gibt ihn mit doppelter oder dreifacher Schlüssellänge (wobei sich die Rechenzeit der Ver- bzw. Entschlüsselung entsprechend erhöht).

3DES mit doppelter Schlüssellänge

Bei dieser Variante besteht der Schlüssel K aus zwei aneinandergefügten DES-Schlüs-seln, d.h. 128 Bits, von denen 112 Bits signifikant sind ($K := K_{left} // K_{right}$)[1].

Die Verschlüsselung erfolgt nach folgendem Muster:

1. DES-Verschlüsselung mit dem ersten Halbschlüssel K_{left} ,
2. DES-Entschlüsselung mit dem zweiten Halbschlüssel K_{right} und noch eine
3. DES-Verschlüsselung mit dem ersten Halbschlüssel K_{left} .

Die Entschlüsselung erfolgt symmetrisch (entschlüsseln, verschlüsseln, entschlüsseln).[2]

3DES mit dreifacher Schlüssellänge

Bei dieser Version wird ein dreifacher Schlüssel K der Länge 192 Bit (168 Bit signifikant) verwendet, der aus drei einfachen DES-Schlüsseln zusammengesetzt ist ($K := K_{left} // K_{center} // K_{right}$). Die Verschlüsselung geschieht wie folgt:

1. DES-Verschlüsselung mit K_{left} ,
2. DES-Entschlüsselung mit K_{center} und
3. DES-Verschlüsselung mit K_{right} .

Die Entschlüsselung erfolgt auch hier symmetrisch zur Verschlüsselung.[3]

3.1.1.3 International-Data-Encryption-Algorithmus (IDEA)

Bei IDEA handelt es sich um einen block-orientierten konventionellen Verschlüsselungsalgorithmus. Er wurde von Xuejia Lai und James Massey vom Swiss Federal Institue of Technology entwickelt und erstmals 1990 veröffentlicht – eine verbesserte Version erschien 1991. Im Gegensatz zum DES, von dem nur der Algorithmus bekannt ist, ist bei IDEA das Entwurfs- und Designkonzept öffentlich zugänglich. Das Ziel war, möglichst einfache, gut bekannte Operationen zu verwenden. Dies sind:[1]

---

[1] „//“ bedeutet Konkatenation, also Aneinanderkettung der beiden Bitstrings unter bestimmten Regeln.
[2] Vgl. Stallings, William, Datennetz, a.a.O., S. 90ff.
[3] Vgl. ebenda, S. 93ff.

- Bitweise Addition zweier Zahlen ohne Übertrag (XOR, $\oplus$),
- Addition zweier Zahlen ohne Berücksichtigung des Übertrags über 2^{16} hinaus und
- Multiplikation zweier Zahlen und Bildung des Rests nach Division durch $2^{16}+1$.

Es wird wie bei DES ebenfalls mit 64 Bit Blöcken gearbeitet, allerdings wird ein 128 Bit Schlüssel benutzt. Jeder 64-Bit-Klartextblock wird in vier 16-Bit-Teilblöcke aufgeteilt. Sie sind das Ausgangsmaterial der ersten der insgesamt acht Iterationen. Aus dem IDEA-Schlüssel werden zunächst Teilschlüssel berechnet, indem der 128-Bit-Schlüssel in acht 16 Bit große Felder zerlegt wird. Dann wird pro Iteration der 128-Bit-Schlüssel um 25 Bit nach links rotiert und wieder in acht 16 Bit große Felder zerlegt, so daß jede Iteration sechs 16-Bit-Teilschlüssel generiert und zusätzlich die abschließende Transformation vier weitere, was eine Gesamtzahl von 52 Teilschlüsseln ergibt.

IDEA ist in den USA, sowie in den meisten europäischen Ländern patentiert und ist für eine Software- und Hardware-Implementation ausgelegt. Die Software-Implementation hat Geschwindigkeitsvorteile gegenüber DES, da nur die Hälfte der Iterationen vorkommt. [2]

3.1.1.4 SKIPJACK (Clipper)

Im April 1993 veröffentlichte die amerikanische Regierung unter Präsident Clinton ein Verschlüsselungsverfahren, das „ *...die Regierung und die Industrie in einem freiwilligen Programm zusammenbringt, um die Sicherheit und Privatsphäre in der Telekommunikation zu erhöhen, ...*“.[3] Das Gesamtverfahren wurde als Clipper[4] bezeichnet, wobei der spezielle Algorithmus unter dem Namen SKIPJACK bekannt ist. Kernelement der Initiative sind die treuhänderische Hinterlegung der Chiffrierschlüssel (sog. Escrowing) in einem „Trust Center“ der Regierung und die Verwendung eines geheimen Chiffrierverfahrens. Die Ermittlungsbehörden der USA hätten somit mit Hilfe dieses EES (= Escrowed-Encryption-Standard) Zugriff auf alle Schlüssel dieser Technologie.[5] Entwickelt wurde der

---

1 Vgl. Stallings, William, Datennetz, a.a.O., S. 353f.

2 Vgl. Becker, K. / Beutelspacher, A.: Hinter Schloß und Riegel ?, in: MC-Magazin, Jg. 1994, Heft 5, S. 88 - 95, hier S. 89; **ebenso** Universität-Gesamthochschule Siegen: IDEA, Security Server, URL=http://www.uni-siegen.de/security/krypto/idea.html: 17.11.1996

3 Stallings, William, Datennetz, a.a.O., S. 365.

4 Aufgrund eines Konfliktes mit einem bestehenden Warenzeichen darf der Ausdruck nicht mehr verwendet werden, er kommt jedoch noch häufig in der Literatur vor. Vgl. Rueppel, Rainer A.: „Clipper“ - Der Krypto-Konflikt am Beispiel der Amerikanischen ESCROW Technologie, in: DuD, Jg. 1994, Heft 8, S. 443 - 451, hier S. 443.

5 Fachliche und rechtliche Einwände zu dieser Thematik sollen hier nicht diskutiert werden.

SKIPJACK-Algorithmus von der NSA (= National Security Agency) und er ist ausschließlich als Hardware- / Chip-Implementation erhältlich. Der Chip enthält:[1]

- Die SKIPJACK-Schlüssellogik,
- den Family-Key von 80 Bit, der in allen Chips gleich ist und geheim gehalten wird – jedoch den Behörden bekannt ist,
- eine Seriennummer N, charakteristisch für jeden Chip und
- den Unit-Key U, der zur Verschlüsselung des Spruchschlüssels dient.

Die SKIPJACK-Schlüssellogik ist eine Blockchiffre, die einen 80-Bit-Schlüssel verwendet, um Daten in Blöcken zu 64 Bit zu verschlüsseln. Der Algorithmus setzt 32 Iterationen für die Berechnung einer einzigen Ver- bzw. Entschlüsselung ein, die jeweils aus einer komplexen, nichtlinearen Funktion bestehen. Der konkrete Algorithmus ist als geheim klassifiziert, womit die Sicherheit nicht bzw. schwer zu beurteilen ist. Um die Verbreitung von SKIPJACK zu unterstützen, hat die Regierung ein Gremium von fünf außenstehenden renommierten Experten eingeladen, die den Algorithmus und die Dokumentationen untersuchten und zu dem Schluß kamen, daß *„keine ernstzunehmende Gefahr besteht, Skipjack könne durch irgendeine Schwachstelle gebrochen werden.“*[2]

3.1.1.5 RC5

RC5 (RC, Ron’s Cipher) baut auf den Vorläufermodellen RC2 / RC4 auf, wurde von Ron Rivest für RSA Data Security entwickelt und im April 1995 vorgestellt, wobei das Design des Algorithmus jedoch geheimgehalten wurde (wie auch bei den Vorgängeralgorithmen). RC5 ist ein Blockverschlüsselungsalgorithmus und ist als möglicher Nachfolger von DES gedacht. Im Gegensatz zu DES bietet RC5 eine variable Schlüssel-, Wortlänge und eine variable Anzahl von Iterationsdurchläufen. Der Algorithmus ist sehr schnell, seine Sicherheit jedoch noch weitgehend unbekannt – er gilt allerdings als „State of the art“.[3]

RC5 ist sowohl für Software- wie auch Hardware-Implementierungen geeignet. Derzeit ist von der RSA Data Security eine RSA-Cryptochallenge ausgeschrieben, bei der es darum geht, zu beweisen, daß die von der US-amerikanischen Regierung als sicher genug erachteten Verschlüsselungsverfahren (u.a. DES) heute mit Ressourcen, die viele Studenten zur Verfügung haben, geknackt werden können. Außerdem will RSA gegen das Exportverbot

---

1 Vgl. Leiberich, Otto: Verschlüsselung und Kriminalität, in: BSI-Forum, 3. Jg. (1995), Heft 1, S. 60 - 61, hier S. 60.

2 Brickell, E. / Denning, D. u.a.: SKIPJACK Review: The skipjack algorithm, Interim Report, 28.07.93, URL=http:// www.cis.ohio-state.edu/hypertext/books/usenet/sj-report/sj-itrep.html: 24.11.1996

3 Vgl. Universität-Gesamthochschule Siegen: RC5, Security Server, URL=http://www.uni-siegen.de/security/krypto/rc5.html: 17.11.1996

von kryptographischer Software, welches in den USA besteht,[1] und die von vielen Regierungen der Welt aus Gründen der Staatssicherheit verbotene Datenverschlüsselung mit sicheren Verfahren, kämpfen. Am 28.1.1997 startete der Wettbewerb – eine an der Technischen Hochschule Zürich koordinierte Gruppe, der 1200 Internet-Rechner zur Verfügung standen, brach das einfachste der Verschlüsselungsprobleme am ersten Tag in vier Stunden. Dieser so schnell gefundene Schlüssel entsprach der in den USA für exportierte Software per dortigem Gesetz vorgeschriebenen maximalen Sicherheit – sie herrscht z.B. in Microsoft- und Netscape-Programmen vor. Am 4.2.1997 brach der Berkeley Diplomand Ian Goldberg in nur dreieinhalb Stunden eine von der RSA Data Security zum Test herausgegebene Geheimnachricht, die nach der sog. RC5-40 Bit Methode verschlüsselt wurde. [2] Dies soll nicht bedeuten, daß RC5 generell unsicher ist, nur die Exportversion dieses Algorithmus mit maximaler Schlüssellänge von 40 Bit.[3]

3.1.2 Asymmetrische Verschlüsselung

Im Jahre 1976 wurde erstmals von Martin E. Hellman und W. Diffie das Prinzip der asymmetrischen Kryptoverfahren vorgestellt, bei dem der Ver- und Entschlüsselungsschlüssel *nicht* übereinstimmen. Entscheidend für dieses Verfahren und seine Sicherheit ist es, daß die Kenntnis eines Verschlüsselungsschlüssels einen Angreifer nicht dazu befähigt, einen damit chiffrierten Schlüsseltext zu entziffern. Damit kann der Verschlüsselungsschlüssel auch veröffentlicht (und somit leicht weitergegeben) werden, wodurch sich auch die Bezeichnung „*Public-Key-Verfahren*“ für asymmetrische Kryptosysteme herleitet, dessen grober Ablauf vereinfacht in Abbildung 7 dargestellt ist.[4]

Damit der Verschlüsselungsschlüssel risikolos öffentlich bekannt gemacht werden kann, müssen diese Algorithmen folgende Forderungen erfüllen:

1. Der Schlüssel zur Entschlüsselung ist nicht aus dem Public-Key ableitbar.

---

[1] In den USA unterliegen sämtliche kryptische Werkzeuge der „International Traffic in Arms Regulation“ (Waffenkontrollgesetz) und somit der Exportkontrolle. Jeder Export muß angemeldet werden und erlaubnisfähig sind nur maximale Schlüssellängen von 40 Bit. Somit ist jeder amerikanische Algorithmus für den europäischen Raum weitgehend wertlos. Vgl. Kyas, Othmar, a.a.O., S. 174ff. Die max. Schlüssellänge soll aber auf 56 Bit erweitert werden, da ab 1998 Kryptosysteme dem US-Wirtschaftsministerium unterstehen. Vgl. Commerce Department: Export Administration Regulations, Interim Rules URL=http://www.eff.org/pub/Privacy/ITARexport/961230_commerce.regs: 02.02.1997.

[2] RSA-Wettbewerbsausschreibung URL= http://www.rsa.com/rsalabs/97challenge/ : 09.02.1997

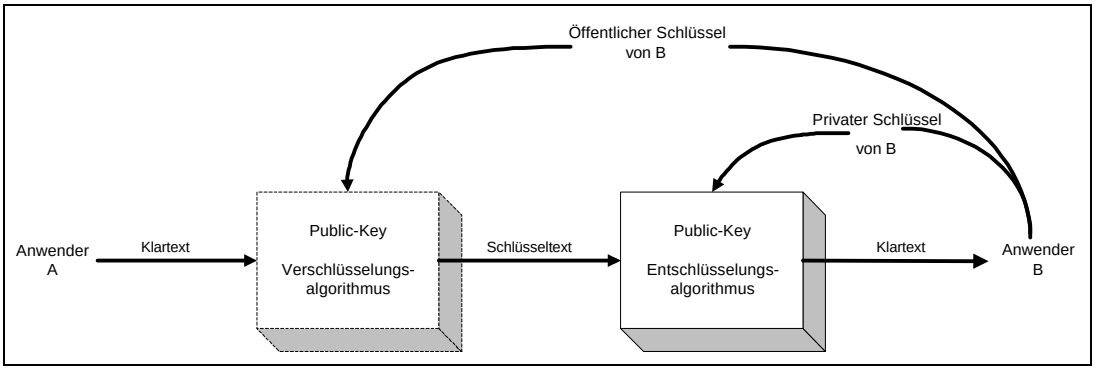
[3] Merke: Die 40 Bit-Grenze betrifft natürlich auch **jeden anderen** US-Kryptoalgorithmus (s.o.) !

[4] Vgl. Hange, M.: Die Rolle der Kryptologie im Rahmen der „IT-Sicherheit“, in: Sicherheit in Informationssystemen, Proceedings SECUNET’91, Hrsg.: Lippold, H. u. a., Braunschweig 1991, S. 15 - 21, hier S. 18.

2. Selbst bei Transformation von ausgewähltem Klartext mit dem Public-Key ist es nicht möglich, den entstandenen Schlüsseltext durch einen Angriff zu brechen.

Weiterhin geheimgehalten werden muß nur der *private Entschlüsselungsschlüssel*. Will Anwender A eine verschlüsselte Nachricht an Anwender B senden, so muß er den öffentlichen Schlüssel von B nehmen, die Nachricht damit verschlüsseln und sie B zustellen. Da B als einziger den zugehörigen privaten Entschlüsselungsschlüssel besitzt, ist er der Einzige, der diese Nachricht wieder entschlüsseln kann. Bei N Kommunikations-teilnehmern gibt es dabei nur $2 \cdot N$ Schlüsselpaare mit N Public-Keys.

Abbildung 7: Vereinfachtes Modell der Public-Key-Verschlüsselung



Quelle: Stallings, William, Datennetz, a.a.O., S. 147.

Großer Nachteil dieser Verfahren ist ihre durch enorme Rechenintensität bedingte niedrige Ver- und Entschlüsselungsgeschwindigkeit, dafür bieten sie digitale Signaturen (s.u. Abschnitt 3.1.3). Die oben genannte erste Forderung ist nicht absolut zu erfüllen. Daher wählt man Verschlüsselungsalgorithmen, die auf der Lösung von Problemen der Komplexitätstheorie beruhen. Derartige Funktionen werden auch als „*one-way trapdoor Funktionen*“ bezeichnet. Das „one-way“ bezeichnet Funktionen, deren Funktionswert „leicht“ zu berechnen ist, während die Berechnung der Inversen „schwierig“ bis „unmöglich“[1] ist. Gibt es zu einer „one-way-Funktion“ einen Schlüssel, mit dem die Inverse „leicht“ zu berechnen ist, stellt dieser Schlüssel eine Falltür (= trapdoor) dar – womit man auf den Namen „one-way trapdoor Funktion“ kommt.[1]

3.1.2.1 RSA-Verschlüsselung

Das bekannteste, bewährteste und am besten untersuchte asymmetrische Verfahren, das heute einen internationalen Quasi-Standard darstellt, wurde nach seinen Erfindern Ronald Rivest, Adi Shamir und Leonard Adleman benannt – das RSA-Verfahren.

---

[1] Die Begriffe „leicht“, „schwierig“ und „unmöglich“ beziehen sich auf die Rechenintensität und hängen somit vom Entwicklungsstand der Computergenerationen ab.

Die hohe Sicherheit des RSA-Algorithmus basiert auf der Schwierigkeit, große Zahlen in Primfaktoren zu zerlegen – also in zwei Primzahlen, die miteinander multipliziert wieder die Ausgangszahl ergeben (bei der Zahl 15 sind z.B. 3 und 5 Primfaktoren). Die derzeit effektivsten Algorithmen zur Primfaktorenzerlegung von sehr großen Zahlen sind lediglich in der Lage, Zahlen mit bis zu 120 Ziffern in Primfaktoren zu zerlegen (eine 512 Bitzahl entspricht in Dezimalschreibweise etwa 155 Ziffern).[2]

Zunächst werden zwei beliebige, sehr große Primzahlen P und Q gewählt (z.B. aus 1024 oder 2048 Bits bestehenden Zahlen). Danach wird eine Zahl E so bestimmt, daß E und $(P-1)\cdot(Q-1)$ teilerfremd[3] sind. E selbst muß dabei keine Primzahl sein, jedoch ungerade. Aus diesen drei Zahlen wird D errechnet, so daß $(D\cdot E-1)$ ganzzahlig durch $(P-1)\cdot(Q-1)$ geteilt werden kann ($(D\cdot E = 1\ mod\ (\mathrm{P}-1)\cdot(Q-1)$ in Modulo-Schreibweise). Die Verschlüsselungsfunktion ist nun wie folgt definiert:

$\boxed{C = \left(T^E\right) \bmod \mathrm{n} \qquad (\mathrm{n} = \mathrm{P}\cdot\mathrm{Q}\ ;\ \mathrm{E}, \mathrm{n}\ \text{öffentlich})}$ wobei T dem Klartext und C dem Schlüsseltext entspricht. Der Klartext wird durch eine positive Integerzahl repräsentiert, die zwischen 0 und $n-1$ liegen muß. Aus diesem Grund müssen Nachrichten, die in ihrer numerischen Darstellung größer als $n-1$ sind, in Blöcke aufgeteilt werden.

Entschlüsselt werden kann nun umgekehrt durch:

$\boxed{T = \left(C^D\right) \bmod \mathrm{n} \qquad (\mathrm{n} = \mathrm{P}\cdot\mathrm{Q}\ ;\ \mathrm{D\ geheim},\ \mathrm{n}\ \text{öffentlich})}$ wenn für C wieder T^E gesetzt wird und $T = T^{DE} \bmod \mathrm{n}$ folgt. Gemäß dem erweiterten Satz von Euklid ist eine Zahl T, die zur Potenz von 1 plus einem Vielfachen von $(P-1)\cdot(Q-1)$ erhoben und modulo „ $p\cdot q$ “ genommen wird, gleich T selbst, womit der Klartext wieder hergestellt wäre.[4]

Der Public-Key besteht aus dem Zahlenpaar (E, n), der Private-Key entspricht dem Zahlenpaar (D, n). E wird als der öffentliche Exponent, D als der geheime Exponent und n als der Modulus bezeichnet. Der geheime Exponent D kann aus dem öffentlichen Schlüssel (E, n) nur errechnet werden, wenn es gelingt, n in die Primfaktoren P und Q zu zerlegen.[5]

Der RSA-Algorithmus benötigt zum Ver- bzw. Entschlüsseln eine recht hohe Rechenleistung. Der derzeit schnellste RSA-Chip erzeugt einen Durchsatz von lediglich 600 kbit/s

---

1 Vgl. Pohlmann, Norbert: Das RSA-Verfahren und dessen Anwendung", in: DuD, Jg. 1990, Heft 1, S. 14 - 22, hier S. 14f.

2 Vgl. Kyas, Othmar, a.a.O., S. 172.

3 D. h., daß sie nicht durch dieselbe Zahl (außer 1) ohne Rest teilbar sind.

4 Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 83.

5 Vgl. Grimm, Rüdiger: Kryptoverfahren und Zertifizierungsinstanzen, in: DuD, Jg. 1996, Heft 1, S. 27 - 36, hier S. 35f.

bei der Verwendung von 512 Bit Primzahlen (zum Vergleich: DES Software-Implementationen arbeiten um Faktor 100 - 1000 schneller), auch Software-Implementation ist möglich. Der Algorithmus ist in den USA patentiert.

3.1.2.2 LUC-Public-Key-Verschlüsselung

LUC ist ein Verschlüsselungsverfahren, das von einer Forschergruppe in Neuseeland entwickelt wurde. Der Funktionsumfang entspricht RSA, dem es generell sehr ähnlich ist, aber da es außerhalb der USA entwickelt wurde, unterliegt es nicht den US-Exportbestimmungen und kann weltweit mit vollem Sicherheitsumfang eingesetzt werden.

LUC basiert auf großen Ganzzahlen in einer Lucas-Sequenz (daher auch der Name). Der Klartext wird in Blöcken verschlüsselt, wobei jeder Block einen binären Wert kleiner einer bestimmten Zahl N hat. Ver- und Entschlüsselung werden dann in folgender Form für einen bestimmten Klartextblock T und dem Schlüsseltextblock C durchgeführt, wobei der Ausdruck „$V_x(y,z)$“ für die Lucas-Sequenz steht:

Verschlüsselung: $\boxed{C = V_e(T,\ 1) \bmod \mathrm{N}}$ Entschlüsselung: $\boxed{T = V_d(C,\ 1) \bmod \mathrm{N}}$

Sender und Empfänger müssen beide den Wert von N kennen, der Sender kennt den Wert von e, und nur der Empfänger kennt den Wert von d. Es handelt sich also um eine Public-Key-Verschlüsselung mit dem Public-Key $(e,\ \mathrm{N})$ und dem Private-Key $(d,\ \mathrm{N})$.

LUC eignet sich für Software- und Hardware-Implementierung.[1]

3.1.2.3 Neuere Algorithmen

Im Bereich der Public-Key-Verschlüsselung ist es in den letzten Jahren zur Entwicklung von verschiedenen neuen Algorithmen gekommen, die in der Literatur noch kaum Erwähnung finden und daher vom näheren Aufbau relativ unbekannt sind. Sie sollen dennoch im folgenden kurz erwähnt werden, damit die Namen dieser kommenden Generationen bekannt werden.

El Gamal

Nach einem (in dieser Arbeit später näher beschriebenen) Verfahren für digitale Signaturen sind 1995 zwei verschiedene asymmetrische Algorithmen zur Verschlüsselung von T. El Gamal vorgestellt worden, die auf Entwürfen aus dem Jahr 1985 basieren und erst durch

---

[1] Vgl. Stallings, William, Datennetz, a.a.O., S. 374ff; **ebenso** Universität-Gesamthochschule Siegen: LUC, Security Server, URL=http://www.uni-siegen.de/security/krypto/luc.html: 17.11.1996

gestiegene Rechnerleistungen interessant geworden sind. Sie basieren auf dem Problem, den „diskreten Logarithmus“ modulo zu berechnen. [1]

ECC - Elliptic Curve Cryptosystem

Ein neues Public-Key Verfahren der Firma Certicom, welches auf Basis von elliptischen Kurven funktioniert und erst vor einiger Zeit ins Rampenlicht gerückt ist. Bisher war eine praktikable Anwendung aufgrund des relativ hohen Rechenaufwandes nur schwer möglich.[2]

3.1.3 Digitale Signatur

Mit den Verschlüsselungswerkzeugen der letzten Kapitel kann man in der dargestellten Weise die Sicherheitsdienste 1 und 2 erfüllen. Jetzt sollen Werkzeuge dargestellt werden, die die Aufgaben der Sicherheitsdienste 3 bis 7 leisten – grob gesagt, die Unterstützung der Authentikation, die Erkennung der Datenunversehrtheit und der Urheber- und Empfängernachweis. Durch Signierung von Programmen ist auch ein Virenschutz[3] möglich.

Diese Forderungen können zum einen mit Hilfe der oben erläuterten Verschlüsselungsverfahren erfüllt werden, indem man sie in besonderer Weise nutzt, zum anderen sind spezielle Verfahren entwickelt worden, die nur der „digitalen Signatur“ dienen. Dabei gibt es zwei Möglichkeiten der Signierung – entweder wird die Nachricht selber transformiert, d. h. signiert, oder es wird ein Authentikator gebildet, mit dessen Hilfe die Unversehrtheit und Urheberschaft der Nachricht überprüft werden kann. Anforderungen an eine digitale Signatur sind:[1]

- Nur der rechtmäßige Absender der Nachricht kann die Signatur erzeugen.
- Der Empfänger der Nachricht kann die Signatur zweifelsfrei prüfen.
- Die Signatur gilt nur im Zusammenhang mit der Nachricht.

3.1.3.1 Message Authentication Code (MAC)

Der MAC ist eine kryptographische Prüfsumme, mit der Veränderungen der Nachricht erkannt werden sollen und die einen Authentikator darstellt. Basis sind symmetrische Verschlüsselungsverfahren, denn der Code wird unter Verwendung eines geheimen Schlüssels und eines kryptographischen N-Block-Algorithmus berechnet. Die Vorgehensweise entspricht dabei einer Blockverkettung im CBC-Modus mit dem Unterschied, daß kein Initiali-

---

[1] Vgl. Grimm, Rüdiger: Kryptoverfahren und Zertifizierungsinstanzen, in: DuD, Jg. 1996, Heft 1, S. 27 - 36, hier S. 29.

[2] Vgl. Universität-Gesamthochschule Siegen: ECC, Security Server, URL=http://www.uni-siegen.de/security/krypto/ecc.html: 17.11.1996

[3] Bei einer Infektion durch einen Virus verändern sich Bytes in der Programmdatei, so daß die digitale Signatur nicht mehr stimmt.

sierungswert verwendet wird. Der gebildete MAC wird der im Klartext verbliebenen Nachricht angehängt, indem von dem „intern“ während der Berechnung entstandenen Schlüsseltext von N Bit Länge m Bit als MAC entnommen werden.[2]

Das Verfahren eignet sich nur für kleine Kommunikationsgruppen und wirft in offenen Umgebungen das Problem auf, daß die Authentikation einer mit einem MAC geschützten Nachricht nur bei Kenntnis des gemeinsamen geheimen Schlüssels möglich ist und aus diesem Grund nicht objektiv gegenüber „unbeteiligten Dritten“ erfolgen kann. Dadurch, daß nur *ein* geheimer Schlüssel von mehreren Beteiligten genutzt wird, besteht zusätzliches Risiko, da jeder identische MAC’s erstellen kann und die Nachricht nicht zweifelsfrei einem Teilnehmer zugeschrieben werden kann. [3] Trotzdem besteht sogar ein ISO-Standard für MAC’s (ISO 9797).

3.1.3.2 Public-Key-Signaturen

Die oben dargestellten asymmetrischen Verschlüsselungsverfahren haben alle eine besondere Anwendungsmöglichkeit, da sie kommutativ sind – es erfolgt zuerst die Transformation der Klartextnachricht mit dem Private-Key, und die inverse Operation wird mit dem Public-Key durchgeführt – ist der eindeutige Beweis möglich, von wem die Nachricht stammt. Die Verfahren müssen also nur „rückwärts“ angewandt werden.[4] Dies wird allerdings meist mit den im nächsten Abschnitt beschriebenen Authentikatoren von Hash-Funktionen gemacht, um Geschwindigkeits- und Sicherheitsnachteile auszugleichen. Denn bei der Notwendigkeit, längere Nachrichten in Blöcke aufzuteilen, können bei Signaturen nach diesem Verfahren Probleme auftreten, denn Briefköpfe enthalten

zum Teil oft denselben Text (bis auf das Datum), so daß ein Angreifer alte unterschriebene Texte aufzeichnen und ein anderes Datum einsetzen könnte, wenn er den ersten Block durch den entsprechenden einer älteren Nachricht austauscht.[5]

El Gamal-Authentikation

Ein von T. El Gamal entwickeltes asymmetrisches Verfahren, daß speziell für die Signierung von Nachrichten zur Verfügung steht (es kann nicht verschlüsseln), ist 1991 vom

---

1 Vgl. Hagemann, H. / Rieke, Andreas, a.a.O., S. 235.

2 Vgl. Albert, Bodo: Authentisierung, digitale Unterschrift und Chipkarte, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’92, Hrsg.: Lippold, H. / Schmitz, P., Braunschweig 1992, S. 331 - 350, hier S. 339f.

3 Vgl. Rihaczek, Karl: Datenverschlüsselung in Kommunikationssystemem, DuD-Fachbeiträge 6, Braunschweig 1984, S. 234.

4 Vgl. Seidel, Ulrich: Gesetzeskonforme elektronische Unterschrift, in: Sicherheit in Informationssystemen, Proceedings SECUNET ’91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 301 - 311, hier S. 308.

5 Vgl. Hagemann, H. / Rieke, Andreas, a.a.O., S. 235.

NIST unter dem Namen Digital Signature Scheme (DSS) veröffentlicht und 1993 unter Einbeziehung des Hash-Algorithmus SHS (s.u.) zum US-amerikanischen Standard[1] erklärt und mittlerweile auch in den Prozeß internationaler Standardisierung eingebracht worden. Die Sicherheit des Algorithmus (eine genauere Darstellung würde den Rahmen der Arbeit sprengen) basiert auf der Schwierigkeit, diskrete Logarithmen langer Zahlen (d.h. den Logarithmus einer Zahl bezüglich eines großen Modulus) in vernünftiger Zeit zu berechnen.[2] Die Signatur wird durch einen zweiteiligen Authentikator repräsentiert, der mit dem Private-Key generiert wurde und dem Empfänger mit dem Klartext zugestellt wird – und ist maximal 318 Bit lang. Dieser kann dann mit dem Public-Key (der aus drei Parametern besteht) des Sendenden die Signatur überprüfen.[3]

3.1.3.3 Hash-Funktionen

Mit ihnen werden Authentikatoren oder „Fingerabdrücke“ von Nachrichten erzeugt. Hash-Funktionen sind als eine Klasse von Funktionen der Form h = H(M) zu verstehen, die eine Nachricht variabler Länge (M) auf einen Ausgabewert (*Hash-Code* H(M)) fester Länge abbilden. Unterteilt werden sie in *einfache* und *strenge Hash-Funktionen*, wobei unter erstere simple Verfahren wie blockweises XOR über die gesamte Nachricht fallen würde, strenge Funktionen jedoch ganz bestimmte geforderte Eigenschaften erfüllen müssen:[4]

- **Eindeutigkeit** – Eine grundlegende Forderung ist die Eindeutigkeit der Abbildung Nachricht ⇒ Prüfwert, es darf nicht etwa bei Sender und Empfänger zu unterschiedlichen Ergebnissen kommen.
- **Einwegcharakter** – Es müssen „*one-way (Hash)-Funktionen*“ sein (s.o.).
- **Kollisionsfreiheit** – Die oben genannte Eindeutigkeit kann nicht absolut gewährleistet werden, da es für Nachrichten variabler Länge naturgemäß mehr Möglichkeiten gibt als für Prüfwerte einer sehr viel kleineren Länge. Es ist also nicht auszuschließen, daß die Hash-Code-Bildung zweier Nachrichten den gleichen Prüfwert ergibt. Kollisionsfreiheit bedeutet nun, daß es zumindest praktisch unmöglich sein muß, aus einem gegebenen Hash-Code eine zugehörige Nachricht zu konstruieren – die zudem noch plausibel ist.

---

1 DSS unterliegt jedoch nicht den US-amerikanischen Exportbestimmungen.

2 Vgl. Fox, Dirk: DSS: Aufwand, Implementierung und Sicherheit, in: Verläßliche Informationssysteme, Proceedings VIS `93, Hrsg.: Horster, P., Braunschweig 1993, S. 333 - 352, hier S.334.

3 Vgl. Horster, P. / Knobloch, H.-J.: Protokolle zum Austausch authentischer Schlüssel, in: Verläßliche Informationssysteme, Proceedings VIS’91, Hrsg.: Pfitzmann, A. / Raubold, E., Berlin et al., S. 321 - 328, hier S. 322.

4 Vgl. Rothe, Joachim: Anwendungsaspekte von Hash-Funktionen, in: DuD, Jg. 1993, Heft 7, S. 401 - 410, hier S. 401f.

- **Sensibilität** – Um nachträgliche Änderungen an gehashten Nachrichten zu verhindern, ohne das sich der Hash-Code ändert, muß dieser hochsensibel gegenüber Änderungen sein. Es wird daher gefordert, daß bei Änderung von nur einem Bit an beliebiger Stelle der Nachricht 50 % aller Bits des Hash-Codes geändert werden.
- **Zufälligkeit** – Die Zuordnung der einzelnen Zeichen oder Bits zu den Zeichen oder Bits des Hash-Codes muß zufällig sein.
- **Datenkompression** – Dies ist ohnehin *die Basiseigenschaft* von Hash-Funktionen. Input beliebiger Größe wird auf einen sehr viel kleineren Output-Wert (z.B. 64 oder 128 Bit) komprimiert, wobei die Größe des Output-Wertes konstant und völlig unabhängig von der Größe des Input ist.
- **Initialisierungsvektor** – Dieser ist als Option gedacht und kann z.B. eine Nachrichtenreihenfolgenummer, das Datum und die Uhrzeit, eine Zufallszahl oder ein abgesprochener Wert sein. Beide Parteien müssen natürlich mit demselben Initialisierungsvektor arbeiten.

Algorithmisch korrespondieren die Hash-Funktionen mit oben bereits beschriebenen Verschlüsselungsverfahren. In der ISO wurden sie standardisiert (ISO-Standard 10118) – in vier Teilen werden die grundlegenden Anforderungen (s.o.) in Teil 1, und drei verschiedene Hash-Typen in den weiteren Teilen, beschrieben.[1] Je Standardisierungstyp wird nachfolgend ein Algorithmus kurz dargestellt.

3.1.3.3.1 Meyer-Matyas-Hash-Algorithmus

Die Hash-Funktionen, die in Teil 2 des ISO-Standards (10118-2) definiert werden, beruhen auf der Verwendung von symmetrischen Verschlüsselungsalgorithmen, die je N Bit Klartext in N Bit Schlüsseltext überführen. Dazu werden zwei Untertypen spezifiziert:

1. Erzeugung eines Hash-Codes *einfacher Länge*, der kleiner oder gleich N lang ist.
2. Erzeugung eines Hash-Codes *doppelter Länge*, der kleiner oder gleich 2 ·N lang ist.

Es sei E = Verschlüsselungsalgorithmus, IV = Initialisierungsvektor, u = Funktion, D = Klartext und H = Hash-Code. Es wird ein Hash-Code *einfacher Länge* erzeugt:

1. Der Klartext D wird in Blöcke (D_1, D_2, ...,D_k) entsprechend der Größe des eingesetzten Chiffrierverfahrens aufgeteilt – evtl. wird der letzte Block mit Hilfe des Padding (s.o.) zum Erreichen der erforderlichen Blockgröße mit Zeichen aufgefüllt.
2. Es sei H_0 der Initialisierungsvektor IV. Die Outputblöcke werden wie folgt berechnet:

   $H_i = E_{K_i}\left(D_i\right) \oplus D_i$ wobei $K_i = u\left(H_{i-1}\right)$ und $i = 1,...,k$

Die Funktion u, die den Schlüssel K_i aus dem Vorgänger-Outputblock H_{i-1} ableitet, ist das jeweilige symmetrische Verschlüsselungsverfahren.

3. Als Hash-Code H werden so viele höchstwertige Bits wie benötigt des letzten Output-Blockes H_k genommen.

Hash-Codes *doppelter Länge* werden mit Hilfe der Konkatenation (s.o.) berechnet. Von jedem Klartextblock werden zwei einfache Hash-Codes berechnet, halbiert und die rechte Hälfte nach jedem Schritt ausgetauscht, so daß sich eine gute Kopplung dieser beiden einfachen Hash-Codes zu einem Hash-Code doppelter Länge ergibt (Schritt 3 wird mit dem letzten Outputblock $H_k//H'_k$ durchgeführt).[2]

Der Meyer-Matyas-Hash-Algorithmus entspricht dem Hash-Code einfacher Länge (eine doppelte Variante ist ebenfalls vorhanden – arbeitet jedoch nicht ISO-konform). Die Funktion u beinhaltet die Auswahl der 56 signifikanten Schlüsselbits nach den Konditionen des DES-Algorithmus. Der Hash-Code ist 64 Bit (bzw. 128 Bit) lang.

3.1.3.3.2 Secure-Hash-Standard / Algorithm (SHS / SHA)

Der SHA wurde vom NIST entwickelt und nach der Erklärung zum ISO-Standard 10118-3 in SHS umbenannt. Der SHS basiert auf dem MD4-Algorithmus (MD, Message Digest), dessen aktuelle Version MD5 im Anschluß vorgestellt werden soll und dabei auch den SHS weitgehend miterklärt.

Der SHS-Algorithmus verarbeitet als Eingabe Klartexte mit der maximalen Länge von 2^{64} Bit und erzeugt einen 160-Bit-Hash-Code. Der Klartext wird in 512-Bit-Blöcken verarbeitet. Es werden 80 Iterationen durchlaufen.

Message-Digest-Algorithmus (MD5)

Dieses jüngste Kind der MD-Familie stammt aus den USA von der „RSA Data Security“ unter Mitarbeit des „MIT Laboratory for Computer Science“. Die erste veröffentlichte Version war der MD2, dem der speziell unter dem Aspekt einer hohen Geschwindigkeit auf 32-Bit-Rechnern entworfene MD4 folgte, der mit 3 Berechnungsverfahren 48 Iterationen durchlief. Der aktuelle MD5 verarbeitet Klartext beliebiger Länge und erzeugt einen 128-Bit-Hash-Code. Der Klartext wird in 512-Bit-Blöcke zerlegt, danach erfolgt ein Padding, und zwar solange bis die Bitlänge (L) kongruent zu 448 modulo 512 ($L \equiv 448 \bmod 512$) ist. Die verbleibenden 64 Bit werden mit einer Angabe über die Länge des Textes vor dem

---

[1] Vgl. Rothe, Joachim, a.a.O., S. 403f.

[2] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 70ff.

Padding belegt. Ausgangspunkt für das Hashen ist ein 128-Bit-Initiali-sierungsvektor, auf dem bzw. im folgenden auf den Hash-Codes der Vorrunde werden im Rahmen von vier Berechnungsverfahren unter Einbeziehung des aktuellen 512-Bit-Textblockes eine Reihe logischer Operationen, Verschiebeoperationen sowie Additionen ausgeführt, deren Parameter nach festgelegten Schemata wechseln (Die Darstellung der vier Berechnungsverfahren würde den Rahmen der Arbeit sprengen – an dieser Stelle liegt auch der Unterschied zwischen MD5 und SHS). Die Textblöcke (512 Bit = 16 · 32) werden wortweise in jedem der vier Berechnungsverfahren verarbeitet, wodurch sich infolge der Verarbeitungsbreite (32 Bit wie bei MD4) intern je 16 Iterationen ergeben, was insgesamt 64 Iterationen insgesamt beträgt. Dadurch ist der MD5 auch schneller als der SHS (etwa 25%), was allerdings durch eine schlechtere Sicherheit des MD5 kompensiert wird (Schwierigkeit der Erstellung zweier Nachrichten mit gleichem Hash-Code: SHS = 2^{80}, MD5 = 2^{64}).[1] Beide gelten jedoch als sicher !

3.1.3.3.3 SqmodN-Algorithmus

Der ISO-Standard 10118-4 behandelt „Hash Functions Using Modular Arithmetic“ – also Algorithmen, die *Modulo-Operationen* wie „square mod n“ nutzen. Dies erscheint dahingehend günstig, da es insbesondere die nachfolgende Verwendung asymmetrischer Verschlüsselungsverfahren unterstützt, die ihrerseits meist auf Modulo-Operationen beruhen (s.o.). Prinzipiell werden zwei grundlegende Schemata derartiger Hash-Funktionen unterschieden. Beide basieren auf Quadrierung und anschließender Reduzierung des Eingabewertes.[2] Der Unterschied besteht darin, daß die Verknüpfung mit dem Hash-Code der vorhergehenden Iteration entweder vor dieser Operation (Typ A) oder danach (Typ B) erfolgt.

Der *SqmodN-Algorithmus* ist ein Vertreter vom Typ A und wird meist in Verbindung mit dem RSA-Algorithmus genutzt. Der zu hashende Text wird in n Blöcke D_i (i = 1,...,n) unterteilt, wobei jeder Block kleiner als der Modul q des RSA-Algorithmus ist. Die Verknüpfung geschieht durch Blockverkettung mit folgendem Algorithmus:

$$H_0 = 0 \quad ; \quad H_i = \left(H_{i-1} \oplus D_i\right)^2 \bmod q \quad ; \quad \mathrm{H_n} = \mathrm{H(D)} \quad \text{wobei} \quad i = 1,...,\mathrm{n}$$

Für die Reduzierung wird das Modul q des RSA-Algorithmus verwendet. Der besondere Vorteil liegt in der großen Blocklänge (abhängig vom Schlüsselpaar, etwa 512 Bit).

---

[1] Vgl. Stallings, William, Datennetz, a.a.O., S. 335ff; **ebenso** Universität-Gesamthochschule Siegen: Hash-Codes, Security Server, URL=http://www.uni-siegen.de/security/krypto/shs.html: 17.11.1996

[2] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 70.

Bei einem Algorithmus vom Typ B würde der Algorithmus wie folgt aussehen:[1]

$H_0 = 0 \quad ; \quad H_i = H_{i-1} \oplus \left(D_i^2 \bmod q\right) \quad ; \quad H_n = H(D) \text{ wobei } i = 1,...,n$

3.1.3.4 Zero-Knowledge-Verfahren (ZKV)

Die ZKV sind keine Verschlüsselungsverfahren, eignen sich jedoch zur Anfertigung von digitalen Signaturen und zur Authentikation von Identitäten. Entwickelt wurden sie jedoch auf Basis einer anderen Problemstellung – *„Kann A (Beweiser) einen B (Verifizierer) davon überzeugen, daß er ein Geheimnis G hat, ohne auch nur den geringsten Teil davon preiszugeben ?* “[2] Eine erste Lösung wurde 1986 von A. Fiat und A. Shamir vorgestellt und als *Fiat-Shamir-Verfahren* bekannt.

„Zero-Knowledge“ bedeutet, daß der Verifizierer B auch mit einem Dritten X, der das Geheimnis nicht kennt, ein Protokoll produzieren kann, das von einem Außenstehenden nicht vom „echten“ Protokoll zwischen A und B unterschieden werden kann. Ein Angreifer kann also beliebig viele Kommunikationsschritte aufzeichnen, ohne dadurch das geringste über G zu erfahren. Die Lösung sieht so aus, daß A und B eine Anzahl von „Proben“ verabreden. Je mehr Prüfungen der Beweiser A besteht, desto größer die Wahrscheinlichkeit, daß er das Geheimnis kennt (sequentielle Version), bzw. je kompliziertere Prüfungen der Beweiser besteht, desto größer ebenfalls die Wahrscheinlichkeit, daß er G kennt (Parallel-Version).[3]

Zuerst weist eine „Zentrale“ allen Teilnehmern (A, B,...) Unterlagen (je einen ID-String, verschiedene Zufallszahlen e und dazu berechnete Schlüssel s) zu, die in mathematischer Abhängigkeit stehen (die Algorithmen dazu werden hier nicht dargestellt). Es handelt sich bei ZKV um Protokollverfahren, weil die Authentikation in mehreren Kommunikationselementen erfolgt, die zwischen Beweiser und Verifizierer ausgetauscht werden – man unterscheidet daher eine *Preprocessing-Phase* (A berechnet eine „Behauptung“ x aus seiner ID und den ihm zugewiesenen Zahlen und schickt sie B), eine *Challenge-and-Response-Phase* (B generiert aus seinen Unterlagen eine „Prüfung“ und schickt sie an A. Dieser erstellt dazu mit seinen Unterlagen eine „Lösung“ y, die er an B schickt) und eine *Verifizierungs-Phase* (B überprüft den Zusammenhang zwischen x und y).[1] Bei der Durchführung kann ein Betrüger mit einer gewissen Wahrscheinlichkeit p ($0 < p < 1$) den Verifizierer täuschen, so daß das Protokoll x-mal mit jeweils einer anderen Zufallsbasis wiederholt wird, bis das errechnete Sicherheitsniveau $q = 1 - p^x$ eine vom Verifizierer ak-

---

1 Vgl. Rothe, Joachim, a.a.O., S. 404.

2 Kiranas, Argiris: Technische Sicherheitsmechanismen in POS-Systemen, in: DuD, Jg. 1996, Heft 7 u. 8, S. 413 - 420 u. 472 - 478, hier S. 477.

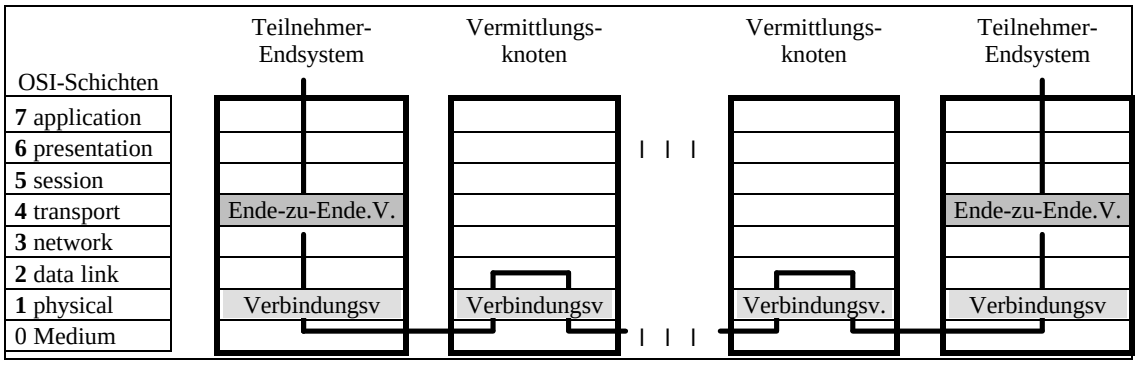
3 Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 90f.

zeptable Grenze überschritten hat. Die Sicherheit des Geheimnisses basiert auf der Schwierigkeit, „one-way Funktionen“ zu invertieren. Bezeichnet man mit p_1 ($0 < p_1 < 1$) die Wahrscheinlichkeit ein solches Geheimnis „zu erraten“, so bildet $q_1 = 1 - p_1$ eine obere Schranke für q (das Sicherheitsniveau ist variierbar und kann maximal den Wert q_1 erreichen).
Bei der Erzeugung einer *digitalen Signatur* mit ZKV muß man den Verifizierer durch den zu signierenden Klartext ersetzen. Man braucht dazu eine kryptographisch starke Funktion, die beliebige Zeichenfolgen in pseudozufällige Matrizen überführt (eine genauere Darstellung unterbleibt im Rahmen dieser Arbeit). Die ZKV’s arbeiten als Sig-nierinstrument sehr schnell. Je nach verwendetem Algorithmus unterscheidet man die Verfahren von Fiat / Shamir, Guillou / Quisquatter, Beth und eine Version von Shamir.[1]

3.1.4 Position der Verschlüsselung

Grundsätzlich gibt es zwei Strategien, die verschlüsselten Informationen von einer Station zu einer bestimmten Empfangsstation zu senden. Sie unterscheiden sich hauptsächlich darin, in welcher Schicht des ISO-OSI Referenzmodells die Verschlüsselung stattfindet, was in Abbildung 8 verdeutlicht wird. Es kann die Technik der Verbindungsverschlüsselung bzw. der Ende-zu-Ende-Verschlüsselung oder eine Kombination gewählt werden. Nachfolgend sollen die Techniken kurz vorgestellt werden.

Abbildung 8: Einordnung der Verschlüsselungspositionen in ISO-OSI



Quelle: Hammerer, C.: Vermittlung der Problematik des sicheren Schlüssel-Verteilens als Lehrprogramm, in: DuD, Jg. 1993, Heft 1, S. 33 - 39, hier S. 35.

3.1.4.1 Verbindungsverschlüsselung

Die Protokolle der Schichten 1 - 3 sind Systemprotokolle, d.h. sie werden zwischen benachbarten Systemen abgewickelt. Werden Daten auf diesen drei Schichten des Endsystems verschlüsselt, so erfolgt die Entschlüsselung im benachbarten System, also im Vermittlungsknoten, so daß die Daten dort im Klartext vorliegen. Für die nächste Teilstrecke wer-

---

[1] Vgl. Beutelspacher, A. / Kersten, A.: Chipkarten als Sicherheitswerkzeug, Berlin et al. 1991, S. 45f.

den die Daten wieder verschlüsselt, dort entschlüsselt usw. – bis sie beim Endsystem des Empfängers ankommen. Für *jede* dieser „Teilverbindungen“ existiert *ein* Schlüssel, jedoch ist der Aufwand der Schlüsselverteilung durch die direkten Wege relativ gering. Und es gibt noch einen weiteren Vorteil, denn man kann *Verkehrsflußanalysen* unterbinden. Eine wirksame Gegenmaßnahme bei diesem Angriff ist das *Dehnen* des Datenflusses mit *Fülldaten*, d.h., die einzelnen Knoten produzieren eine kontinuierliche Ausgabe von Schlüsseltext, selbst wenn kein zu chiffrierender Klartext vorliegt. Dazu wird vor den Verschlüsselungsalgorithmus ein Zufallsdatengenerator geschaltet, der für einen kontinuierlichen Datenstrom sorgt – ein Angreifer kann dann nicht zwischen „echtem“ und „gedehntem“ Datenstrom unterscheiden.[1] Die Verschlüsselung vollzieht sich auf der Bitübertragungs- oder Verbindungssicherungsschicht. Bei sensiblen Daten ist es in offenen Informationsnetzen bei Nutzung „öffentlicher“ Vermittlungsknoten natürlich nicht von Interesse, daß die Daten „unterwegs“ in den Knoten klar lesbar sind.

3.1.4.2 Ende-zu-Ende-Verschlüsselung

Bei sensiblen Daten wird eine Ende-zu-Ende-Verschlüsselung auf den Schichten 4 - 7 vorgezogen. Bei dieser Technik wird beim Sender verschlüsselt und erst bei Empfänger wieder entschlüsselt, so daß die Schlüsseltexte transparent übertragen und von den Knoten vermittelt werden. Es können jedoch nicht alle Daten, die gesendet werden, in dieser
Form verschlüsselt werden, da z.B. die *Verbindungsdaten* (Vorspann) zum Aufbau der Verbindung und zur Vermittlung der Daten in den Knoten in Klartext vorliegen müssen. Gerade bei paketvermittelnden Netzwerken muß darauf geachtet werden, daß der Vorspann der einzelnen Pakete unverschlüsselt bleibt. Um effektive Sicherheit zu erlangen, müssen die Anwenderdaten einer Ende-zu-Ende-Verschlüsselung unterworfen werden, die Verbindungsdaten jedoch verbindungsverschlüsselt werden. Nun sind die Daten weitgehend gesichert – nur in den Knoten sind noch die Verbindungsdaten klar zu lesen.
Die Verschlüsselung sollte auf der Transportschicht oder höher vollzogen werden. Bei bestimmten Konstellationen sollte im Internetzwerk auf der Anwendungsschicht verschlüsselt werden, da an Gateways oft die OSI-Struktur verlassen wird und z.B. mit einem auf TCP/IP (=Transmission Control Protocol / Internet Protocol – s. Abb. 11, S. 48) basierenden Netzwerk verbunden wird (häufig bei E-Mail oder EDI (= Electronic Data Interchange)). Bei TCP/IP gibt es kein Ende-zu-Ende-Protokoll unterhalb der Anwendungsschicht. Nachteil hierbei ist, daß (besonders extrem auf der Anwendungschicht) die Anzahl der zu

---

[1] Vgl. Kiranas, Argiris, a.a.O., S. 477f.

berücksichtigenden Systeme dramatisch ansteigt und somit der Schlüsselverteilaufwand eklatant groß ist.[2] Je höher die genutzte Schicht, desto schlechter läßt sich eine Verkehrsflußanalyse verhindern. Auch hier ist wieder eine Verbindung beider Techniken anzuraten. Generell muß noch beachtet werden, ob eine verbindungslose oder eine -orientierte Kommunikationsbeziehung bedient werden soll (s. Tabelle 1).

3.1.5 Schlüsselmanagement und Zertifizierung

Die Stärke eines jeden schlüsselorientierten kryptographischen Systems steht und fällt mit der *Schlüsselvergabetechnik*. Dieser Begriff bezieht sich darauf, einen Schlüssel über unsichere Kommunikationswege an zwei Parteien weiterzugeben, die Informationen austauschen möchten, ohne daß dabei andere den Schlüssel (Private-Key) sehen und manipulieren können. Bei den Public-Keys darf jeder den Schlüssel sehen, aber es kann auch jeder einen solchen Schlüssel fälschen und in Umlauf bringen. Hier ist also zusätzlich noch auf die *Schlüsselverwaltungstechnik* zu achten. Schlüsselvergabe und -verwaltung sollen nun im folgenden untersucht werden.

Erstens kann ein Schlüssel von A gewählt und B physisch übergeben werden. Zweitens kann ein Dritter den Schlüssel wählen und ihn physisch an A und B übergeben. Drittens können A und B beim Schlüsselaustausch auf einen evtl. vorhandenen alten Schlüssel zurückgreifen oder viertens können A und B auf eine für beide bestehende verschlüsselte Verbindung zu einem Dritten zurückgreifen, und über diesen Dritten einen Schlüssel vergeben bzw. tauschen.[3]

Die ersten beiden Varianten sind z.B. für eine Verbindungsverschlüsselung denkbar, da dabei nur mit dem direkten Partner Schlüssel getauscht werden. Für Ende-zu-Ende-Verschlüsselung ist diese „manuelle“ Anlieferung jedoch zu umständlich, zumal bei symmetrischen Verfahren ja die Anzahl der benötigten Schlüssel quadratisch zu der Teilnehmerzahl zunimmt. Die dritte Variante wäre bei beiden Verschlüsselungspositionen praktikabel, jedoch besteht das Risiko, daß der alte Schlüssel bereits kompromittiert wurde. Genauer soll nun die vierte Variante dargestellt werden.

3.1.5.1 Schlüsselhierarchien und -vergabezentren

Wir gehen davon aus, daß symmetrische Verfahren genutzt werden und mit einer „Stelle“ ein Private-Key auf sicherem Weg abgesprochen wurde. Da dieser „sichere“ Austausch

---

1 Vgl. Stallings, William, Security, a.a.O., S. 80f.
2 Vgl. Stallings, William, Security, a.a.O., S. 82ff.
3 Vgl. Stallings, William, Datennetz, a.a.O., S. 118.

schwer zu bewerkstelligen ist, muß *dieser* Schlüssel nun besonders gesichert werden. Trotzdem sollen zur Sicherheit regelmäßig die Schlüssel gewechselt werden. Daher wird der „sichere“ Public-Key nur als Master-Key verwendet, der die Aufgabe hat, die Verabredung von untergeordneten Schlüsseln zu ermöglichen – da dieser Schlüssel andere Schlüssel verschlüsselt, heißt er Key Encrypting Key (KEK). Mit diesem KEK wird nun ein Data Encrypting Key (DEK) verschlüsselt, mit dem der Datenverkehr gesichert wird (Verschlüsselung und MAC-Berechnung). Dabei sollte der DEK um weitere Parameter wie z.B. Zeitstempel oder Zähler erweitert werden, um Wiederholungen oder Verzögerungen durch Angreifer erkennen zu können. Er kann jedoch auch zum verschlüsselten Transport von weiteren Schlüsseln verwendet werden, die letztendlich als Session-Key nur für die Dauer einer logischen Verbindung genutzt und dann gelöscht werden.[1] Damit ergibt sich eine *Schlüsselhierarchie* – wobei der Master-Key der Hierarchiestufe 0 entspricht – bei der mit den Schlüsseln der Stufe n jeweils Schlüssel der Stufe n+1 verschlüsselt werden.

Um nun zu vermeiden, daß alle n Kommunikationsteilnehmer n-1 sicher speichern müssen und ja ohnehin im Vorwege ein „sicherer“ Schlüssel bestehen muß, wird ein Schlüsselvergabezentrum (SVZ) eingerichtet, das als integere Instanz mit jedem einen Master-Key abspricht und durch die Schlüsselhierarchie danach alle weiteren Schlüssel herleiten kann. Wenn A Kontakt zu B aufnehmen will, wendet er sich an das SVZ, das aus den Master-Key von A und B und dem Einbau z.B. eines Zeitstempels die nötigen Session-Keys generiert und zustellt. In großen Informationsnetzen sollten auch die SVZ hierarchisch aufgebaut sein – z.B. auf Domainebene.

Als weitere Möglichkeit gibt es ein von IBM in seiner „Common Cryptographic Architecture“ vorgestelltes Konzept des Schlüsselmanagements mit Kontrollvektoren für symmetrische Verfahren. Es arbeitet mit einer Schlüsselhierarchie und dezentraler Vergabe, da die Schlüssel und die Kontrollvektoren von bestimmten Hardwarekomponenten in jedem Teilnehmersystem generiert werden, was die Einsatzmöglichkeit in globalen Informationsnetzen jedoch stark relativiert.[2]

3.1.5.2 Diffie-Hellman-Schlüsselaustausch

Noch einmal soll ein *asymmetrisches Verfahren* dargestellt werden, dessen Algorithmus allerdings auf den Schlüsselaustausch beschränkt ist. Dieser Algorithmus basiert erneut auf

---

[1] Vgl. Oppliger, Rolf, a.a.O., S. 49f.

[2] Vgl. Staudinger, Bernd: Sicherer Datentransfer in heterogenen Netzen, in: KES, 10. Jg. (1994), Heft 2, S. 12 - 16, hier S. 14.

der Berechnung diskreter Logarithmen und verläuft grob wie folgt:[1] Beide Parteien verwenden einen öffentlichen Modulus n (n ist eine große Primzahl) und eine Ganzzahl g (g ist ein sog. primitives Element). Mit Hilfe von n generieren beide Parteien ihre *eigenen Private-Keys* und berechnen damit jeweils einen Parameter, den sie austauschen. Damit berechnen beide einen *gemeinsamen Private-Key* zum Verschlüsseln und mit Hilfe des Euklid'schen Algorithmus erhalten sie den Entschlüsselungsschlüssel, so daß die eigentliche Datenkommunikation aufgenommen werden kann.

Der Vorteil ist, daß beide Partner vor der Schlüsselvereinbarung über keinen gemeinsamen Private-Key verfügen müssen – wie bei asymmetrischen Verfahren üblich – , und daß beide Partner den gemeinsamen Schlüssel für z.B. eine Session *gleichberechtigt* beeinflussen, so daß Angriffe durch Wiederholung bzw. Wiedereinspielung unmöglich sind. Nachteil ist, daß in der Schlüsselvereinbarung keine Authentikation erfolgt, die Partner also nicht wissen, mit wem sie den gemeinsamen Schlüssel vereinbart haben – diesen Nachteil haben aber alle Verfahren mit einem Public-Key.[2] Abhilfe schafft hier der Einsatz von Zertifizierungsinstanzen.

3.1.5.3 Zertifikate und Zertifizierungsinstanzen

Um Public-Key-Verfahren effizient einsetzen zu können, muß gewährleistet sein, daß der Ersteller des Public-Key auch wirklich die Person ist, die er zu sein vorgibt – es muß seine Echtheit überprüfbar sein. Diese *Authentikation* läßt sich nur durch *Zertifikate* real und verläßlich realisieren. Dabei wird der Public-Key der Kommunikationsteilnehmer von einer vertrauenswürdigen dritten Instanz – der *Zertifikationsinstanz* – mit der Bestätigung der Authentizität zur Verfügung gestellt, so daß der einzelne Benutzer durch Vergleich zugehende Public-Keys überprüfen kann. Die Zertifikationsinstanz stellt eine Art Kreuzung zwischen Einwohnermeldeamt und Telefonbuch dar und ist in den meisten Fällen unabhängig (angeboten werden solche Dienste von kommerziellen Firmen, aber auch durch wissenschaftliche Vereinigungen wie z.B. das CERT (=Computer Emergency Response Team). Die Anmeldung dort geschieht persönlich oder auf andere sichere Art. In den Zertifikaten stehen in einer bestimmten Struktur die Zertifikats-ID, der eindeutige Name (mit diversen Attributen) des Zertifikatsinhabers, der eindeutige Name der Zertifizierungsinstanz, ein evtl. Gültigkeitsdatum, der Public-Key des Inhabers, die Authentikations-Algorithmen von Inha-

---

[1] Vgl. Stallings, William, Datennetz, a.a.O., S. 421.

[2] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 167f.

ber und Instanz, die Hash-Funktion der Instanz und eine über alle bisherigen Punkte berechnete digitale Signatur der Zertifizierungsinstanz (standardisiert in ISO 9798-1).[1]
Die Zertifizierungsinstanzen sind oft mit den Schlüsselvergabezentren identisch und generieren oft auch den geheimen Schlüssel bei Public-Key-Verfahren. Die Zertifikate werden auf verschiedenen Medien zur Verfügung gestellt – gängig ist die Bereitstellung und Verwaltung der Zertifikate auf sog. *Authentikations-Servern*. Unabhängige Stellen, die diese Funktionen anbieten, werden häufig auch „*Trust-Center*“ oder „*Trusted Third Party*“ genannt. Sie bieten auch sog. *Notariatsfunktionen* (elektronischer Notar) an, bei denen sie zertifizierten Teilnehmern auf Wunsch Kommunikationsdokumente mit Zeitstempeln signieren, um zu bestätigen, daß dieses Dokument zum angegebenen Zeitpunkt in bestimmter inhaltlicher Form dem elektronischen Notar vorgelegen hat.[2]

Die Zertifizierungsinstanzen sind in globalen offenen Netzen hierarchisch und dezentral aufgebaut. Wie kann nun Teilnehmer A, der bei der Instanz x zertifiziert ist, das Zertifikat von B überprüfen, das von Instanz y ausgestellt wurde, ohne den Public-Key von y zu besitzen ? Genau das ist die Aufgabe der Authentikations-Server – sie stellen Zertifikate öffentlich zur Verfügung, damit eine authentische Kommunikation auch zwischen Teilnehmern möglich ist, die ihre Zertifikate gegenseitig nicht verifizieren können. Dazu werden *Zertifikatspfade* geknüpft, die angeben, wie die Zertifizierungsinstanzen organisatorisch zusammenhängen. Die Zertifikats-ID stellt einen Token dar, mit dem diese Pfade nachvollzogen werden können. Die Zertifikatspfade sind logische Zertifizierungsketten, die zu einem weltweiten Netz geknüpft sein können, um die Authentikation durchzuführen.[3]

3.1.6 Authentikation der Kommunikationspartner

Der Authentikationsprozeß bezüglich der Kommunikationspartner soll hier nun noch einmal genauer dargestellt werden. Klassische Mittel wie Paßwortmethoden, Rückrufmethoden und geschlossene Benutzergruppen sollen dabei außer betracht gelassen werden, da sie den Anforderungen an ein offenes Informationsnetz nicht gewachsen sind.

---

1 Vgl. Plattner, B. / Lanz, C. et al.: Elektronische Post und Datenkommunikation, 1. Aufl., Bonn, München et al. 1989, S. 192ff.

2 Vgl. Reimer, H.: Vertrauenswürdige Kommunikation in offenen IT-Systemen, in: KES, 11. Jg. (1995), Heft 5, S. 24 - 29, hier S. 26ff; **ebenso** Blab, H. A.: Chipkarten und Kryptosysteme in digitalen Kommunikationsanlagen, in: Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 11-13.11.1992, Hrsg.: ITG, Berlin 1993, S. 291 - 301, hier S. 300.

3 Vgl. Jacobson, G.: Grenzenlose Sicherheit, in: Datacom, 13. Jg. (1996), Heft 1, S. 48 - 56, hier S. 52; **ebenso** Eisele, R.: Sicherheit und Elektronische Unterschriften - SmartDisk, in: DuD, Jg. 1995, Heft 7, S. 401 - 406, hier S. 404.

Die nachfolgenden Methoden arbeiten auf Basis asymmetrischer Algorithmen, die durch das Bestehen des Public-Keys für eine Authentikation besser geeignet sind als symmetrische Verfahren[1]. Es werden dabei Time Variant Parameters (TVP) in Form von Zeitstempeln, Reihenfolgenummern oder vorgegebenen Zufallszahlen genutzt, um jede gültige Authentikation einmalig zu machen, und vor Wiederholung durch Angreifer zu schützen. Desweiteren werden für Challenge/Response-Abläufe vorgegebene Textproben (z.B. Pseudozufallszahlen) eingesetzt. Die Protokolle gehen von folgenden Voraussetzungen aus:[2]

1. Jeder Teilnehmer (Anwender oder ein Prozeß) ist in der Lage, Zertifikate (oder auch nur Public-Keys) des Kommunikationspartners zu verifizieren.
2. Jeder Teilnehmer verfügt über einen Private-Key, den nur er kennt.
3. Jeder Teilnehmer ist in der Lage, TVP's zu generieren.

3.1.6.1 Einseitige Authentikation

Bei dieser Gruppe wird nur *ein* Kommunikationsteilnehmer authentisiert. Die Darstellung der Verfahren erfolgt wieder als Ergebnis von Konkatenationen der Teilnehmerstrings. Dabei steht $s_x(Y)$ für die digitale Signatur des Teilnehmers x unter der Nachricht Y, R_x für von x erzeugte Pseudozufallszahlen und die „Text"-Angaben für applikationsabhängige Texte, die mitgesendet bzw. mitunterschrieben werden und optional sind. Zudem kommen noch TVP und Zertifikate der jeweiligen Teilnehmer (TVP_x, $ZERT_x$):[3]

One Pass

Um die Authentizität eines Teilnehmers festzustellen, ist mindestens die Signatur unter einen TVP erforderlich, die in einem einzigen Schritt (One Pass) erfolgen kann. Der Urheber A sendet $ZERT_A$ (optional) und folgendes Token AB an B:

$$\text{Token AB} = TVP_A \,//\, B \,//\, \text{Text2} \,//\, s_A(TVP_A \,//\, B \,//\, \text{Text1})$$

Im unterschriebenen Teil ist die Identität des B enthalten, damit er überprüfen kann, daß die Authentikation für ihn erfolgt ist. So wird verhindert, daß ein Dritter, der das Token abgehört hat, dieses bei einem Teilnehmer E vorlegen und sich dort für A ausgeben kann. Nach dem Empfang überprüft B die Gültigkeit des empfangenen oder bereits bei ihm vorhandenen Zertifikates $ZERT_A$, die digitale Signatur unter dem Token und die Plausibilität des TVP's.

---

[1] Es gibt auch Ansätze auf symmetrischer Basis – diese werden hier jedoch vernachlässigt.
[2] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 125.
[3] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 125f.

Two Pass

Um einen Challenge/Response-Mechanismus[1] durchzuführen, sind zwei Schritte (Two Pass) notwendig. Als „Challenge“ dient eine Aufforderung des B, bei der er eine Zufallszahl R_B vorgibt, die die Zeitrichtigkeit (und natürlich Einmaligkeit) gewährleistet. Als „Response“ sendet A optional $ZERT_A$ und das Token AB:

$$\text{Token AB} = R_A \,//\, B \,//\, R_B \,//\, \text{Text2} \,//\, s_A(R_A \,//\, B \,//\, R_B \,//\, \text{Text1})$$

Die Zufallszahl R_A wird verwendet, damit A nicht Texte oder Hash-Codes unterschreibt, die B präpariert hat. Nach dem Empfang überprüft B die Gültigkeit des $ZERT_A$, die digitale Signatur unter dem Token und die Übereinstimmung seiner R_B mit der im Token enthaltenen R_B.

3.1.6.2 Gegenseitige Authentikation

Die einseitigen Authentikationsmechanismen werden nun gegenseitig angewendet, so daß jeder Teilnehmer den anderen authentisiert:[2]

Two Pass

Hierbei läuft eine gegenseitige One Pass-Authentikation ab.

$$\text{Token AB} = TVP_A \,//\, B \,//\, \text{Text2} \,//\, s_A(TVP_A \,//\, B \,//\, \text{Text1})$$

$$\text{Token BA} = TVP_B \,//\, A \,//\, \text{Text4} \,//\, s_B(TVP_B \,//\, A \,//\, \text{Text3})$$

Die beiden Authentikationen müssen nicht sequentiell erfolgen, sondern können auch parallel ablaufen. Es erfolgt optional gegenseitiger Zertifikatsaustausch.

Three Pass

Hierbei fordert A mit einer Zufallszahl R_A B zur Identifizierung auf. Dann werden *sequentiell* zwei Unterschrifts- und vier Verifikationsschritte ausgeführt.

$$\text{Token BA} = R_B \,//\, A \,//\, R_A \,//\, \text{Text2} \,//\, s_B(R_B \,//\, A \,//\, R_A \,//\, \text{Text1})$$

$$\text{Token AB} = R_A \,//\, B \,//\, R_B \,//\, \text{Text4} \,//\, s_A(R_A \,//\, B \,//\, R_B \,//\, \text{Text3})$$

Neben den Token werden auch optional gegenseitig die Zertifikate ausgetauscht.

Two Pass Parallel

Hierbei kommt es zu einer gegenseitigen „Challenge“, bei der A R_A an B und B R_B an A schickt. Danach werden als gegenseitige „Response“ *parallel* zwei Unterschrifts- und vier Verifikationsschritte ausgeführt.

---

[1] Bei einem solchen Mechanismus kommt es zu einem interaktiven Austausch von Fragen und Antworten.

[2] Vgl. Ruland, Christoph: Info.sicherheit, a.a.O., S. 127ff.

$$\text{Token AB} = R_A \,//\, B \,//\, R_B \,//\, \text{Text2} \,//\, s_A(R_A \,//\, B \,//\, R_B \,//\, \text{Text1})$$

$$\text{Token BA} = R_B \,//\, A \,//\, R_A \,//\, \text{Text4} \,//\, s_B(R_B \,//\, A \,//\, R_A \,//\, \text{Text3})$$

Auf diesem Weg wird die Zeit für die gegenseitige Authentikation um ca. 50 % verringert. Bei der „gegenseitigen Challenge“ werden optional die Zertifikate ausgetauscht.

Schlüssel-Management

Die vorangegangenen gegenseitigen Authentikationsprotokolle können erweitert werden, um für nachfolgende Datentransfers Schlüssel abzusprechen. Dafür werden die Token mit einem Private-Key ($e_x(Z)$ = Verschlüsselung der Daten Z mit dem Private-Key des Teilnehmers x) verschlüsselt. Nachdem sich beide Teilnehmer gegenseitig authentisiert haben (s.o.), schickt A folgendes Token zur Absprache des Schlüssels:

$$\text{Token AB} = e_B(TVP_A \,//\, B \,//\, TVP_B \,//\, \text{Text2} \,//\, s_A(TVP_A \,//\, B \,//\, TVP_B \,//\, \text{Text1})$$

Der abzusprechende Schlüssel steht im Textfeld Text1.

3.1.7 Hybrid-Verfahren

Die oben angeführten Verfahren der Verschlüsselung, digitaler Signaturen und des Schlüsselmanagements lassen sich zu Hybrid-Verfahren vereinen, um z.B. Geschwindigkeit, Sicherheit und Funktionalität zu steigern. Verschlüsselungsverfahren und Hash-Funktionen existieren ohnehin in einer Art „Symbiose“, aber auch die Verschlüsselungsverfahren werden untereinander verquickt. So zieht man häufig die Vorteile der symmetrischen mit den Vorteilen der asymmetrischen Verfahren zusammen, ohne jedoch ihre Nachteile zu übernehmen.

Die meistgenutzten Kombinationen sind:

- RSA- und DES-Algorithmus
- RSA- und IDEA-Algorithmus
- Diffie Hellman-Verfahren und DES

Die Hybrid-Verfahren haben einen unterschiedlichen Funktionsumfang, im einzelnen sind dies:

- Reine Verschlüsselung
- Reine Vergabe von digitalen Signaturen
- Schlüsselmanagement

⇒ jegliche Kombination der obigen drei Funktionen

Es gibt im Bereich der Hybrid-Verfahren bereits Normungen im internationalen Bankgewerbe und auch die Tendenz gebräuchlicher Kryptoprogramme geht eindeutig dahin.[1]
Die symmetrischen Verfahren (DES, IDEA) werden zur Verschlüsselung der Nachricht verwendet, da ihre Verarbeitungsgeschwindigkeit hier besonders gut ist. Der RSA-Algorithmus (oder der DSS bzw. Hash-Funktionen) dient zur digitalen Signatur der Nachricht. Soll die Nachricht insgesamt verschlüsselt werden, wird der RSA auch noch zur Verschlüsselung des benutzten DES-Schlüssels (meist als Session-Key) verwendet, damit dieser in geschützter Form der Nachricht beigefügt werden kann. Es wird auch oft das Diffie-Hellman-Verfahren eingebaut, um den verabredeten Schlüssel dann für ein symmetrisches Verfahren zu nutzen.
Als erstes wird meist die digitale Signatur erzeugt, danach die Nachricht mit einem zufällig erzeugten symmetrischen Schlüssel chiffriert, worauf der symmetrische Zufallsschlüssel mit Hilfe des Public-Keys (z.B. des RSA) des Empfängers verschlüsselt wird. Abschließend wird der signierte Schlüsseltext mit dem verschlüsselten, symmetrischen Zufallsschlüssel zusammengefügt und verschickt – der Empfänger muß nur den Public-Key kennen. Die Entschlüsselung verläuft dann in umgekehrter Reihenfolge mit den inversen Funktionen.[2]

3.2 Hardware-Mechanismen

Die nachfolgend beschriebenen „Hardware-Mechanismen“ stellen teilweise eine Alternative zu den vorher beschriebenen kryptologischen Möglichkeiten dar, andere machen die Kryptographie praktikabler und bauen funktional auf ihr auf. Auf die Beschreibung der reinen Implementation von kryptologischen Algorithmen in Chips soll verzichtet werden.

3.2.1 Chipkarten

Chipkarten können durch die Art des Chips, der in die Plastikkarte mit der Länge von 85,6 mm, der Breite von 53,9 mm und der Dicke von 0,76 mm eingebettet wurde, unterschieden werden – sie dürfen dabei nicht mit den Magnetstreifenkarten wie z.B. der normalen Eurochequekarte verwechselt werden. Es gibt *Speicherchipkarten* ohne Sicherheitslogik (z.B. Krankenversichertenkarte), *intelligente Speicherchipkarten* mit festverdrahteter Sicherheitslogik (z.B. Telefonkarte) – und *Prozessorchipkarten* (*Smart Cards*), die Thema dieses Abschnittes sein sollen. Die Chipfläche ist auf 25 mm^2 begrenzt, da der Chip sonst bei ei-

---

[1] Vgl. Widmer, Walter: Banken: Durchsetzung von Sicherheitsstandards, in: DuD, Jg. 1992, Heft 5, S. 237 - 240, hier S. 239.

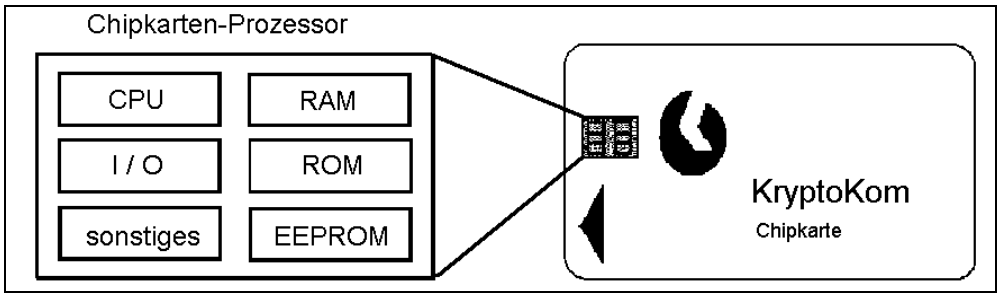
[2] Vgl. Abel, H.G. / Ermer, D. J.: Sicherheitsmaßnahmen bei Vernetzung, in: Sichere EDV, Band 2, Hrsg.: Wißner, B, Augsburg 1996, Abschnitt 5/5, hier 5/5.6.3.3.

nem Durchbiegen der Karte beschädigt werden könnte. Die Smart Cards sind von der ISO als Standard (ISO-7816) genormt und heißen dort „Integrated Circuit Card“ (ICC). Die Kommunikation geschieht über 8 offenliegende Kontakte, von denen bis jetzt aber erst sechs für Aufgaben definiert wurden (Ver-sorgungsspannung (5 Volt), Masse, Programmierspannung, Rücksetzen, Takt und serielle Ein- / Ausgabeschnittstelle).[1] Es gibt die ICC’s auch kontaktlos, dann wird mittels flacher Spulen induktiv gekoppelt. Die Kopplung erfolgt über ein Chipkartenlesegerät, daß bei Eingabemöglichkeit auch PIN-Pad (= Personal Identify Number) genannt wird.

Der enthaltene Chipkarten-Prozessor (s. Abb. 9) enthält einen vollständigen Mikrocomputer mit folgenden Einzelkomponenten:

- CPU (= Central Processing Unit), 8 Bit, 5 - 10 MHz,
- Maskenspeicher ROM (= Read Only Memory), 8 - 16 Kbyte,
- Datenspeicher EEPROM (= Electrically Erasable Programmable ROM), 2 - 8 Kbyte,
- Arbeitsspeicher (RAM, Random Access Memory), 128 - 512 Byte und
- einer Input- / Outputschnittstelle, 9,6 - 56 Kbit/s.

Abbildung 9: Aufbau einer Chipkarte



Quelle: Pohlmann, N.: Bausteine für die Sicherheit: Chipkarten und Sicherheits-Module, in: KES, 11. Jg. (1995), Heft 5, S. 16 - 22, hier S. 18 (Änderung im Aufbau durch den Verfasser).

Für den Einsatz in Sicherheitssystemen sind verschiedene Funktionalitätsanforderungen definiert, die im folgenden aufgezeigt werden sollen:[2]

Transport- und Speicherungsfunktionen:

Die ICC soll Zertifikate (oder andere Token für Zugangsberechtigungen), Public-Keys (z.B. der Zertifizierungsinstanz) und den Private-Key des Anwenders sicher speichern können.

---

[1] Vgl. Kruse, D. / Peuckert, H.: Chipkarte und Sicherheit, in: DuD, Jg. 1995, Heft 3, S. 142 - 149, hier S. 143; **ebenso** Weimann, J.: Chipkarten: Realisierungs- und Anwendungsmöglichkeiten, in: DuD im Wandel der Informationstechnologien, Hrsg.: Spies, P. P., Berlin 1985, S. 26 - 32, hier S. 27f.

[2] Vgl. Alles, P. / Hueske, T.: Netzwerksicherheit und Chipkarteneinsatz, in: DuD, Jg. 1993, Heft 4, S. 214 - 219, hier S. 215f; **ebenso** Bauer, P. / Peuckert, H.: Chipkarten mit Kryptographie erschließen neue Anwendungsfelder, in: DuD, Jg. 1994, Heft 7, S. 380 - 384, hier S. 381f; **ebenso** Kruse, D.: Sicherheitszertifikat für Chipkarten, in: DuD, Jg. 1995, Heft 9, S. 537 - 542, hier S.539f.

Zugangskontrollfunktionen:

Die ICC soll sich dem Kommunikationssystem gegenüber identifizieren können – zudem soll sie ihren Benutzer identifizieren. Dies geschieht meist via PIN-Eingabe (Tastenfeld im Lesegerät oder auf der ICC – sog. Super-ICC mit numerischer Tastatur und einzeiligem LC-Display) mit Fehlbedienzähler, der nach dreimaliger Fehleingabe die ICC sperrt. Es sind auch Challenge/Response-Identifikationen möglich. Zudem die Überprüfung biometrischer Merkmale (s. Abschnitt 3.2.3).

Algorithmische Funktionen:

Die ICC muß Hash-Codes oder MAC's berechnen und verifizieren, digitale Signaturen erstellen, Pseudozufallszahlen generieren, verschlüsseln und entschlüsseln können.

Multifunktionalität:

Konzeptionell müssen ICC's darauf ausgelegt sein, mehrere Anwendungen gleichzeitig zu fahren, wozu Datenbereiche streng getrennt und sicher selektiert werden müssen. Es ist also eine effektive Schlüsselverwaltung erforderlich, die neben dem eigentlichen Management auch tiefergehende Datenbankfunktionen beherrschen muß. *Multifunktional* ist z.B. eine Karte, die dem Benutzer den Gebäudezugang ermöglicht, die Arbeitszeitabrechnung vornimmt, den Zugang zum Rechnersystem und der Telefonanlage verifiziert (mit einer Hierarchie von Benutzerrechten), kryptographische Sicherheitsdienste während der Kommunikation leistet und über ein integriertes Debitsystem die Bezahlung in der Firmenkantine ermöglicht.

Um ICC's sicher nutzen zu können, müssen natürlich auch bestimmte Sicherheitsvorkehrungen bei der Herstellung und Personalisierung beachtet werden, die hier aber nicht näher beleuchtet werden.

In Anlehnung an das bekannte ISO-OSI-Referenzmodell unterscheidet die ISO für die ICC im wesentlichen *vier Schichten*, auf denen kommuniziert wird:[1]

Physikalische Schicht:

Entspricht der Schicht 1 des OSI-Modells und ist in ISO 7816-1 geregelt. Hier findet die physische Datenübertragung zum Lesegerät statt.

Übertragungsprotokollschicht:

---

[1] Vgl. Hartleif, S.: Multifunktionale Chipkarten an Kommunikationsendgeräten, in: Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 11-13.11.1992, Hrsg.: ITG, Berlin 1993, S. 303 - 313, hier S. 304ff.

Diese Schicht ist in ISO 7816-3 geregelt und entspricht den OSI-Schichten 2 und 3. Hiermit wird praktisch der „Briefumschlag“ bereitgestellt, mit dem die Informationen zwischen ICC und Endgerät übertragen werden sollen. Zuvor synchronisieren sich ICC und Endgerät nach festgelegten Verfahren. Auch eine byte- oder blockorientierte Übertragung wird hier festgelegt.

Anwendungsprotokollschicht:

Hier geht es um die Frage, in welcher Form Anwendungen, die sich auf einer ICC befinden, überhaupt angesprochen und verwaltet werden können, sowie um die Bedeutung der ausgetauschten Daten (ISO 7816-4). Entspricht grob der OSI-Schicht 6.

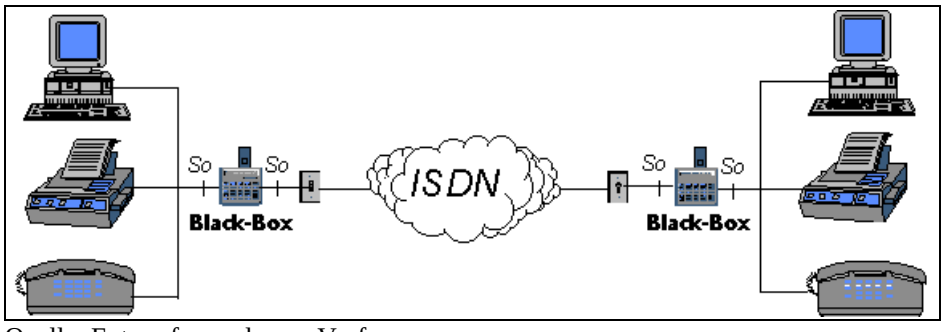
Anwendungsschicht:

Entspricht vollständig der OSI-Schicht 7 (ISO-7816-4).

3.2.2 Security-Black-Boxes

Bei den Security-Black-Boxes handelt es sich um Hardwaresicherheitseinrichtungen, die schnittstellenneutral zwischen das Endsystem und den Netzanschluß geschaltet werden (s. Abb. 10) und stellvertretend für das zu schützende Rechnersystem erweiterte Sicherheitsdienste erbringen. Sie stellen in dem Sinne keinen neuen Sicherheitsmechanismus dar, sondern sind eher als „Shell“ für die kryptographischen Verfahren zu sehen. In Abb. 10 wurde die Black-Box als Vorschaltgerät an der S_0-Schnittstelle im ISDN eingesetzt, es sind natürlich auch alle anderen WAN-Trägernetze wie z.B. Datex P (X.25) oder Standleitungen (X.21) möglich (und auch LAN- oder Backbone-Netze).[1] In Zusammenarbeit mit einer entsprechenden Box auf der Gegenseite schützen sie die Kommunikation

Abbildung 10: Security-Black-Box im ISDN



Quelle: Entworfen und gez.: Verfasser

über das Informationsnetz hinweg. Die angebotenen Sicherheitsdienste bestehen in:

- Vertraulichkeit,

---

[1] Vgl. Pohlmann, Norbert: Schutz von LAN’s und LAN-Kopplung über öffentliche Netze, in: Datacom, 12. Jg. (1995), Heft 6, S. 50 - 56, hier S. 51. (nachfolgend zitiert als: öffentliche Netze)

- Authentikation,
- Zugangskontrolle,
- Beweissicherung,
- Rechteverwaltung und
- Protokollauswertung.

Dadurch wird erreicht, daß keine Informationen im Klartext gelesen werden können, nur logische Verbindungen zustande kommen, die erlaubt sind, die Endgeräte gegenüber Dritten abgeschottet sind, nur über Protokolle und Applikationen zugegriffen werden kann, die definiert wurden, und sicherheitsrelevante Ereignisse protokolliert und ausgewertet werden können. Die Security-Black-Boxes werden oft zusätzlich mit einem Chipkartensystem versehen, damit sie nicht unbefugt manipuliert werden können.

Die *Vorteile* sind die Unabhängigkeit von Endgeräten und ihren evtl. Betriebssystemen (die Boxes können auch zwischen Telefax- und Telefonverbindungen im ISDN geschaltet werden), so daß bei jeglichem Hardware- und Plattformwechsel die Sicherheitseinrichtung beibehalten werden kann. Dies ermöglicht auch den Einsatz in heterogenen Netzen mit unterschiedlichsten Plattformen bei ein und derselben Black-Box, was einer enormen Aufwandsverringerung entspricht. Zuletzt arbeiten die Black-Boxes absolut anwendungsunabhängig – was sie leichter „sicher“ realisierbar macht als Endgeräte.

Nachteilig ist, daß alle Beteiligten zusätzliche Hardware beschaffen müssen, was in offenen Netzen zu einem Problem werden könnte. Der Urheber- und Empfängernachweis sind nur eingeschränkt möglich und es ist keine Einbindung in bestimmte Applikationen möglich, was z.B. für digitale Signaturen nötig wäre.[1]

3.2.3 Biometrie

Die sogenannten biometrischen Verfahren sind eine Möglichkeit zur Realisierung oder Verbesserung von Zugangskontrolltechniken physikalischer Art oder des Zugriffs auf Informationen. Die traditionellen Techniken beruhen darauf, daß der Teilnehmer nur ihm bekanntes Wissen besitzt oder einen persönlichen Berechtigungsschlüssel erhält – was er in beiden Fällen auch verlieren kann (durch Vergessen oder auch Raub). Im Gegensatz dazu nutzt die Biometrie physiologische oder verhaltenstypische Charakteristika des Teilnehmers zur automatischen Identitätsverifikation oder Authentikation des Benutzers – diese haben den Vorteil, daß sie nicht verloren gehen, Raub unmöglich ist und Kopien nur mit größtem

---

[1] Vgl. Pohlmann, Norbert, öffentliche Netze, a.a.O., S. 52.

Aufwand erstellt werden können. Es gibt verschiedene Ansätze biometrischer Verfahren, die sich in unterschiedlichen Entwicklungsstadien befinden (auf die Ansätze der Stimmverifikation und der Analyse der Tippdynamik wird nicht eingegangen, da sie sich bereits als zu unsicher erwiesen haben):[1]

- **Analyse von Fingerabdrücken** – Der Finger wird optisch abgetastet und das entstehende Bild in digitale Signale umgewandelt, die dann mit einem Referenzbild verglichen werden. Das System ist sehr sicher, hat jedoch eine Anfälligkeit gegenüber Verletzungen und Schmutz – zudem lassen sich (mit großem Aufwand) Fingerabdruckfolien erstellen. Weiterhin ist der Fingerabdruck bzgl. seiner Akzeptanz durch die Nutzung der Fingerabdrücke bei der Kriminalistik negativ vorbelastet.
- **Analyse der Handgeometrie** – Diese Technik beruht entweder auf der Messung der Fingerlänge oder des Handflächenmusters einer Person und dem Vergleich mit Referenzdaten. Das Verfahren liefert gute Ergebnisse.
- **Unterschrifts- / Handschriftsverifikation** – Hierbei geht es nicht nur um das „statische“ zweidimensionale Bild der Unterschrift, sondern auch um Zeitinformationen während des dynamischen Unterschriftsprozesses. Es werden Daten aus Schreibgeschwindigkeit, Schreibrichtung, Schreibdruck und dem Unterschriftsbild ausgewertet und mit Referenzdaten verglichen. Dieses Verfahren wird bereits recht häufig eingesetzt – vor allem im Bankgewerbe (z.B. Zugangsberechtigung der „Bank of Scotland“[2]).
- **Retinaabtastung** – Durch ein Binokular wird hierbei die Netzhaut abgetastet und die vorliegenden Blutgefäße gescannt – diese sind bzgl. ihrer Größe, Lage und gebildeten Muster höchst personenindividuell. Danach erfolgt ein Referenzmustervergleich. Nachteil ist, daß die Messung bei einem Menschen, der unter Anstrengung steht, zum Teil nicht durchgeführt werden kann. Zudem besteht nach wie vor Uneinigkeit über evtl. Gesundheitsschädigungen durch häufige Abtastung der Netzhaut.
- **Auswertung der Physiognomie** – Es wird ein Bild der Gesichtsfläche (z.B. Überwachungskamera) digitalisiert, bzgl. 20 bis 30 Merkmalen ausgewertet und mit Referenzwerten verglichen. Dieses Verfahren wird immer weiter perfektioniert und erkennt sogar Personen, die sich einen Vollbart haben wachsen lassen, mit Referenzwerten „ohne Bart“. Dieses Verfahren hat eine große Zukunft.

---

[1] Vgl. Wirtz, Brigitte: Automatische Unterschriftsverifikation, in: DuD, Jg. 1994, Heft 7, S. 385 - 395, hier S. 386f; **ebenso** Rinderknecht, H. / Ilg, H. / Schäfer, W.: Sicherheitssystem: Biometrische Techniken, in: DuD, Jg. 1992, Heft 5, S. 241 - 243, hier S. 241f.

[2] Vgl. Wirtz, Brigitte, a.a.O., S. 387.

Einige der oben kurz beschriebenen Verfahren werden bereits eingesetzt, um normale PIN-Systeme zu ersetzen – häufig im Zusammenhang mit Smart-Cards. Generell ist die Hardware sehr teuer, und daher sind diese Techniken derzeit für offene Informationsnetze mit einem öffentlichen Zugang relativ ungeeignet. Kommende technische Entwicklungen und steigende Rechnerleistungen könnten dies jedoch bald ändern.

3.3 Firewalls

Der Begriff „*Firewall*“ kommt aus der Architektur und kann mit „Brandschutzmauer“ übersetzt werden. Brandschutzmauern sollen die Ausbreitung eines Feuers stoppen oder es zumindest solange aufhalten, bis Hilfe eintrifft. Die Aufgabe einer Firewall bei Netzwerken ist ähnlich, geht jedoch über das Stoppen oder Aufhalten von Angriffen hinaus: „*Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen*.“[1] Es wird dafür gesorgt, daß *jede* Kommunikation zwischen den beiden Netzen *ausschließlich* über die Firewall geführt werden muß. Auf der Firewall sorgen Zugriffskontrolle und Audit (Aufzeichnung sämtlicher Kommunikationsgeschehnisse) dafür, daß das „Prinzip der geringsten Berechtigung“[2] durchgesetzt wird und potentielle Angriffe schnellstmöglich erkannt und abgewehrt werden. Die Firewall stellt die physikalische und logische Schnittstelle zwischen dem „externen“ Internetzwerk und dem zu schützenden Informationsnetz, dem Schutznetz, dar. Nach außen hin öffnet die Firewall den Zugang zum Schutznetz über unterschiedliche Übertragungsschnittstellen wie ISDN, Modem-Leitungen und X.25- oder X.21-Leitungen. Diesen Schnittstellen nachgeordnet arbeiten die jeweiligen Kontrollmechanismen, die den Verbindungsaufbau zwischen Internetzwerk und Schutznetz je nach Dienst und Teilnehmer zulassen, kontrollieren oder verhindern. Die Elemente, die diese Funktionen realisieren, werden als Zugriffskontrollelemente bezeichnet und im folgenden Abschnitt beschrieben.

Das Internetzwerk, von dem sich derzeit die meisten Informationsnetze abzuschotten suchen, ist das *Internet*, dessen Charakteristika nachfolgend kurz angesprochen werden sollen. Dieses 1969 als Forschungsvorhaben des US-Verteidigungsministeriums (DoD = Department of Defence) als ARPANET aufgebaute Netz hat sich mittlerweile zum größten weltumspannenden Netz etabliert, dessen Nutzung zunehmend die alleinige Schiene von Forschung und Lehre verläßt und fortschreitender Kommerzialisierung unterliegt. Die wesentlichen Dienste im Internet sind:[3]

- E-Mail (digitaler Nachrichtenaustausch), SMTP (= Simple Mail Transfer Protocol)

---

[1] Schlette, Joachim: Internet - Sicherheit durch Firewalls, in: Datacom, 13. Jg. (1996), Heft 1, S. 62 - 66, hier S. 63.

[2] „Alles, was nicht explizit erlaubt ist, ist erst einmal verboten.“ Vgl. Chapman, D. B. / Zwicky, E. D.: Einrichten von Internet Firewalls, Bonn 1996, S. 51.

[3] Vgl. Koritnik, Andreas: Firewalls - Welche Bastion für welchen Dienst ?, in: KES, 11. Jg. (1995), Heft 6, S. 31 - 38, hier S. 31; **ebenso** Wallich, Paul: Piraten im Datennetz, in: Spektrum der Wissenschaft, Jg. 1994, Heft 5, S. 64 - 70, hier S. 69.

- News (Teilnahme an weltweiten Foren),
- FTP (=File Transfer Protocol – Übertragen von Dateien),
- Telnet (Dialogzugriff / Online-Datenbankrecherche),
- Gopher (Strukturierung von Archiven und Recherchematerial) und
- WWW (= World Wide Web – integriert andere Dienste unter einer Multimedia-Oberfläche, die zur Verbreitung und Kommerzialisierung des Internet führte).

Diese Dienste wurden ursprünglich nicht mit Sicherheitsfunktionen versehen, zudem kommen Schwächen in diesen Dienstprogrammen, in der klassischen Internetsystemumgebung UNIX und weitere Schwächen in den verwendeten Datenübertragungsprotokollen. Diese Protokollfamilie wird in Abb. 11 dem OSI-Schichtenmodell gegenübergestellt, um eine Orientierung zu ermöglichen. Das verwendete Protokoll IP und die dar-

Abbildung 11: DoD-Protokollfamilie

ISO-OSI		TCP/IP-Protokollfamilie					
7	Anwendungsschicht	5	Process/ Application	Telnet inter-aktiver Terminal-verkehr	FTP File Transfer Protocol	SMTP Simple Mail Transfer Protocol	NSP Name Server Protocol
6	Darstellungsschicht						
5	Kommunikations-steuerungsschicht						
4	Transportschicht	4	Transport	TCP Transmission Control Prot.		UDP User Datagram P.	
3	Vermittlungsschicht	3	Internet	IP Internet Protocol			
2	Sicherungsschicht	2	Network	Netz als Datentransportressource, wie X.25-Wide Area Network, LAN nach IEE 802 , Nebenstellenanlage oder privates Daten-leitungsnetz (nicht im Sichtbereich der TCP/IP-Protokolle)			
1	Bitübertragungsschicht	1	Physical				

Quelle: Eigene Darstellung in Anlehnung an: Pohlmann, Norbert: Sicherheit in UNIX-Netzen, in: Datacom, 10. Jg. (1993), Heft 12, S. 122 - 129, hier S. 123.

überliegenden Protokolle TCP und UDP beinhalten keine sicheren Mechanismen zur Identifikation und Authentikation im Netz [1] – das ohne Firewall auch in das Schutznetz reicht, da zur Nutzung aller Dienste das Schutznetz transparent auf TCP/IP-Ebene an das Internet gekoppelt werden muß.[2] Auf der Ebene der transparenten Netzkopplung setzen die Firewalls an und verhindern eine „unkontrollierte Kopplung“ zwischen dem sicheren, bekannten Schutznetz und dem unüberschaubaren, anonymen Internet.

---

[1] Vgl. Koritnik, Andreas: Firewalls für’s Internet - Alle Schotten dicht ?, in: KES, 11. Jg. (1995), Heft 3, S. 36 - 42, hier S. 36 (nachfolgend zitiert als: Schotten dicht); **ebenso** Stang, David / Becker, Lutz: Flächenbrände im Netz ?, in: Datacom, 12. Jg. (1995), Heft 6, S. 66 - 76, hier S. 68ff.

[2] Vgl. Siyan, Karanjit / Hare, C.: Internet Firewalls und Netzwerksicherheit, München 1995, S. 173f.

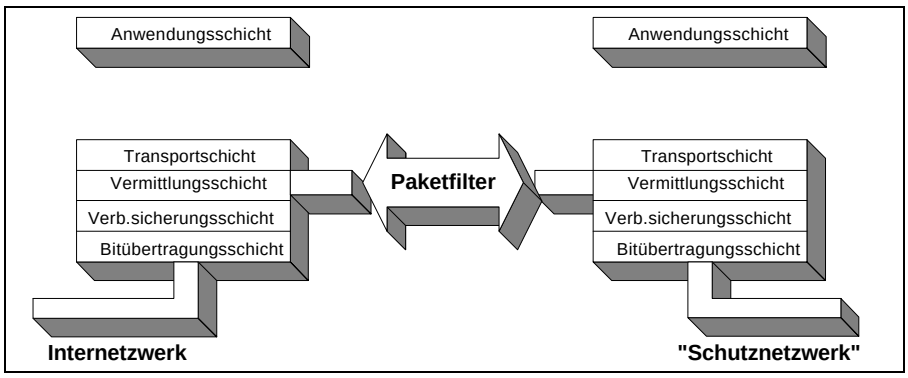
3.3.1 Firewall-Zugriffskontrollelemente

Für die Realisierung von Firewall-Systemen stehen drei Zugriffskontrollelemente zur Verfügung, die in den verschiedenen Firewall-Architekturen (s.u.) einzeln oder meist in Kombination miteinander zur Anwendung kommen.

3.3.1.1 Paketfilter

Diese Filterkomponente ist ein Zugangsschutzmechanismus, der auf der Schicht 3 des OSI-Modells entsprechend der IP-Ebene angesiedelt ist (s. Abb. 12) und in der Regel von Routern wahrgenommen wird. Die Paketfilter sind in der Lage, Datenpakete nach Kriterien wie Sende- / Empfangsadresse, Protokollen, Protokoll-Ports und benutzerdefinierten Bitmasken zu filtern. Darüber hinaus ist eine Richtungsfestlegung (inbound / outbound) für einzelne Dienste bzw. Ports möglich (z.B. im Internet FTP-Zugriff nur vom Schutznetz nach „außen“). Korrekte Datenpakete werden weitergeleitet, inkorrekte

Abbildung 12: Paketfilter und das OSI-Schichtenmodell



Quelle: Kyas, Othmar, a.a.O., S. 135.

werden unterdrückt. Die Filtervorschriften werden in Tabellen festgehalten (Access Control Lists, ACL), was sich bei komplexen Netzwerken schnell als unübersichtlich erweist. Bei Client/Server-Anwendungen auf Basis von Remote Procedure Calls (RPC) können Paketfilter nicht wirksam werden, da bei dynamischer Portwahl durch den Portmapper auf dem Server einer Applikation die Portnummer auf Zufallsbasis zugewiesen wird – für die natürlich im vorhinein keine Filterregel aufgestellt werden kann.[1]

Benutzerbezogene Identifikation und Authentikation für bestimmte Dienste oder ein effektives Auditing werden nicht vorgenommen. Die Paketfilter werden meist in die ohnehin vorhandenen Router integriert, die ebenfalls auf Schicht 3 arbeiten, und als Vorfiltersystem für die folgenden Kontrollelemente genutzt.

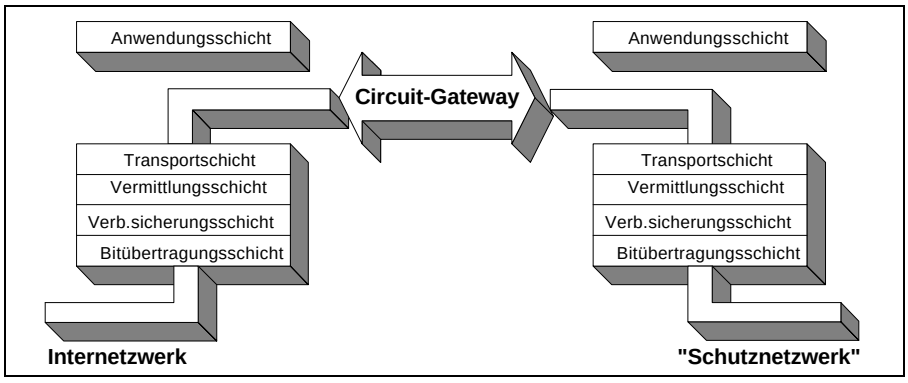
---

[1] Vgl. Schlette, Joachim, a.a.O., S. 63.

3.3.1.2 Circuit Level Gateways

Eine deutliche Erhöhung der Netzwerksicherheit wird durch den Einsatz von auf Circuit Level Gateways (oder auch nur Circuit Gateway) basierenden Firewall-Zugriffskontrollelementen erreicht. Diese ermöglichen im Internet-Bereich den Betrieb von auf den

Abbildung 13: Circuit Level Gateway und das OSI-Schichtenmodell



Quelle: Kyas, Othmar, a.a.O., S. 135.

Kommunikationsprotokollen TCP bzw. UDP aufsetzenden Applikationen wie WWW, Telnet etc., ohne eine durchgehende Kommunikationsverbindung zuzulassen – die Firewall setzt hier also über der OSI-Schicht 4 auf (s. Abb. 13). Die IP-Verbindungen laufen vom Schutznetz zum Gateway und vom Gateway zum Zielcomputer im Internetzwerk. Alle Adressen werden also am Circuit Level Gateway dynamisch ausgetauscht, so daß es eine Art *Vermittlungsstelle* darstellt – die Rechner des Schutznetzes bleiben der Außenwelt so verborgen. Ein Nachteil dabei ist, daß die Client-Applikationen des Schutznetzes allesamt an das Circuit Level Gateway angepaßt werden müssen, was mitunter sehr aufwendig ist. Den Mechanismus, *stellvertretend* für den jeweiligen Client den Auf- und Abbau von Kommunikationsverbindungen zu übernehmen, nennt man Proxy – das Gateway *Proxy Server*.[1] Mit Circuit Level Gateways ist es also möglich, durch die Bearbeitung der Adreß- und Portinformationen der Datenpakete einzelne Verbindungswege für einzelne Dienste zwischen spezifischen Kommunikationspartnern dediziert zu öffnen, obwohl ansonsten jegliches Routing zwischen Schutznetz und Internetzwerk unterbunden ist. Der Verbindungsaufbau, die genutzten Dienste und die passierenden Datenpakete werden protokolliert. Eine Benutzer-Authentikation an der Vermittlungsstelle ist eingeschränkt mittels Paßwortabfrage oder Challenge/Response möglich[2], und es ist hervorzuheben, daß diese Gatewayform

---

[1] Vgl. Kossel, Axel: Innere Sicherheit. Sichere Intranet-Lösungen, in: c't Magazin für Computertechnik, Jg. 1996, Heft 10, S. 332 - 334, hier S. 333.

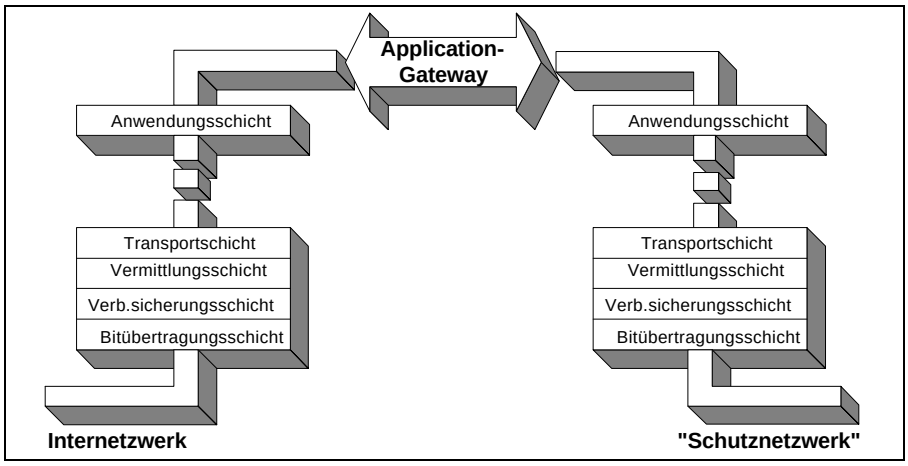
[2] Vgl. Munzert, M. / Wolff, C.: Firewalls - Schutz vor Angriffen aus dem Internet, in: DuD, Jg. 1996, Heft 2, S. 89 - 93, hier S. 91.

relativ wenig Rechenleistung erfordert und in leistungsfähige Public-Domain-Versionen verfügbar ist.[1]

3.3.1.3 Application Gateways

Application Gateways stellen das Extrem der Kontrollelemente einer Firewall dar, denn statt den gesamten Verkehrsfluß mit einem Allzweckmechanismus zu kontrollieren, wird für jede Anwendung ein spezielles Programm zur Verfügung gestellt – das natürlich erst erstellt werden muß. Wie in Abbildung 14 ersichtlich, arbeitet dieses Gateway daher auf der Anwendungsschicht, der Schicht 7 des OSI-Modells. Dem hohen Aufwand steht jedoch ein System gegenüber, das sicherer ist als alle anderen Kontrollelemente und am

Abbildung 14: Application Gateway und das OSI-Schichtenmodell



Quelle: Kyas, Othmar, a.a.O., S. 136.

besten das „Prinzip der geringsten Berechtigung“ erfüllt.[2] Dies ermöglicht die Zugriffskontrolle auf Benutzer- und Anwendungsebene, wobei zudem noch eine intelligente Protokollierung bezüglich der Anwendungsnutzung und ein- und ausgehender Datenströme realisierbar ist. Das je Anwendung speziell erstellte Programm arbeitet als Stellvertreter (Proxy) der eingehenden Anforderungen von beiden Netzseiten, das anhand einer Zugriffsliste feststellt, welche Art von Anforderung für welchen Benutzertyp erlaubt ist. Der Proxy-Server vertritt bei diesem Gateway den Anwendungsserver, der nach Prüfung und Erlaubnis die Anforderung an den entsprechenden Server weiterleitet, so daß der Proxy als Client und Server arbeitet, und die Client-Systeme keinerlei Modifikation unterworfen werden müssen.[3] Auch bei diesem Zugriffskontrollelement besteht keinerlei direkte Kommunikationsverbindung auf Protokollebene und die Rechner des Internetzwerkes erhalten keinerlei In-

---

1 Vgl. Kyas, Othmar, a.a.O., S. 167.

2 Vgl. Cheswick, W. / Bellovin, S.: Firewalls and Internet Security, Reading 1996, S. 89.

3 Vgl. Gaissmaier, Karl: Implementation eines Firewalls unter Verwendung frei verfügbarer Software, CERT: DFN-Bericht Nr. 78, URL:http://www.cert.dfn.de/dfn/berichte/db078/firewall/: 23.11.1996

formationen über ihr tatsächliches Gegenüber im Schutznetz, sondern kennen nur das Application Gateway als Kommunikationspartner. Es ist zudem möglich, nach der Zuweisung und Verbindung mit dem Port, auf dem der Proxy-Server läuft, eine spezielle Eingabeaufforderung einzubauen. Es kommt daher zu einer starken Benutzeridentifikation und -authentikation und einem umfassenden Auditing mit vielfältigen Informationen.
Es gibt auch eine Variante des Application Gateway, die ohne Proxy-Server arbeitet und den Anwendern Accounts zuweist, auf denen ihnen nach einem Login erlaubt wird, die entsprechenden (gewünschten) Dienste selbst zu nutzen – diese Variante ist jedoch durch die Accounts und ihre Paßwortsicherheit nicht sehr effektiv und wird hier daher nicht weiter vertieft.[1]

3.3.2 Firewall-Architekturen

In Firewall-Systemen werden meist Kombinationen der drei oben beschriebenen Zugriffskontrollelemente verwendet, woraus sich grob vier verschiedene Firewallarchitekturen ergeben, die nachfolgend anhand ihrer Konfiguration und Funktionsweise sowie ihrer Vor- und Nachteile beschrieben werden sollen. Bei den Dual Homed Gateways und Screened Subnets sind noch diverse Varianten und Ausprägungen denkbar, die nicht näher dargestellt werden – die Möglichkeit der Kaskadierung ist als fünfte Architektur kurz erwähnt.

3.3.2.1 Screening Router

Dies ist die einfachste Art, einen geschützten Zugang zum Internetzwerk zu realisieren. Die Funktionsweise beruht auf einer reinen Paketfilter-Firewall, die (im Falle des Internet) IP-Pakete dahingehend filtert, ob es sich um eine erlaubte Nutzung eines Kommunikationsdienstes handelt oder nicht. Dabei erweist sich die Verwendung von „*Pass-Filtern*“ in den Access Control Lists aus Performance-Gründen als praktikabler, denn es werden nur die Adressen und Ports durchgelassen, die erlaubt sind. Bei „*Deny-Filtern*“ kann es zu drastischen Performance-Einbußen kommen, denn es werden alle Filter überprüft, ob nicht doch ein „Pass“ gesetzt ist. Zudem weiß man im voraus oft nicht, was gefährlich – und damit zu verbieten – ist. Von *Vorteil* ist, daß die Installation einfach und preisgünstig ist. *Nachteile* sind:[2]

- Keine benutzerbezogene Sicherheit, sondern rein maschinenbezogene Kontrolle, bei der falsche IP-Adressen durch einen Angreifer leicht vorzutäuschen sind.

---

[1] Vgl. Schlette, Joachim, a.a.O., S. 63.
[2] Vgl. Koritnik, Andreas, Schotten dicht, a.a.O., S. 40.

- Kein Audit der Verbindung.
- Netzstruktur des Schutznetzes wird nicht verborgen.
- Komplizierte Pflege der ACL mit begrenzten Filtermöglichkeiten – zudem nur bei bekannten Portnummern möglich.
- Einzige Barriere zum Internetzwerk.
- Korrekte Konfiguration jedes Schutznetzrechners ist sicherheitsrelevant.

3.3.2.2 Screened Gateway

Ein Screened Gateway ist eine Kombination aus einem Screening Router und einem *Bastion Host*, wobei letzterer einen speziell konfigurierten Rechner bezeichnet, über den als Gateway die gesamte Kommunikation zwischen Internetzwerk und Schutznetz stattfindet und der physikalisch wie ein normaler Rechner mit dem Schutznetz verbunden ist. Die Kontrolle der Kommunikation erfolgt hierbei auf der Anwendungsschicht durch den Einsatz von zusätzlichen Application-Gateways. Direkte Verbindungen zwischen den beiden Netzen werden auf einer logischen Ebene durch die Konfiguration der Komponenten unterbunden.

Am Application-Gateway liegen bedeutend mehr Informationen vor als bei der reinen Router-Lösung, so daß hier eine Authentikation der Benutzer stattfinden kann. Auch das Auditing ist umfangreicher und aussagekräftiger. Das Gateway arbeitet als transparenter Vermittler auf der Vermittlungsschicht (IP).[1] Die Vorteile dieser Lösung sind:

- Benutzerbezogene Sicherheit mit Authentikation.
- Die Schutznetzstruktur wird verborgen.
- Logging und aussagekräftiges Auditing sind möglich.
- Nur korrekte Konfiguration des Bastion Host ist sicherheitsrelevant.

Folgende Nachteile sind jedoch vorhanden:

- Benutzer müssen einen zusätzlichen Anmeldevorgang über sich ergehen lassen.
- Es ist weiterhin nur eine Barriere zwischen den Netzen zu überwinden.
- Die Administration des Gesamtsystems ist aufwendiger als bei einem Router allein.

3.3.2.3 Dual Homed Gateway

Ein Dual Homed Gateway trennt das Internetzwerk und das Schutznetz physikalisch, indem der Bastion Host mit zwei Netzwerk-Adaptern ausgestattet wird, die jeweils eines der beiden Netze bedienen. Ansonsten besteht diese Architektur aus einem (oder auch zwei – je einen pro Netzwerk-Adapter) Screening Routern und einem Circuit Level Gateway oder

Application Gateway. Durch eine entsprechende Konfiguration des Gateways ist sichergestellt, daß kein direkter Informationsfluß an dem Circuit Level Gateway oder Application-Gateway vorbei zwischen den Netzen möglich ist. Diese Maßnahme führt zu einer hochwirksamen Netztrennung für sämtliche tieferliegenden Protokolle. Zudem sind bei dieser Architektur zwei bis drei Hürden für Angreifer zu nehmen, da selbst bei Überwindung des zum Internetzwerk liegenden Routers noch das Gateway und ein eventuell weiterer Router vor dem Schutznetz liegen. Zusätzlich zu den Vorteilen des Screened Gateways haben Dual Homed Gateways folgende Vorteile:[2]

- Es können öffentliche Dienste (z.B. WWW) zwischen Router und Bastion angeboten werden.
- Zwei bzw. drei Barrieren.
- Das Gateway (Bastion) ist auch von „hinten“ durch einen Router geschützt.

Weitere Nachteile zu denen des Screened Gateways:

- Noch aufwendigere Administration des Systems.
- Starke Unflexibilität bei Anwendungen, für die kein Proxy besteht, da kein Umweg angeboten werden kann.

3.3.2.4 Screened Subnet

Diese Firewall-Architektur beruht auf dem Prinzip, daß ein separat isoliertes Teilnetz zwischen Internetzwerk und Schutznetz von zwei Screening Routern gebildet wird, in dem mehrere Gateways und Server für verschiedenste Dienste installiert werden können. Der Standort eignet sich besonders für Informations-Server und Mail-Server (die Benutzer des Schutznetzes holen sich ihre E-Mails dann aus dem Screened Subnet), aber auch für Modem-Pools für asynchrone Verbindungen, wodurch eine wirkungsvolle Authentikation schon vor dem Schutznetz möglich ist. Direkte Datenfluß wird natürlich auch hier durch die Router und die Anbindung der Gateways an diese unterbunden.[3] Es werden folgende spezifische Vorteile geboten:

- Eigene Server für spezielle Dienste.
- Öffentliche Dienste (wie z.B. WWW) können im Teilnetz angeboten werden.

Zusätzliche Nachteile:

---

[1] Vgl. Koritnik, Andreas, Schotten dicht, a.a.O., S. 40f.
[2] Vgl. Schlette, Joachim, a.a.O., S. 64f.
[3] Vgl. Pohlmann, Norbert: Corporate Networks, in: KES, 12. Jg. (1996), Heft 3, S. 56 - 60, hier S. 60.

- Sehr komplexe Struktur, die hohen Aufwand erfordert.
- Preislich teuere Architektur.

3.3.2.5 Kaskadierende Firewall-Systeme

Bei komplexen Schutznetzen und bei heterogenem Schutzbedürfnis des Schutznetzes bezüglich eventueller Teilschutznetze oder einzelner Rechner ist eine Kaskadierung von Firewall-Systemen erforderlich. Dem Screening Router sind dabei zwei oder mehrere Bastion Hosts nachgeordnet, wodurch eine feinere Abstimmung der jeweiligen Schutzbedürfnisse möglich ist (es gibt innen- und außenliegende Bastion Hosts).[1] Eine genauere Darstellung soll wegen der großen Komplexität des Themas in dieser Arbeit nicht geschehen. Dem zusätzlichen Vorteil der feineren Schutzabstimmung stehen sehr hoher organisatorischer, administrativer und finanzieller Aufwand als Nachteile gegenüber.

3.3.3 Grenzen von Firewalls

Zum Schutz von Informationsnetzen sind Firewalls ein Mechanismus von großer, aber dennoch beschränkter Mächtigkeit. Es ist wichtig, ihre Grenzen ebenso wie ihre Möglichkeiten zu kennen. Sie sind lediglich in der Lage, Netzwerkaktivitäten zwischen den OSI-Schichten 2 und 7 (Sicherungsschicht bis Anwendungsschicht) zu überwachen. Daten, die innerhalb von Applikationen transportiert werden und z.B. in Form von Viren das Schutznetz bedrohen, können nicht blockiert werden – zu vielfältig sind die Möglichkeiten, die Dateninhalte zu verschlüsseln, um spezifische Bitfolgen zu verbergen.

Firewalls bieten auch keine Sicherung gegen unautorisierte physikalische Zugriffe auf das Schutznetz. Desweiteren können Firewalls weitgehend nur gegen derzeit bekannte Angriffsformen schützen und müssen generell laufend einer sorgfältigen Überwachung, Anpassung und Pflege unterworfen werden. Auch Sicherheitslücken „von hinten“ aus dem Schutznetz unterwandern natürlich eine Firewall (wenn z.B. ein Schutznetzanwender ein Modem an seinen Rechner anschließt und damit eine Hintertür öffnet).[2]

---

[1] Vgl. Ellermann, Uwe: Firewalls - Klassifikation und Bewertung, DFN-CERT Workshop URL=http://www.cert.dfn.de/team/ue/fw/workshop/: 15.12.1996

[2] Vgl. Vgl. Chapman, D. B. / Zwicky, E. D, a.a.O., S. 23ff; ebenso Cheswick, W. / Bellovin, S., a.a.O., S. 97ff.

4 Evaluierung

Nachdem im dritten Abschnitt verschiedene Mechanismen vorgestellt wurden, die jeweils einen Teil der in Abschnitt 2.3 geforderten neun Sicherheitsdienste erfüllen, stellt sich die Frage, in welchem Maße welche der neun Sicherheitsdienste (oder der vier Sicherheitskriterien) objektiv erfüllt werden. Um Mechanismen oder Produkte bzw. Konzepte im Bereich der IT beurteilen zu können, wurden nationale bzw. internationale Richtlinien geschaffen, anhand derer eine Wertbestimmung (*Evaluierung*) objektiv nach einheitlichen Kriterien erfolgen kann. Die Evaluierung stellt konkret eine Musterprüfung einer IT-Komponente dar, bei der auch die Dokumentation und der Herstellungsvorgang in die Bewertung einbezogen werden. Bei einer anerkannten Prüfstelle (z.B. TÜV Rheinland) wird die Evaluierung beantragt, dort vorbereitet, gemäß den Vorschriften durchgeführt und letztendlich dem Antragsteller (im positiven Fall) ein Zertifikat ausgestellt, in dem alle Daten der Komponente, der Prüfung und der Bewertung festgehalten werden.[1] Nachfolgend werden die drei bekanntesten Bewertungsgrundlagen *kurz* vorgestellt. Es wird von der ISO angestrebt, zu einem einheitlichen Standard der Evaluierung zu kommen. Wichtig erscheint in diesem Zusammenhang das Ziel, die Sicherheitskriterien der einzelnen Bewertungsgrundlagen so zu präzisieren, daß sie sich auf den einzelnen Schichten des OSI-Referenzmodells abbilden lassen.

4.1 Orange Book (TCSEC) / Red Book

Der eigentliche Titel lautet „Trusted Computer System Evaluation Criteria“ (TCSEC) und wurde 1983 im Auftrag des DoD (US-Verteidigungsministerium) erstellt – wegen der Farbe seines Einbandes nennt man es *Orange Book*. Es beurteilt die Sicherheit nach sechs Hauptkriterien und die Klassifizierung erfolgt in vier Gruppen mit insgesamt sieben Sicherheitsklassen. Dabei wurde ursprünglich nicht auf Netzwerke reflektiert, so daß 1987 eine Erweiterung in Form der „Trusted Network Interpretation“ (TNI) als *Red Book* unter Beibehaltung der Sicherheitsklassen veröffentlicht wurde.[2]

---

[1] Vgl. Kersten, H.: Evaluierung und Zertifizierung von IT-Systemen, in: Sicherheit in Informationssystemen, Proceedings SECUNET ’91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 333 - 348, hier S. 338ff (nachfolgend zitiert als: Evaluierung); **ebenso** Stiegler, H. G.: Welche Sicherheit bietet ein evaluiertes System ?, in: Verläßliche Informationssysteme, Proceedings VIS’91, Hrsg.: Pfitzmann, A. / Raubold, E., Berlin et al., S. 277 - 288, hier S. 284.

[2] Vgl. Roberts, D. W.: Evaluation Criteria For IT-Security, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 151 - 161, hier S. 153f; **ebenso** Russell, Deborah / Gangemi Sr., G. T., a.a.O., S. 226ff.

Die sechs Beurteilungskriterien sind:[1]

1. Sicherheitspolitik (security policy) – Sie beschreibt die Art des Zugriffs auf Objekte: benutzerunbestimmbarer Zugriff: Zugriff aufgrund eines festgelegten Sensivitätsgrades / benutzerbestimmbarer Zugriff: Zugriff nur für den Eigentümer der Daten.
2. Kennzeichnung (marking) – Voraussetzung für die Sicherheitspolitik ist eine Klassifizierung der Objekte nach Schutzgraden und der Subjekte nach Zugriffsrechten auf die Objekte – differenziert nach Schutzgraden.
3. Identifikation – Objekte müssen zuverlässig identifiziert werden können; die Angaben über Identifikation und Rechte müssen im System sicher gespeichert sein.
4. Nachvollziehbarkeit (accountability) – Protokollierung sicherheitsrelevanter Aktionen
5. Funktionsgarantie (assurance) – Die Funktion sämtlicher sicherheitsrelevanter Komponenten des Systems ist zu gewährleisten und muß analysiert und getestet sein.
6. Funktionsschutz (continuous protection) – Die Sicherheitsmechanismen müssen permanent vor jeglicher Manipulation und unautorisierten Zugriffen geschützt sein.

Zur Handhabung des Kriterienkatalogs werden sieben Sicherheitsklassen (s. Tabelle 2) definiert, deren Sicherheit D < C1 < C2 < B1 < B2 < B3 < A ansteigt.

Tabelle 2: Die Sicherheitsklassen des Orange Book

Sicherheitsklassen (SK)	Erläuterung
D: Minimale Sicherheit	Minimaler Schutz.
C: Benutzerbestimmbare Sicherheit	Der Benutzer vergibt selbst Zugriffsbeschränkung.
C1	Anforderung ist der Zugriffsschutz durch Identifikation, Authentikation, Rechteverwaltung und Rechteprüfung.
C2	Protokollierung der Vorgänge sowie Zuordnung der Vorgänge dem jeweiligen Benutzer.
B: Festgelegte Sicherheit	Der Zugriffsschutz wird von einer übergeordneten Instanz vergeben.
B1	C2 plus Zugriffskontrolle durch Attributvergabe an Benutzer und Programme.
B2	B1 plus Verwaltung der Zugriffsrechte über den Referenzmonitor.
B3	B2 plus die Systemfähigkeit, sicherheitsrelevante Er-eignisse zu überwachen, zu protokollieren und Abwehrmaßnahmen zu ergreifen.
A: Verifizierte Sicherheit	Die Anforderungen von B3 werden in verifizierter Form abermals überprüft.

Quelle: eigene Darstellung, Inhalte entnommen aus: Kyas, Othmar, a.a.O., S. 185f.

Das bei Punkt B2 genannte Referenzmonitor-Konzept stellt die erlaubten Beziehungen (Referenzen) zwischen Benutzer (Subjekt) und Programmen bzw. Daten (Objekt) dar. Sie werden in einer Datenbasis abgebildet, in der die Sicherheitsanforderungen enthalten sind und die vom Referenzmonitor verwaltet wird. Unberechtigte Zugriffe werden aufgezeichnet.

[1] Vgl. Wähner, Gerd W., a.a.O., S. 165.

4.2 IT-Sicherheitskriterien (ITSK89, ITEH90)

Die IT-Sicherheitskriterien (ITSK) wurden am 01.06.1989 im Bundesanzeiger veröffentlicht und wenden sich an Anwender, Betreiber und Hersteller von IT-Systemen sowie an Prüfstellen (wie z.B. das Bundesamt für Sicherheit in der Informationstechnik (BSI)). Im Gegensatz zum Orange Book nehmen die IT-Kriterien eine getrennte Beurteilung von Funktionalität (10 Kriterien) und Qualität (8 Qualitätsklassen) vor. Die Funktionskriterien wurden zum Teil vom Orange Book abgeleitet (Hierarchische Gliederung) und durch zusätzliche Kriterien erweitert (s. Tabelle 3).[1]

Tabelle 3: Die Funktionalitätsklassen der IT-Kriterien

Funktionalitätsklassen (abgeleitet aus Orange Book Klasse)		
F1	Benutzerbestimmbarer Zugriffsschutz (C1)	1. Hierarchiestufe
F2	Protokollierungsmechanismen (C2)	2. Hierarchiestufe
F3	Benutzerunbestimmbarer Zugriffsschutz (B1)	3. Hierarchiestufe
F4	Vertrauenswürdiger Zugriffspfad (B2)	4. Hierarchiestufe
F5	Überwachung sicherheitsrelevanter Vorgänge (B3 / A1)	5 . Hierarchiestufe
F6	Anforderungen an Datenintegrität	nicht hierarchisch gegliedert
F7	Anforderungen an Verfügbarkeit	
F8	Anforderungen an Integrität der Datenübertragung	
F9	Anforderungen an Geheimhaltung während der Datenübertragung	
F10	Anforderungen an Vertraulichkeit und Integrität der Daten in Netzwerken	

Quelle: eigene Darstellung, Inhalte entnommen aus: Zentralstelle für Sicherheit in der Informationstechnik: IT-Sicherheitskriterien - Kriterien für die Bewertung der Sicherheit von Systemen der IT vom 11.01.1989, Köln 1989, S. 27ff.

Die acht Qualitätsklassen, die hierarchisch gegliedert sind, stellen einen Bewertungsmaßstab für die Tiefe der Systemprüfung und die Stärke der Sicherheitsmechanismen dar (s. Tabelle 4).

Tabelle 4: Die Qualitätsklassen der IT-Kriterien

Klasse	Prüfungstiefe	Sicherheitsmechanismen
Q0	unzureichende Qualität	unwirksam bzw. schwach
Q1	getestet	mittelstark mit Ausnahmen
Q2	methodisch getestet	mittelstark
Q3	Q2 + teilanalysiert	stark mit Ausnahmen
Q4	Q3 + informell analysiert	stark
Q5	Q4 + semiformal analysiert	sehr stark mit Ausnahmen
Q6	Q5 + formal analysiert	sehr stark
Q7	Q6 + formal verifiziert	maximaler Schutz

Quelle: eigene Darstellung, Inhalte entnommen aus: Zentralstelle für Sicherheit in der Informationstechnik, a.a.O., S. 54f.

Das IT-Evaluationshandbuch (ITEH) wurde im August 1990 veröffentlicht und beschreibt den Prüfvorgang bei der Evaluierung eines Systems. Es wendet sich in erster Linie an Hersteller von IT-Produkten und Prüfstellen.

---

[1] Vgl. Kersten, H., Evaluierung, a.a.O., S. 336.

4.3 ITSEC (Vier-Nationen-Entwurf)

Am 2. Mai 1990 wurde im Auftrag der EG-Kommission in Zusammenarbeit der vier Nationen Bundesrepublik Deutschland, Frankreich, Großbritannien und der Niederlande ein Kriterienkatalog zur Bewertung von IT-Sicherheit, die *Information Technology Security Evaluation Criteria* (ITSEC), herausgegeben. Mit den Kriterien soll eine Basis für eine weitergehende internationale Harmonisierung geschaffen werden. Sie sind in Funktionalitätsklassen und Qualitätsklassen gegliedert. Bezüglich dieser Klassen ist in den ITSEC die Systematik der deutschen ITSK89 übernommen worden, wobei aber zugunsten eines klareren Aufbaus auf Sicherheitsanforderungen verzichtet wurde.[1] In Tabelle fünf sieht man eine Übersicht der Funktionalitätsklassen, wobei auffällt, daß bei der Namensgebung zur Parallelisierung auch TCSEC-Begriffe eingearbeitet wurden.

Tabelle 5: Die Funktionsklassen der ITSEC-Kriterien

Funktionsklassen		
F-C1	Benutzerbestimmbarer Zugriff.	analog F1 / ITSK89
F-C2	Protokollierungsmechanismen.	analog F2 / ITSK89
F-B1	Benutzerunbestimmbarer Zugriffsschutz.	analog F3 / ITSK89
F-B2	Vertrauenswürdiger Zugriffspfad.	analog F4 / ITSK89
F-B3	Überwachung sicherheitsrelevanter Vorgänge.	analog F5 / ITSK89
F-IN	Anforderung an Datenintegrität von Programmen und Informationen.	analog F6 / ITSK89
F-AV	Anforderung an Verfügbarkeit.	analog F7 / ITSK89
F-DI	Anforderung an Integrität der Datenübertragung.	analog F8 / ITSK89
F-DC	Anforderung an Geheimhaltung von Informationen bei der Datenübertragung (Verschlüsselung).	analog F9 / ITSK89
D-DX	Anforderungen an Vertraulichkeit und Integrität der Daten in Netzwerken.	analog F10 / ITSK89

Quelle: Wagner, M.: Evaluierung von IT-Systemen und Produkten nach den ITSEC, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’92, Hrsg.: Lippold, H. / Schmitz, P., Braunschweig 1992, S. 151 - 172, hier S. 161.

Bei der Bewertung der Qualität von IT-Komponenten wird hier zwischen der Korrektheit der Komponente und ihrer Wirksamkeit unterschieden. Die Vertrauenswürdigkeit (Qualität) der Korrektheit wird in sieben Stufen (E0 - E6) mit steigender Prüftiefe bewertet (s. Tabelle 6).[2]

Zu den ITSEC gibt es auch ein Evaluationshandbuch, das Information Technology Security Evaluation Manual (ITSEM), das die gleiche Funktion hat wie das ITEH90 für die ITSK89.

---

[1] Vgl. Meyer, M. / Rannenberg, K.: Eine Bewertung der ITSEC, in: VIS’91 Verläßliche Infomationssysteme (Proceedings), Informatik-Fachberichte 271, Hrsg.: Pfitzmann, A., Berlin u.a. 1991, S. 133 - 145, hier S. 243ff; **ebenso** Mackenbrock, Markus: ITSEC Funktionalitätsklasse für die Sicherheit von digitalen TK-Anlagen, in: BSI-Forum, 3. Jg. (1995), Heft 3, S. 47 - 51, hier S. 48.

[2] Vgl. Keus, Klaus: Aktuelle IT-Sicherheitskriterien, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’93, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1993, S. 171 - 200, hier S. 181f.

Tabelle 6: Die Qualitätsklassen der ITSEC-Kriterien

Qualitätsklassen	
E0	Unzureichende Sicherheit
E1	Eine informelle Beschreibung des Architekturentwurfs muß vorliegen. Das System wurde mit funktionalen Tests getestet
E2	E1 plus informelle Beschreibung des Feinentwurfs sowie Bewertung der Aussagen der funktionalen Tests
E3	E2 plus Bewertung des Quellcodes und der Hardwarekonstruktionszeichnungen
E4	E3 plus ein formales Sicherheitsmodell und eine semiformale Notation des Feinentwurfs und des Architekturentwurfs
E5	E4 plus enger Zusammenhang zwischen Feinentwurf, Quellcode und Hardwarekonstruktionszeichnungen
E6	E5 plus Vorlage des Architekturentwurfs und der sicherheitsspezifischen Funktionen in formaler Notation deren Prüfung auf Konsistenz mit dem zugrundeliegenden Sicherheitsmodell.

Quelle: Wagner, M., a.a.O., S. 164

5 Sicherheitskonzepte in praxi

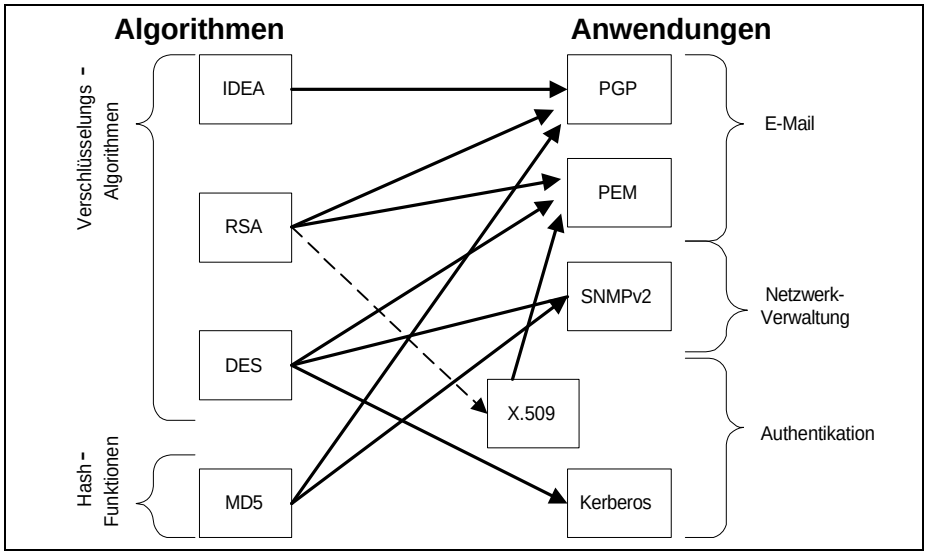
In diesem Abschnitt soll nun aufgezeigt werden, welche der in Abschnitt drei beschriebenen Technologien in IT-Sicherheitsprodukte umgesetzt wurden, am Markt für Informationssicherheit angeboten werden und in Informationsnetzen zum Einsatz kommen. Der Vollständigkeit halber werden auch Produkte aufgezeigt, die nicht ausschließlich oder gar nicht auf bereits beschriebenen Technologien fußen, aber im Rahmen einer modernen Sicherheitskonzeption nicht fehlen dürfen.

Jede der im ersten Unterabschnitt dargestellten Sicherheitskomponenten stellt für sich ein Sicherheitskonzept dar, das allerdings im Zusammenspiel mit weiteren Komponenten zu mächtigeren Konzeptionen aggregiert werden kann. Im zweiten Unterabschnitt soll daher auf dieses Zusammenspiel einzelner Komponenten als Gesamtkonzeption eingegangen werden. In beiden Unterabschnitten kann die Thematik nur auszugsweise behandelt werden, da eine große Produktpalette am Markt angeboten wird.

5.1 Sicherheitskomponenten am Markt

Hierbei handelt es sich zum einen um einzelne Produkte[1], die eine oder mehrere der bereits vorgestellten Technologien in sich vereinen und am IT-Markt erhältlich sind, zum anderen um netzspezifische Sicherheitselemente. In Abbildung fünfzehn ist beispielhaft im Überblick zu sehen, welche kryptographischen Algorithmen in welche der unten dargestellten kryptographischen Anwendungen eingeflossen sind. Auf Hardware-Sicherheitskomponenten wird nur sehr knapp eingegangen, da die Produkte den gleichnamigen angesprochenen Technologien auch weitgehend entsprechen.

Abbildung 15: Kryptographische Algorithmen und Anwendungen



Quelle: Entworfen und gez.: Verfasser

5.1.1 Kerberos

Kerberos ist ein Authentikations-System, das im Rahmen des Projektes Athena am MIT entwickelt und 1988 vorgestellt wurde. In offenen Informationsnetzen ist es möglich, daß sich jeder, der bestimmte technische Anforderungen erfüllt, an das System anschließen kann. Dadurch ist es erforderlich, daß sich ein Server von der Authentizität des Benutzers (Client) überzeugt, bevor er Zugangsrechte prüft und letztendlich evtl. freigibt. Um die Authentikation durchzuführen, nutzt Kerberos einen Authentikations-Server, der von allen als „Trusted Third Party“ angesehen wird. Zusätzliche Zeitstempel sollen die Entdeckung von Wiederholungsangriffen ermöglichen. Kerberos verfügt über eine Datenbank mit seinen Clients und deren Private-Keys, die jeweils nur Kerberos und dem Client bekannt sind. Falls der Client ein Anwender ist, handelt es sich bei dem Private-Key um ein verschlüsseltes Paßwort. Die weit verbreitete Version 4 nutzt den DES-Algorithmus im CBC-Mode, die neuere Version 5 ermöglicht den Einsatz jeglichen symmetrischen Verschlüsselungsverfahrens.[2]

Kerberos generiert Nachrichten, mit denen es den Clients möglich ist, sich gegenseitig zu authentisieren und generiert Session-Keys, die an Client und Server übergeben werden, die

---

[1] Die Produkte sind zufällig anhand des Literaturangebotes ausgewählt worden – es gibt natürlich auch Geräte anderer Hersteller. Die E-Cash-Anwendung soll hier auch als „Produkt“ gesehen werden.

[2] Vgl. Reif, Holger: Netz ohne Angst. Sicherheitsrisiken im Internet, in: c’t Magazin für Computertechnik, Jg. 1995, Heft 9, S.174 - 183, hier S. 175.

miteinander vertraulich kommunizieren wollen. Dadurch werden drei Sicherheitsdienste geboten, die in der Anwendungsschicht realisiert sind:[1]

- Authentikation der Kommunikationspartner bei Verbindungsaufbau.
- Authentikation der Nachrichten innerhalb einer Session.
- Vertraulichkeit von Nachrichten.

Damit der Nutzer sich nicht ständig beim Authentikations-Server identifizieren muß, erhält er ein Ticket (Ur-Ticket) für einen sog. *Ticket Granting Server* (TGS), der danach die weiteren Tickets erteilt. Auch diese werden durch eine Verschlüsselung mit einem Private-Key erstellt. Die Tickets enthalten den Namen des Servers, den Namen des Clients, die Internet- oder Rechneradresse, einen TVP, die Gültigkeitsdauer des Tickets und einen zufälligen Session-Key. Das Ticket kann während der Gültigkeitdauer mehrfach verwendet werden, die Authentikatoren dagegen nur einmal. Letztere enthalten den Clientnamen, die Clientadresse und einen TVP, sie sind mit dem im Ticket vereinbarten Session-Key verschlüsselt.[2]

5.1.2 X.509

Der Verzeichnisprüfungsdienst X.509 ist ein Standard der CCITT (=Comité Consultatif International Télégraphique et Téléphonique), Bestandteil der Reihe X.500 und aktuell in einer 1993 überarbeiteten Empfehlung. Das Verzeichnis ist in Wirklichkeit ein Server oder eine verteilte Gruppe von Servern, die eine Informations-Datenbank über Anwender verwalten, und es kann als Aufbewahrungsort für Zertifikate von Public-Keys, wie in Abschnitt 3.1.5.3 beschrieben, dienen. Jedes Zertifikat enthält den Public-Key eines Anwenders und ist mit dem Private-Key einer vertrauten Zertifikations-Autorität versehen. Es wird in X.509 genau beschrieben, wie die Zertifikate zu erstellen und über Zertifikatspfade zu liefern sind. Zusätzlich sind weitere Dienste wie z.B. Schlüssel-Management und digitale Signaturen beschrieben. Es kann somit eine Authentikation des Kommunikationspartners durchgeführt , Datenunversehrtheit nachgewiesen und ein Urheber- / Empfängernachweis erstellt werden.

---

1 Vgl. Ruland, Christoph, Info.sicherheit, a.a.O., S. 261.

2 Vgl. Pohlmann, N.: Sicherheit in UNIX-Netzen, in: Datacom, 10. Jg. (1993), Heft 12, S. 122 - 129, hier S. 124.

X.509 basiert auf dem Gebrauch der Kryptographie von Public-Keys und digitaler Signatur. Der Standard schreibt nicht die Verwendung eines bestimmten Algorithmus vor, empfiehlt aber RSA. Zusätzlich wird eine Hash-Funktion benötigt, die unbestimmt ist.[1]

5.1.3 E-Mail-Sicherheitskomponenten

Die elektronische Mail ist im wesentlichen bei allen installierten Rechnerumgebungen die meistbenutzte Netzwerkanwendung – vor allem in Internetzwerk- und Groupwareumgebungen wie z.B. Lotus Notes. Sie ist zudem gleichfalls die einzige verteilte Anwendung, die weitgehend über alle Architekturen und Herstellerplattformen verwendet wird. Zudem wird durch das explosionsartige Wachstum des Internet das E-Mail-Auf-kommen bei persönlichen Nachrichten und „Usenet News“ quasi täglich größer und beginnt Anteile des normalen Brief-, Telefax- und Telefonverkehrs zu übernehmen. Fast alle Mailsysteme, ob sie nun das Simple Mail Transfer Protocol (SMTP) oder X.400 (ISO-Norm für elektronische Post) verwenden, arbeiten nach dem Store-and-Forward-Prinzip, das mit der Verbindungsverschlüsselung (ohne Verschlüsselung) vergleichbar ist. Auf den Knotenrechnern kann jeder Administrator (oder Angreifer) die E-Mail problemlos lesen – oder manipulieren.[2] Um dieses zu verhindern und E-Mail auch im Internet sicher zu machen, sind zwei Programme entwickelt worden, die sich derzeit rasend schnell verbreiten und nachfolgend erläutert werden sollen. Es handelt sich dabei um Programme, die hybride Verschlüsselung auf der Anwendungsschicht nutzen.

5.1.3.1 Pretty Good Privacy (PGP)

PGP ist ein bemerkenswertes Programm, das schon fast einem Phänomen gleichkommt. Es wurde weitgehend von einer einzelnen Person, dem Amerikaner Phil Zimmermann, entwikkelt und ist als Public-Domain-Software für nicht-kommerzielle Nutzung erhältlich, was eine rasende Ausbreitung im Internet auslöste. Das Programm wird als Paket mit ausführlicher Dokumentation und dem C-Quellcode angeboten, was zudem eine Ausbreitung auf verschiedenste Rechnerplattformen ermöglichte. Durch die Verbreitung im Ausland handelte sich der Programmautor großen Ärger mit Regierungsvertretern und ein bis heute

---

[1] Vgl. Klein, Stefan / Weller, Stefan: EDI ? Aber sicher, in: KES, 9. Jg. (1993), Heft 2, S. 52 - 60, hier S. 56ff..

[2] Vgl. Fuhrberg, Kai: Gefährdungen bei der Benutzung des Internets, in: BSI-Forum, 3. Jg. (1995), Heft 6, S. 41 - 45, hier S. 42; **ebenso** Kauffels, F.-J.: Netzsicherheit, in: Datacom, 10. Jg. (1993), Heft 1, S. 96 - 103, hier S. 100.

andauerndes staatliches Ermittlungsverfahren ein.[1] Um eine legale internationale Nutzung zu ermöglichen, hat der Norweger Staale Schuhmacher eine eigene überarbeitete PGP-Version[2] herausgebracht, die nur legale Komponenten (Implementa-tionen von RSA (speziell Version RSAREF), die außerhalb der USA erstellt werden, fallen nicht unter die US-Exportbestimmungen) enthält. Diese Version (2.6.2i , i = international) ist sogar fehlerfreier und vorteilhafter als das aktuelle Original 2.6.2 von Phil Zimmermann. Eine kommerzielle Version wird von der Firma Viacrypt vertrieben.

PGP basiert auf bereits im dritten Abschnitt erläuterten Algorithmen – dies sind RSA für die Erstellung des Public-Key und digitale Signaturen, IDEA für die Verschlüsselung von Nachrichten und MD5 für Hash-Codierung (digitale Signaturen). In Abb. 16 ist ein exemplarischer Public-Key von PGP abgebildet. Den Keys werden E-Mail-Adressen zugewiesen (mehrere pro Key möglich), so daß bei einem Serverwechsel auch ein überarbeiteter Key „verteilt“ werden muß. Die Schlüsselgrößen können von 384-Bit bis zu

Abbildung 16: 512-Bit PGP 2.6.2i Public-Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2i

mQBNAjB02Q4AAAECAK1O7o1h5OhWYEStQlkor3tYqAqWTA4kKmYkAVroDuFZiFx+
zPS1QrwcDX2IZ+51ZK1cDJpUtO+J/hs5reQE5LUABRG0GzxTLlZPTFFVQVJUWkBI
RFMuU0hORVQuT1JHPrQtU29lbmtlIFZvbHF1YXJ0eiA8Uy5WT0xRVUFSVFpAUE9F
VC5TSE5FVC5PUkc+tCE8Uy5WT0xRVUFSVFpASC1TLVAuREJOLkRJTkVULkNPTT4= =HH0r
-----END PGP PUBLIC KEY BLOCK-----
```

Quelle: Verfasser – Public-Key für die E-Mail-Master-Adresse: S.Volquartz@HDS.shnet.org

2048-Bit eingestellt werden. Zudem werden Session-Keys pro Nachricht von IDEA verwendet, die 128-Bit groß sind. Die digitalen Signaturen sind mit einer Zeitmarke versehen. Es ist kein Zertifizierungssystem für Authentikationsserver vorgesehen, die einzelnen Schlüssel können jedoch von anderen „vertrauenswürdigen“ PGP-Nutzern signiert werden (die Signatur gibt der Anwender frei, womit er darüber entscheiden kann, wann ein Partner vertrauenswürdig ist). Die Authentikation der Schlüssel kann (z.B. über Telefon) mit Hilfe eines 128-Bit langen MD5-Musters des Schlüssels im Radix-64-Format, dem sog. Fingerabdruck des Schlüssels (`3D 7F A9 84 1F 96 9D 33  3C 31 3A 22 75 09 68 8B` passend zu dem Key aus Abb. 16), geschehen. Mit diesen Funktionen leistet PGP:[3]

- Integrität der Nachricht.

---

[1] Vgl. Fox, Dirk: Schlüsseldienst. Private Kommunikation mit PEM und PGP, in: c’t Magazin für Computertechnik, Jg. 1995, Heft 9, S.184 - 187, hier S. .

[2] Die aktuelle Version kann immer unter URL=http://www.ifi.uio.no/ staalesc/PGP/home.html legal bezogen werden.

[3] Vgl. Litterio, Francis: Cryptography, PGP, and Your Privacy, URL=http://world.std.com/~franl/crypto.html: 17.11.1996

- Urhebernachweis.
- Vertraulichkeit der Nachricht.
- Authentikation des Absenders.

In das PGP-Programmpaket ist auch eine komfortable Schlüsselverwaltung integriert, die auch Unterschriftszertifikate automatisch über eine sog. „Ownertrust“-Funktion verwaltet und innerhalb des „Schlüsselbundes“ auf logische Konsistenz überprüft.

5.1.3.2 Privacy Enhanced Mail (PEM)

PEM ist ein Internet-Standard, der ebenfalls sicherheitsbezogene Dienste für Anwendungen der elektronischen Mail bietet. Seine verbreitetste Verwendung findet er in Verbindung mit dem Internet-Standard SMTP, er kann jedoch auf jedes Schema von E-Mail angewandt werden, einschließlich X.400. Auch PEM ist für verschiedene Plattformen erhältlich, wenn auch nicht in dem Umfang wie PGP. Es bietet die gleichen Sicherheitsdienste wie PGP. PEM hat seinen Ursprung in den Aktivitäten der Privacy and Security Research Group unter der Schirmherrschaft des Internet Architecture Boards (IAB), seine aktuelle Fassung erschien im Februar 1993 und sein Konzept und die Funktionen sind in den Internet Request for Comments RFC 1421 - 1424 standardisiert worden.[1]

Besondere Funktionen bei PEM sind die Unterstützung von Mailing-Listen und ein auf einer Zertifikatshierarchie basierender Schlüsselverwaltungsdienst, der der Architektur des oben beschriebenen X.509 entspricht. PEM spezifiziert zwei Nachrichtentypen: integritätsgeschützte, authentische Nachrichten (Typ MIC = Message Integrity Check) und solche mit zusätzlich verschlüsseltem Nachrichteninhalt (Typ ENCRYPTED). Die Berechnung und das Anhängen eines MIC sichert Datenintegrität und -authentizität (ent-spricht digitaler Signatur). Dabei wird zwischen MIC-CLEAR- und MIC-ONLY-Nachrichten unterschieden. Bei letzteren verhindert eine abschließende 6-Bit-Transportverschlüsselung, daß bei der Übertragung Umcodierungen des Nachrichteninhalts durch Mail-Gateways erfolgen, die Integritätsverletzungen verursachen könnten. MIC-CLEAR-Mails ermöglichen Kommunikationspartnern, die nicht über PEM zur Umkehrung der Transportverschlüsselung verfügen, das Lesen von MIC-geschützten Nachrichten. Die Nachrichten vom Typ ENCRYPTED mit verschlüsselten Nutzdaten werden grundsätzlich transportverschlüsselt. Zur Nachrichtenverschlüsselung wird mit DES im CBC-Mode ein Session- (hier Interchange-) Key verwendet, aber es sind auch andere symmetrische Algorithmen mit einer Block-

---

[1] Vgl. Horster, P. / Portz, M.: Privacy Enhanced Mail: Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet, in: DuD , Jg. 1994, Heft 8, S. 434 - 442, hier S. .

länge von 64-Bit möglich. Für die digitale Signatur wird RSA mit der MD5-Hash-Funktion genutzt. Zertifikate für Public-Keys werden mit MD2 erzeugt und mit RSA wird der Hash-Code verschlüsselt. Die Schlüsselgröße kann zwischen 512 und 1024-Bit variieren. Die MD-Hash-Codes weisen eine Länge von 128-Bit auf und werden in zwei 64-Bit Blöcken DES-ECB verschlüsselt, um dann die 128-Bit lange Verschlüsselung von MIC zu bilden.[1]
PEM unterliegt den US-Exportbestimmungen und ist somit in den Implementierungsformen TIS/PEM (PEM der Firma Trusted Information Systems) und RIPEM (Riordan's Internet PEM) nicht in Deutschland erhältlich. Das einzige in Deutschland erhältliche PEM-Derivat ist integriert in das von der Gesellschaft für Mathematik und Datenverarbeitung entwickelte Programmpaket SecuDE (SecuDE-PEM) und hat weitgehend vollständige Funktionalität – ist jedoch nur für UNIX-Systeme erhältlich.

5.1.4 Simple Network Management Protocol (SNMP)

Die Weitläufigkeit eines WAN oder Internetzwerkes kann nicht allein durch menschliche Anstrengungen aufgebaut und verwaltet werden, sondern es bedarf automatisierter Verwaltungswerkzeuge. Je heterogener die Netzausstattung, desto nötiger sind Werkzeuge dieser Art. Als Antwort auf diesen Bedarf wurden Standards entwickelt, die sich mit Netzwerkverwaltung, Protokollen und Schutzdiensten befassen, wobei der am häufigsten verwendete Standard der des Simple Network Management Protocol (SNMP) ist. Dem steigenden Wunsch nach umfangreicheren Sicherheitsmechanismen wurde mit der Version 2 von SNMP im Jahre 1993 Rechnung getragen. SNMP wurde als Teil der TCP/IP-Protokollreihe auf der Anwendungsschicht entwickelt und stellt eine Netzwerkverwaltung mit Sicherheitserweiterungen dar, die die einzelnen Verwaltungspunkte (Verwaltungs-Rechner der einzelnen Operatoren und Verwaltungsagenten wie Hosts, Bridges, Router und Hubs) des Netzwerkes als Protokoll verbindet. Speziell die Version 2 soll jedoch auch auf die OSI-Protokollreihe aufsetzen. Gerade diese Punkte im Netz sind besonders Angriffen ausgesetzt. [2]
Die Sicherheitseinrichtungen von SNMPv2 werden in den RFC 1445 - 1447 beschrieben und die Sicherheitsfähigkeiten sind so ausgelegt, daß ein Datenaustausch der „Netzverwalter" unter SNMPv2 gegen die Bedrohungen Abhören, Maskerade, Datenmanipulation, sowie Verzögerung und Wiederholung gesichert ist. Nur die Verkehrsflußanalyse

---

[1] Vgl. Jacobson, Gunnar, a.a.O., S. 54f.
[2] Vgl. Borowka, Petra: Sicherheit durch Netzwerkmanagement, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '93, Hrsg.: Lippold, Heiko / Schmitz, Paul u.a., Braunschweig 1992, S. 137 - 170, hier S. 141ff.

und die Verweigerung können nicht unterbunden werden. Es werden Vertraulichkeit, Erkennung von Datenunversehrtheit und Zugriffskontrolle als Sicherheitsdienste angeboten. Der spezifische Mechanismus zur Vertraulichkeit, der für SNMPv2 gewählt wurde, ist DES-Verschlüsselung. Die Datenunversehrtheit wird mit Hash-Codes unter Anwendung von MD5 mit Verwendung eines speziellen Zeitstempels realisiert, wozu eine Synchronisation der Uhren der beteiligten Verwalterparteien angeboten wird. Die Zugriffskontrolle wird über Zugriffskontrolltabellen abgewickelt, nachdem die verschlüsselten Anforderungen mit dem Private-Key entschlüsselt (Authentikation) und auf den Hash-Code überprüft (Integrität) wurden.[1]

5.1.5 Spezielle Internet-Sicherheitskomponenten

Der große Durchbruch des Internet kam mit dem World Wide Web, dessen auffälligste Merkmale die Verweise auf anderen Web-Seiten, die Einbindungsstandards für Grafiken, Fotos, Videos und Sounds sowie die leichte Bedienbarkeit per Computer-Mouse sind. Die einzelnen Seiten werden in dem einheitlichen HTML-Format auf den einzelnen Server in der Welt abgelegt, auf die der Nutzer mit Hilfe eines Browsers zugreifen kann. Seit 1994 bieten auch zunehmend kommerzielle Dienste „kostengünstig“ Anbindungsmöglichkeiten an das Internet / WWW an, so daß es jedermann möglich ist, zum günstigen Ortstarif Kontakt mit jedem im Internet angebundenen Rechner auf der Welt aufzunehmen. Dieser Markt und die Fähigkeiten des WWW wurden natürlich auch von der Wirtschaft entdeckt, denn hierüber lassen sich Verkaufsangebote wahrlich multimedial an den potentiellen Käufer bringen. Wer sich jedoch am Online-Business als Anbieter beteiligt, muß den Zugriff auf seinen (evtl. firmeninteren) WWW-Server selbstredend für jeden potentiellen Kunden freischalten oder für einen bestehenden Kundenstamm via Paßwortvergabe den Nutzerkreis von vornherein einschränken, um Supportangebote etc. anzubieten. Zudem soll bei einer Produktorder natürlich Vertraulichkeit gewahrt und eine Rechtsverbindlichkeit gegeben sein. All dies ist mit dem Hypertext Transfer Protocol (HTTP) in dieser Form nicht machbar – daher sollen nun zwei Verfahren angesprochen werden, mit denen es möglich ist, daß WWW-Client, WWW-Proxy und WWW-Server mit signierten und / oder verschlüsselten Requests / Responses untereinander arbeiten können.[2]

---

[1] Vgl. Stallings, William, Datennetz, a.a.O., S. 526ff.

[2] Vgl. Abel, Horst / Schoberth, Andreas: Effektive und sichere Nutzung von Internet-Diensten, in: KES, 12. Jg. (1996), Heft 4, S. 32 - 36, hier S. 34; **ebenso** Ermer, Dieter: Grundsätze für Benutzerrichtlinien für das Internet, in: KES, 12. Jg. (1996), Heft 4, S. 37 - 42, hier S. 38f.

5.1.5.1 SSL

Das Protokoll SSL steht für *Secure Socket Layer* und wurde von der Firma Netscape Communications Corporation entwickelt. Es ist nicht nur für HTTP vorgesehen, sondern kann jedes Transportprotokoll um ein Konzept für einen „sicheren Kanal“ erweitern. Dazu setzt SSL auf die Socket-Schnittstelle auf (grob zwischen Transport- und Anwendungsschicht), den Standard für den Zugriff auf TCP unter Windows und UNIX, und ersetzt sie durch eine um Sicherheitseigenschaften erweiterte Version (sichere virtuelle Verbindung auf einer unsicheren TCP/IP-Verbindung). Damit stehen die neuen Sicherheitsmerkmale auch FTP, Telnet etc. zur Verfügung, welche im einzelnen Authentikation von Client und Server, Datenunversehrtheit und Vertraulichkeit sind – die darüber arbeitenden Anwendungen bekommen nichts davon mit.[1] Es werden in großem Umfang kryptographische Verfahren aus Abschnitt drei verwendet. Es wird auf Challenge/Response-Ebene eine Two Pass Parallel Authentikation eingesetzt. Zertifikatsprüfung ist im X.509-Format zulässig. Bei der Abarbeitung dieses Handshake-Protokolls wird neben der Authentikation auch der Session-Key ausgetauscht, sofern bereits eine frühere Sitzung stattfand. Ansonsten wird mit dem Diffie-Hellman-Verfahren ein Master-Key generiert und ausgetauscht, aus dem mit MD5-Hash-Codes RSA-verschlüsselte Session-Keys abgeleitet werden. Datenverschlüsselung wird im Rahmen eines Record-Protokolls mit RC4 (oder IDEA in neueren Beta-Tests der internationalen Version) vorgenommen und mit MAC’s zur Gewährleistung der Dateninteграität versehen.[2]

Das SSL-Protokoll stellt eine sehr einfache und effiziente Sicherheitskomponente zur Befriedigung der Sicherheitsbelange vieler Anwendungsprotokolle dar und ist in der Version 3.0 kryptoanalytisch auch sehr sicher. Probleme gibt es erneut mit den US-Exportbeschränkungen, die derzeit eine internationale Version mit geringerer Sicherheit erfordern. SSL ist sehr weit verbreitet, da es in dem meistgenutzten Web-Browser, dem Netscape Navigator, implementiert ist.

5.1.5.2 S-HTTP

Einen zu SSL alternativen Ansatz bietet Secure-HTTP, das auf der Anwendungsebene realisiert ist. Es ist Ergebnis eines Joint-Ventures zwischen RSA Data Security und EIT (= Enterprise Integration Technologies), das Mechanismen für die kommerzielle Nutzung des

---

[1] Vgl. Klute, Rainer: Verschlußsache - Sicherheit im WWW, in: iX Multiuser, Multitasking Magazin, Jg. 1995, Heft 12, S. 132 - 145, hier 142f.

[2] Vgl. Freier, A. O./ Karlton, P.: The SSL Protocol Version 3.0, Netscape Communications, (Expires 9/96), URL=http://www.uni-siegen.de/security/internet/ssl.draft-freier-ssl-version3-01.txt: 19.01.1997

WWW entwickelt. S-HTTP nimmt nicht nur am Transferprotokoll Erweiterungen vor, sondern definiert auch neue Elemente für die HTML-Sprache. Es stellt einen Rahmen für die Anwendung verschiedener kryptographischer Sicherheitskomponenten dar, wobei zu den Funktionen von SSL hier noch die digitale Signatur hinzukommt. Die Nachrichten werden zwischen einer Beginn- und Ende-Zeile gekapselt. Als Formate für die gekapselten Nachrichten werden die Standards PGP, PEM und PKCS#7 (PEM-ähnlich von RSA Data Security) unterstützt. Der eigentlichen gekapselten Nachricht werden Kopfzeilen vorangestellt, die die gewählten Erweiterungen und ihre Einstellungen gegenüber HTTP angeben (s. Abb. 17), auf die sich Client und Server einigen. Diese Einstellungen können Nachrichtenformate, Zertifikatstypen, Schlüsselaustauschmechanismen, digitale Signierverfahren, Hash-Algorithmen und Verschlüsselungsverfahren sein. Die Liste der unterstützten Verfahren ist fast lückenlos. Folgende Verfahren sind voreingestellt – Verschlüsselung mit DES im CBC-Mode und RC4, Zertifikate nach X.509-Standard, digitale Signaturen mit RSA / MD5 / TVP und Austausch des Session-Keys mit Kerberos-Tickets (oder als normaler RSA-Public-Key oder sogar als Schlüsseltausch über Briefpost / Telefax). Durch den Zeitstempel des TVP sind hier Wiederholungs-Angriffe unmöglich. Im Gegensatz zu SSL, wo sich alles im Hintergrund ab-

Abbildung 17: S-HTTP-Nachricht an einen Server

```
============================================================
Secure * Secure-HTTP/1.1
Content-Transfer-Encoding: base64
Content-Type: application/http
MAC-Info:2ffc120b,rsa-md5,1425a951f1bbf3bd8d6dc7d07ab731bb,inband:alice1
Content-Privacy-Domain: PKCS-7

-----BEGIN PRIVACY-ENHANCED MESSAGE-----
MIAGCSqGSIb3DQEHAYBjR0VUIC9wcml6ZS5odG1sIEhUVFAvMS4wClNlY3VyaXR5
LVNjaGVtZTogUy1IVFRQLzEuMQpVc2VyLUFnZW50OiBXZWItTy1WaXNpb24gMS4x
YmV0YQpBY2NlcHQ6ICouKgoKAAA=
-----END PRIVACY-ENHANCED MESSAGE-----
============================================================
```

Quelle: Schiffman, A. / Rescorla, E.: The Secure HyperText Transfer Protocol, EIT, S. 34, URL=http://www. uni-siegen.de/security/internet/shttp.draft-ietf-wts-shttp-00.txt: 19.01.1997

spielt, ist bei S-HTTP mit Hilfe von Icons alles für den Benutzer im Browser sichtbar (z.B. Siegel auf dem Bildschirm, wenn eine Nachricht signiert ist). Auch hier wird eine Two Pass Parallel Authentikation als initiales Handshake genutzt.[1]

SSL liegt derzeit aufgrund größerer Verbreitung am Markt vorn, S-HTTP ist aber vielfältiger von den Anwendungsmöglichkeiten, da die Krypto-Verfahren auf der Anwendungsschicht liegen und damit dem Benutzer – Informationsanbieter wie -kunden – zugänglich

[1] Vgl. Schiffman, A. / Rescorla, E.: The Secure HyperText Transfer Protocol, EIT, (Expires Jan-96), S. 4ff, URL=http://www.uni-siegen.de/security/internet/shttp.draft-ietf-wts-shttp-00.txt: 19.01.1997

sind. Hier lassen sich auch die Vorteile der digitalen Signatur, wie z.B. Vertragsschluß oder die Veröffentlichung verbindlicher Mitteilungen, nutzen. Es gehen bereits Bemühungen dahin, SSL und S-HTTP zusammenzuführen.[1]

5.1.6 Sicherheit im ISDN / X.25-Netz

ISDN besitzt, wie z.B. auch X.25-Netze, einige einfache Sicherheitseigenschaften. Dies sind Teilnehmererkennung, Anschlußerkennung und die Übernahme gewisser Benutzerangaben beim Verbindungsaufbau. Es handelt sich dabei in beiden Netztypen jedoch um einfache Authentikationsverfahren, die dem Anspruch als vollwertiger Sicherheitsdienst nicht gerecht werden.

Dazu gibt es in der ISO den Standardisierungsvorschlag des „*Network Layer Security Protocols*“ (NLSP), das die Sicherheitsdienste der ISO-Security Architecture anbieten soll. Es wird dazu nicht versucht, bestehende Vermittlungsprotokolle zu modifizieren oder zu erweitern, sondern einen *Sublayer* eingeführt, der ein eigenes Protokoll oberhalb der Vermittlungsschicht und unterhalb der Transportschicht ausführt. Das hat den Vorteil, daß der Sublayer unabhängig von dem verwendeten Vermittlungsprotokoll ist – er gilt also für leitungsvermittelnde Netze ebenso wie für paketvermittelnde Netze oder Standleitungen. Die Dienstelemente des NLSP werden mit Hilfe von MAC’s, digitalen Signaturen, Authentikationsmechanismen, dem Dehnen vom Daten – kurz, weitgehend allen im Abschnitt 3.1 genannten Verfahrenstypen realisiert. Gewisse leitungsorientierte Funktionen werden auch auf den Vermittlungsknoten im Netzwerk angeboten, um mit Hilfe des NLSP Ende-zu-Ende-Sicherheitsdienste nutzen zu können.[2]

Bei *X.25-Netzen* werden Realisierungen des ISO-Standardisierungsvorschlags als Produkte mehrerer Hersteller angeboten, wobei es sich um Security-Black-Box-Lösungen handelt. Eine solche Lösung kommt auch in Abschnitt 5.2.2 vor, so daß hier nicht näher darauf eingegangen wird.

Auch im *ISDN* gibt es Realisierungen als Security-Black-Box-Lösungen (s. Abschnitt 5.2.1), allerdings sprechen hier auch viele Gründe gegen eine solche Lösung, wie z.B. hoher Aufwand für die teilnehmer- und netzseitige Realisierung des D-Kanal-Protokolls[3], verschiedenartige Konfigurationsmöglichkeiten der S_0-Schnittstelle (die ohnehin nicht stabil

---

1 Zudem hat Microsoft gerade ein Private Communication Technology Protocol (PCT) veröffentlicht.

2 Vgl. Ruland, Christoph, Info.sicherheit, a.a.O., S. 203ff.

3 Im ISDN muß zwischen dem D-Kanal für Verbindungsaufbau und Verbindungssteuerung auf Basis der Paketvermittlungssteuerung und den B-Kanälen für die Nutzdatenübertragung unterschieden werden.

ist und durch Euro-ISDN abgelöst wird) und zudem eine weite Verbreitung des U_{p0}-Schnittstellentyps bei Anschlüssen an Nebenstellenanlagen.

Für eine im Endsystem integrierte Lösung spricht die Unabhängigkeit vom D-Kanal, die Kostengünstigkeit und ein von den Herstellern als Standard verabschiedetes CAPI (= Common Application Programming Interface).

Aus Sicht des OSI-Modells liegt das CAPI oberhalb der dritten Schicht, d.h. es bietet darüberliegenden ISDN-Anwendungen transparente Ende-zu-Ende-Verbindungen auf einem B-Kanal. Das NLSP wird so auf das CAPI gesetzt, daß nach wie vor alle Meldungen der CAPI unverändert sind und weder Anwender noch CAPI merken, daß ein Security sublayer integriert wird. Die Kombination wird auch als Security-CAPI (S-CAPI) bezeichnet. Zur Steuerung ist wie bei Black-Boxes ein Sicherheitsmanagement erforderlich und die Private-Keys können optional auf Chipkarten eingebracht werden. Dies hat den weiteren Vorteil gegenüber der Black-Box-Lösung, daß sich die Authentikation nicht nur auf den ISDN-Anschluß, sondern auf eine bestimmte Person – den mittels PIN identifizierten Chipkartenbesitzer – bezieht.

S-CAPI arbeitet mit einer Schlüsselhierarchie, wobei RSA für den Public-Key zuständig ist. Für die Nutzdatenverschlüsselung kommen DES und IDEA und für digitale Signaturen El Gamal und DSS, für die Benutzerauthentikation kommt ein Two Pass Parallel Verfahren und für Keymanagement und Zertifikatsprüfung X.509 zum Einsatz.[1]

Künftig wird man im Rahmen von Videoconferencing und Bildtelefonen aufgrund der hohen Datendichten optimiertere Versionen entwickeln müssen.

5.1.7 E-Cash

Unter Electronic Cash sollen hier hier im Rahmen einer sehr kurzen Behandlung die Elektronische Geldbörse auf ICC's als Debitsystem, POS-Banking (= Point-of-Sale) als Kreditsystem und „am Rande" die neue Form des Internet-Banking verstanden werden – auf Cybercash wird nicht eingegangen.

Die *elektronische Geldbörse* wird in Deutschland 1997 flächendeckend durch ICC-Eurochequekarten realisiert (EC-Karten waren bisher reine Magnetstreifenkarten). Der Chipspeicher kann bis zu einer bestimmten Summe an einer Ladestation mit PIN-

---

[1] Vgl. Dienst, Detlef / Fox, Dirk: Transparente Sicherheitsmechanismen für ISDN-Anwendungen, in: Informationstechnische Gesellschaft im VDE (ITG) Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 09-10.11.1994 , ITG Fachbericht 131, Hrsg.: ITG, Berlin 1994, S. 81 - 95, hier 88ff; **ebenso** Rudeloff, Roger: IT-Sicherheitsfunktionen im ISDN, in: BSI-Forum, 2. Jg. (1994), Heft 3, S. 53 - 55, hier S. 54f.

Überprüfung aufgeladen werden, die dann über Lesegeräte an den Kassen in den Geschäften ohne erneute PIN-Überprüfung (aus Gründen des zügigeren Bezahlens) abgebucht werden kann. Beim Ladevorgang wird nach PIN-Eingabe mittels einer Two Pass Parallel Authentikation der Benutzer über einen Authentikations-Server authentisiert und dann eine bestimmte Summe auf die ICC gebucht. Wichtig bei diesem System ist, daß Anonymität und Unverfolgbarkeit der Zahlungen und damit des Anwenders gewahrt bleiben. Es muß also mit Session-Keys während der Bezahlung gearbeitet werden, die nicht auf den Kartenbesitzer schließen lassen, aber gleichzeitig die Geldsumme authentisieren. Dazu werden temporäre Schlüssel aus einer Schlüsselhierarchie eines asymmetrischen Verfahrens zugewiesen, die dann sog. „Blind Signatures“ erstellen. Es gibt derzeit sowohl Kassen-Abbuch-Systeme, die offline arbeiten als auch Systeme für den Online-Betrieb.[1]

Beim POS-Banking beginnt das elektronische Bezahlen mit der Entscheidung des Kunden, den angezeigten Betrag zu bestätigen, seine EC-Karte in das POS-Terminal zu stecken und nach Aufforderung seine PIN einzugeben. Danach wird die Transaktion an einen Netzknoten geschickt, wo anhand der Magnetstreifendaten die Transaktionsdaten zu den Autorisierungszentralen der Geldinstitute weitergeleitet werden. Im POS-Terminal werden die Transaktionsdaten und die PIN kryptisch gegen Verfälschung und Ausspähung gesichert. In der Autorisierungszentrale wird die Nachricht auf Integität geprüft und der Kunde dann mittels der PIN und der Kartendaten authentisiert. Die Prüfungen laufen innerhalb physikalisch angriffsgeschützter Sicherheitsmodule ab. Nach erfolgter Authentikation wird die Transaktion an das kontoführende Geldinstitut weitergeleitet, wo der gewünschte Geldbetrag am persönlichen Verfügungsrahmen des Kundenkontos autorisiert wird. Der Kunde erhält die Bestätigung der Zahlung und den Kassenbon, auf dem der Vorgang mit speziellen Informationen wie Transaktionsnummer, Kartennummer, Kontonummer und temporärer Autorisierungs-ID festgehalten ist. Bei diesen Vorgängen werden symmetrische Verfahren wie DES und für die Beweisbarkeit MAC’s genutzt. Die Schlüssel werden in Hierarchien über ein Control-Vector-Conzept vergeben und verwaltet.[1]

Beim *Internet-Banking* (nicht zu verwechseln mit Online-Banking über Mailboxen der Geldinstitute) wird auf WWW-Ebene über das Internet die jeweilige Transaktion an das Geldinstitut weitergeleitet. Dies soll am Beispiel der „Bank 24“ dargestellt werden. Bank und Internet sind über Firewalls getrennt, die von zwei Prüfungsgesellschaften testiert wur-

---

[1] Vgl. Janson, Phil / Waidner, Michael: Electronic Payment Systems, in: DuD, Jg. 1996, Heft 6, S. 350 - 359, hier S. 352f; **ebenso** Chaum, David: Prepaid Smart Card Techniques, Digicash, URL= http://www.digicash.com/publish/sciam.html: 09.02.1997

den. Es wird ein X*PRESSO Security Package genutzt, das in JAVA programmiert ist und eine 128-Bit Verschlüsselung präsentiert. Die Identifizierung der Bank beim Login vollzieht sich automatisch, wobei ein Schlüsselpaar zum Einsatz kommt, das von einer anerkannten „Trusted Third Party“ zertifiziert wurde. Damit soll der Bankkunde die Gewähr haben, daß am anderen Ende wirklich die Bank 24 ist. Es wird IDEA mit 128-Bit Schlüssellänge und RSA mit 1024-Bit Schlüssellänge verwendet. Geschützt sind diese durch digitale Signaturen, die vor und nach der Übertragung gebildet werden.[2] Abschließend gibt nun der Kunde seine PIN und die Transaktionsnummer (TAN) ein, die auf seinem PC verschlüsselt werden, wozu die Secure Request Technology (SRT) zum Einsatz kommt. Hierbei handelt es sich um eine Umsetzung von Netscapes oben beschriebenem SSL, die freie mächtige Kryptoverfahren nutzt (keine US-Exportversionen) und zusätzlich auf eine bestehende SSL-Verbindung aufbaut (s.o.). Auf der SRT-Ebene gibt es zwei RSA-Session-Keys, von denen einer nur einmalig und der andere längerfristig zur Zertifizierung der Einmalschlüssel verwendet wird. Mit MD5 und SHA werden aus Zufallswerten der Session Hash-Codes gebildet, die zu einem Master-Secret zusammengefaßt werden, daß als Grundlage für den Einmal-Session-Key dient. In weiteren Schritten wird mit Hilfe von RSA-Verschlüsselung, RC4-Verschlüsselung und verschiedenen MAC’s und TVP’s der sichere Kanal aufgebaut und PIN und TAN verschlüsselt zur Authentikation übermittelt. Diese verläuft grob wie beim POS-Banking.[1]

5.2 Exemplarische Gesamt-Sicherheitskonzeptionen

Nach einigen dargestellten Sicherheitskomponenten soll in diesem Abschnitt nun die Verdichtung der Einzelkomponenten zu mächtigen Gesamt-Sicherheitskonzeptionen veranschaulicht werden. Dazu wird im ersten Unterabschnitt kurz gezeigt, daß man mittlerweile auch Gesamtkonzeptionen aus einer Hand erwerben kann und ein spezieller IT-Sicherheits-Dienstleistermarkt entsteht. In dem ersten Abschnitt soll jedoch nicht näher auf die Funktionen der Komponenten des Konzeptes eingegangen werden, da sie in Abschnitt drei ausführlich dargestellt wurden.

Anders im zweiten Unterabschnitt, der explizit auf den Funktionsablauf einer Gesamtkonzeption abgestellt wird und sich der Einsatz und die Funktionalität von Chipkarten, Kryptographie und Black-Boxes in praxi anschaulich erkennen läßt.

---

1 Vgl. Kiranas, Argiris, a.a.O., S. 415f.

2 Vgl. Birkelbach, Jörg: Safer Banking, in: c’t Magazin für Computertechnik, Jg. 1996, Heft 12, S.104 - 108, hier S. 105.

5.2.1 Telesec – ein Rundumangebot

Die Abkürzung Telesec steht für den Begriff „Telecommunication Security“ und ist ein spezielles Produktzentrum der Deutsche Telekom AG. Es werden in Zusammenarbeit mit den Hersteller und über Forschungsprojekte modular Hard- und Softwarepakete für kundenspezifische Sicherheitsdienstleistungen angeboten, die folgenden Grundprinzipien folgen:[2]

- „Alles aus einer Hand“-Prinzip für jeglichen IT-Bereich.
- Autarkie der Ende-zu-Ende-Kommunikation.
- normenkonforme Sicherheit nach dem technischen Stand.
- Rechtssicherheit.
- Berücksichtigung des Anonymitätsanspruches des Kunden.
- Transparenz der Produkte / bekannte kryptographische Methoden.
- Evaluierung aller Produkte.

Zudem kommt noch ein kompletter Security-Consulting-Bereich, der bei der Konzepterstellung hilft. In einem Sicherheitskonzept werden hier zunächst die individuellen Schutzziele definiert, nach Betrachtung des Systems kann eine Bedrohungsanalyse und Risikobewertung durchgeführt werden. Danach können mögliche Sicherheitsmaßnahmen beschrieben werden, inkl. einer Kostenabschätzung zu den jeweiligen Maßnahmen. Es werden weitgehend „standardisierte“ Lösungen mit geringem Anpassungsspielraum und individuelle Sicherheitskonzepte unter genauer Betrachtung des Systems angeboten.

Die Funktion einer sog. „Trusted Third Party“ übernimmt für die Schlüsselerzeugung der „NetKey Service“ (NKS) der Telesec. Das Trust-Center im NKS der Telesec beinhaltet alle für das Key Management notwendigen zentralen Funktionen einer TTP. Hierzu gehören insbesondere die Schlüsselerzeugung, Schlüsselbeglaubigung oder -zertifizierung, Ausgabe der Schlüssel (evtl. auf Chipkarten) an die Benutzer und Beglaubigung der Gültigkeitsdauer von Schlüsseln. Das Trust-Center der Telekom ist in einer physikalisch besonders gesicherten Umgebung realisiert und wird von speziell geschultem Personal betrieben.[3] Nachfolgend sollen nun verschiedene Produkte kurz vorgestellt werden, um

---

[1] Vgl. Luckhard, Norbert, a.a.O., S. 112f.

[2] Vgl. Wolfenstetter, Klaus-Dieter: TeleSec und Sicherheit in Telekommunikationssystemen, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’93, Hrsg.: Lippold, Heiko u. a., Braunschweig 1993, S. 445 - 462, hier S. 452.

[3] Vgl. Kowalski, B.: Telesec, in: Secure Information, Hrsg.: Eberspächer, J., Berlin u.a. 1994, S. 134 - 166, hier S.147f.

einen groben Überblick über das Angebot zu bieten:[1]

- **B1-Universelles Chipkartenlesegerät** – Im B1-Chipkartenterminal werden die verschiedensten ICC-Typen weitestgehend eigenständig erkannt, die entsprechenden Protokolle eingestellt und dem PC auf eine einheitliche Weise zur Verfügung gestellt. Es werden verschiedene Standardschnittstellen angeboten, wie z.B. V24/V28, PCMCIA, Centronix oder SCSI, und verschiedene Host-Anbindungen.
- **Security 1st** – ist ein umfangreiches Software- und Hardwarepaket, welches die Voraussetzungen für den ersten Einstieg in die Sicherheitswelt bietet.
- **TCOS-Telesec Chipcard Operating System** – ist ein Betriebssystem für ICC's, das auf verschiedenen Hardwareplattformen einsetzbar ist. Optional unterstützt TCOS Arithmetikprozessoren, die geeignet sind, modulare Rechenoperationen für Public-Key-Anwendungen durchzuführen. Unter Ausnutzung der Hardwareschutzmöglich-keiten bietet TCOS noch zusätzliche Softwareschutzmöglichkeiten. Die Daten werden von TCOS in einem Filesystem verwaltet. Zum Schutz der Daten bietet TCOS für jedes File verschiedene Zugriffsrechte und kryptographische Sicherheitsmechanismen. Weiterhin schützt TCOS die Daten und Informationen durch Überprüfung der Identität (PIN) und Authentizität mit Hilfe von Authentisierungsverfahren. Durch einen errechneten MAC überprüft TCOS die Authentizität der Daten und Befehle. Es kann Zufallszahlen und symmetrische Schlüssel (DES / 3DES) in verschiedenen Längen erzeugen und diese z.B. als Session Keys einsetzen. Unter Anwendung von asymmetrischen Kryptoalgorithmen (RSA) können mit TCOS digitale Signaturen erzeugt und Verschlüsselungen mit verschiedenen Schlüsseltypen durchgeführt werden.
- **Telesec Security Modul 95** (TSM95) – ist eine PCMCIA Steckkarte Typ II mit High-Level Security Funktionen. Das TSM95 erfüllt die Sicherheits- und Performanceanforderungen an Hardwarekomponenten, die in Telekommunikationsnetzen, z.B. mit den Protokollen ISDN, LAN (TCP/IP) und X.25 und Datenverarbeitungsendgeräten, z.B. PC´s mit entsprechender PCMCIA-Schnittstelle benötigt werden. Die hierzu notwendigen Security Funktionen beinhalten: Zugriffsschutz, symmetrische und asymmetrische Datenverschlüsselung, Datenintegrität, digitale Signaturen und verschiedene Authentikationsverfahren.

---

[1] Vgl. Telekom-Produktzentrum Telesec: Produktübersicht, Deutsche Telekom AG, Telesec, URL=http://www.telesec.de/produkte.htm: 17.11.1996

- **SecureFile** (SFile) – ist ein Softwarepaket, welches die Vorraussetzungen liefert, um Dateien/Files mit kryptographischen Sicherheitsmerkmalen zu versehen. Zudem ist die Erweiterung um Telesec-Hardwarekomponenten möglich (Kartenleser etc.).
- **DOKRYPT für Windows** – Das Softwarepaket ermöglicht Anwendungen den Zugriff auf Funktionen zur kryptographischen Bearbeitung von Daten. DOKRYPT besteht aus einzelnen Programmodulen, die in einer Art Baukastensystem implementiert werden können. DOKRYPT ist nicht als Anwendung konzipiert, sondern bietet einer Anwendung die Möglichkeit, ohne ressourcenintensive Modifikationen Sicherheit zu integrieren. Die Anwendung benötigt zur Funktion der DOKRYPT-Module eine personalisierte TCOS-Chipkarte und einen über die serielle Schnittstelle angeschlossenen B1-kompatiblen Chipkartenleser.
- **STE** (Security Terminal Equipment) – ist eine Security-Black-Box zur Erreichung systemunabhängiger IT-Sicherheit im ISDN, digitalen Festverbindungen, Datex P (X.25), Standleitungen (X.21) und auf TCP/IP Protokollen basierenden Netzwerken. Die Sicherheitsfunktionen der STE gewährleisten einen gesicherten Zugriff auf vorhandene Informationssysteme. Die STE verhält sich völlig transparent. Das STE identifiziert und authentisiert Benutzer eindeutig mit Hilfe von Telesec (TCOS) Chipkarten. Die Personalisierung und die Ausgabe der Chipkarten an die Benutzer wird vom Telesec Trust Center der Deutschen Telekom AG übernommen. Als weitere Sicherheitsfunktion der STE wird durch kryptographische Verfahren eine sichere Datenübertragung mit hoher Vertrauenswürdigkeit und Zuverlässigkeit gewährleistet. Die eingesetzten kryptographischen Verfahren sind:
  - RSA für Keymanagement, Session-Key-Austausch und Authentikation.
  - DES / 3DES für die Nutzdatenverschlüsselung.
  - Der Schlüsselaustausch erfolgt in Anlehnung an CCITT X.509.

Man kann sehen, wie sich hier exemplarisch aus einzelnen Sicherheitskomponenten Konzeptionen unterschiedlicher Stärke modular und bedarfsgerecht zusammenstellen lassen – mit der ständigen Option der Erweiterung.

5.2.2 Sicherheit in Mobilfunknetzen

In den letzten Jahren ist Mobilität ein wichtiger Begriff in unserer Gesellschaft geworden, dem auch im Bereich der IT und Kommunikation Rechnung getragen wurde. Die aktuellen Mobilfunksysteme faßt man unter dem Oberbegriff GSM zusammen, wobei es sich um einen internationalen Standard (ursprünglich ein paneuropäischer Standard, der mittlerweile

aber von 56 Ländern übernommen wurde) für digitale zellulare Mobilfunk-netze handelt. Zellular bedeutet, daß das geographische Kommunikationsgebiet für den Funkbetrieb in wabenförmige Zellen aufgeteilt ist. Durch die vollständige Digitalisierung können neben Sprachdaten natürlich auch Text- oder Bildinformationen übertragen werden. In Deutschland steht GSM für zwei Netztypen, die jeweils von verschiedenen Anbietern genutzt werden. Es gibt das DCS900 (= Digital Cellular System), das im 900-MHz-Bereich arbeitet und entsprechend das DCS1800. DCS900 wird von den Anbietern Deutsche Telekom D1 und Mannesmann Mobilfunk D2 repräsentiert, DCS1800 durch den Anbieter E-Plus Mobilfunk (E1) und einen in 1997 entstehenden Betreiber für E2. [1]

Die nachfolgende Darstellung des Sicherheitskonzeptes bezieht sich generell auf alle GSM-Netze, in speziellen Bereichen werden Details aus dem D2-Netz genannt. Zu den bereits bekannten Sicherheitsforderungen kommt im „Mobilbereich“ noch die Forderung nach *Anonymität*, denn sonst ließen sich Bewegungsprofile von den Benutzern erstellen. Ein GSM-System besteht aus einer Vielzahl verschiedener sicherheitsrelevanter Netzkomponenten, die kurz genannt werden sollen (es werden auch verschiedene Algorithmen mit den Bezeichnern Ax (x = 2,...,8) genannt, da die konkreten Krypto-Algorithmen von den Netzbetreibern geheimgehalten werden):[2]

- **Subscriber Identify Module (SIM)** – Jeder Benutzer hat eine teilnehmerindividuelle Chipkarte, die dem ICC-Standard entspricht, aber auch als sog. Plug-In-SIM mit 25mm x 15mm Größe für kleine Geräte am Markt ist. Es werden Algorithmen (A3 und A8), Teilnehmerdaten und Telefonverzeichnisse gespeichert.
- **Mobile-Equipment (ME)** – Das ME ist das eigentliche Handy, in das das SIM eingesteckt wird, womit es zur *Mobilstation* wird. Es enthält keine teilnehmerspezifischen Daten, jedoch eine Geräte-ID und Verschlüsselungsalgorithmen (A5).
- **Base Station System (BSS)** – Die Basisstation bildet das Gegenstück zur Mobilstation und empfängt die Daten der Funkstrecke. Auch sie enthält den Algorithmus A5.
- **Mobile Switching Center (MSC)** – Die Vermittlungsstellen, denen für ihren Betrieb Visited Location Register (VLR) zugeordnet werden, in denen die temporären Daten (Kennung, Authentikationsversuche) eines Teilnehmers gespeichert werden.

---

[1] Vgl. Beheim, Johannes: Sicherheit und Vertraulichkeit bei europaweiter Mobilkommunikation, in: DuD , Jg. 1994, Heft 6, S. 327 - 331, hier S. 327.

[2] Vgl. Michel, U.: Sicherheitsfunktionen im paneuropäischen Mobilfunknetz, in: Verläßliche Informationssysteme, Proceedings VIS’91, Hrsg.: Pfitzmann, A. / Raubold, E., Berlin et al. 1991, S. 133 - 145, hier S. 135ff.

- **Home Location Register (HLR)** – In diesem „Heimatregister“ werden überwiegend permanente Daten des Teilnehmers gespeichert.
- **Authentication Center (AC)** – Das AC bildet das Gegenstück zur SIM im ortsfesten Teil des Netzwerkes und enthält Schlüssel sowie die Algorithmen A3 und A8. Zudem sind hier die Algorithmen A2 und A4 in einer Security-Box implementiert.
- **Gateway-MSC** – Diese Vermittlungsstellen-Gateways stellen den Übergang zu anderen Mobilfunknetzen und zum ISDN-Festnetz dar.

Im folgenden soll nun der *Ablauf der Sicherheitsmechanismen* in den Netzkomponenten dargestellt werden.[1] Zunächst wird der Teilnehmer mit einer ihm zugewiesenen Teilnehmer-ID im AC registriert, wobei auch der aus der Kartenvorbereitung stammende Private-Key K_T abgespeichert wird. Bei der Übertragung zum AC wird K_T mit A4 selbst verschlüsselt und nach der A4-Entschlüsselung wird der Schlüssel im AC sofort wieder mit A2 zur nachfolgenden Speicherung verschlüsselt. Dafür ist im AC eine Security-Box mit eigenem Prozessor und Betriebssystem (in einem EPROM fest verbunden) installiert, die durch eine mechanische Sicherung vor unerlaubtem Entfernen geschützt ist. Sobald ein Teilnehmer im AC eingerichtet ist, berechnet die Security Box die für den Netzzugang erforderlichen Sicherheitsparameter (Security Tripletts). Dazu erzeugt ein Zufallsgenerator eine Zahl (RND, 128-Bit), die gemeinsam mit K_T die Eingangsparameter für die Sicherheitsalgorithmen A3 / A8 bildet. A3 liefert daraus den Wert „Signed Response“ (SRES, 32-Bit), der später bei der Berechtigungsprüfung des SIMs gegenüber dem Netz benötigt wird. A8 liefert als Ergebnis den Schlüssel K_V (64-Bit Länge), der zur Datenverschlüsselung auf der Funkstrecke (Übertragung in der Luft) benutzt wird, womit Schlüsselhierarchien genutzt werden. Nach der Registrierung im AC können für den Teilnehmer im HLR beantragte Dienste, Telefonbuchnummern etc. eingetragen werden.

Unabhängig davon, wo sich der Teilnehmer aufhält, werden an seinem jeweiligen Aufenthaltsort für ihn Sicherheitsparameter gebraucht. Deshalb sorgt das VLR immer dafür, daß „Security Tripletts“ über das Heimatregister vom AC besorgt werden. Sobald nur noch zwei solche Parametersätze aus RND, SRES und K_V zur Verfügung stehen, werden fünf neue angefordert. Das VLR hat noch eine weitere wichtige Aufgabe zur Geheimhaltung / Anonymisierung des Teilnehmers. Damit die spezifische internationale Mobil-

---

[1] Vgl. Vedder, Klaus: Security Aspects of Mobile Communication, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 193 - 210, hier S. 196ff.

funkteilnehmerkennung (IMSI) nicht bei jedem Netzzugang übertragen werden muß, weist das VLR dem Teilnehmer beim erstmaligen Anmelden eine temporäre Teilneh-meridentität (TMSI) zu, die für Dritte völlig ohne Bezug zur IMSI ist. Da die TMSI's laufend geändert werden, bleibt die Identität des Teilnehmers während der Funkübertragung vertraulich. Wichtigste Sicherheitsfunktion in Mobilfunknetzen ist die *Teilnehmerauthentikation*:[1]

Als erstes muß sich der Teilnehmer seiner SIM gegenüber identifizieren, was mit Hilfe einer vier- bis achtstelligen PIN-Eingabe in die Mobilstation geschieht. Anschließend übergibt die Mobilstation dem VLR, welches seinem momentanen Aufenthaltsort zugeordnet ist, seine TMSI und die Location Area Identification (LAI) des Aufenthaltsortes (LA, Location Area), in dem die letzte erfolgreiche Authentikation stattfand. Danach wird eine Überprüfung der Netzzugangsberechtigung der Mobilstation vorgenommen, wozu ein einseitiges, symmetrisches und schnelles Authentikationsprotokoll nach dem Challenge/Response-Verfahren abläuft. Dies geschieht mit A3 und A8, die ja im SIM und der Security-Box vorhanden sind. Stimmt die übergebene LAI mit der Kennung des aktuellen VLR's *nicht* überein, so wird anhand der LAI das vorherige VLR (alt) ermittelt und von dort vorrätige Security Tripletts abgerufen – ansonsten ruft das VLR aus seiner eigenen Datenbank ein Security Triplett ab oder fordert bei Erstbenutzung des Teilnehmers dessen IMSI ab, um Security Tripletts beim AC anzufordern.

Als *Challenge* schickt das VLR aus dem Security Triplett die Zufallszahl RND an die CPU des im Handy untergebrachten SIM. Mit Hilfe des dort befindlichen Teilnehmerschlüssels K_T liefert A3 einen SRES, den die Mobilstation als *Response* zurück an das VLR überträgt. Dieses vergleicht nun diese SRES mit dem vom AC vorberechneten und in sich selbst (VLR) bereitstehenden SRES. Bei Nichtübereinstimmung wird der fehlerhafte Authentikationsversuch in Security Records aufgezeichnet und durch den Netzbetreiber später ausgewertet. Zusätzlich wird noch die Handykennung IMEI (= International Mobile Equipment Identificator) angefordert, um das Gerät zu überprüfen und festzustellen, ob es evtl. im Geräteidentifizierungsregister (EIR) als gestohlen gemeldet ist.

Der Authentikation folgt die *Verschlüsselung*[2] – Im Zuge der Authentikation wird im SIM vom Algorithmus A8 der Schlüssel K_V berechnet (somit muß dieser nicht über die Funkstrecke gesendet werden). Auf der anderen Seite ist die Basisstation für die Verschlüsse-

---

[1] Vgl. Pütz, Stefan: Lösungsansätze für Authentikation in künftigen Mobilfunksystemen, in: Mobile Kommunikation: Vorträge der ITG-Fachtagung vom 26-28.09.1995, ITG Fachbericht 135, Hrsg.: ITG,Berlin 1995, S. 411 - 422, hier S. 412ff.

[2] Vgl. Beheim, Johannes, a.a.O., S. 330; **ebenso** Eberspächer, J.: Sichere Daten, sichere Kommunikation, Berlin, Heidelberg 1994, S. 217.

lung verantwortlich, wofür ihr das VLR der zuständigen Vermittlungsstelle den erforderlichen Schlüssel K_V übermittelt – womit die verschlüsselte Datenübertragung mit Hilfe von A5 auf der Funkstrecke beginnen kann. A5 ist eine Stromchiffre, weil ständig Bitströme ohne Verzögerung zu verschlüsseln sind. Eingangsparameter sind K_V sowie die TDMA-Rahmennummer (= Time Division Multiple Access) von 22-Bit Länge, woraus A5 alle 4,615 ms eine Folge von 114 pseudozufälligen Bits generiert. Die Berechnung mit A5 erfolgt für jeden TDMA-Rahmen extra, wobei das Ergebnis von A5 mit der Nutzinformation des Teilnehmers modulo verknüpft wird.

Die Verschlüsselung erfolgt nur auf der Funkstrecke zwischen Mobil- und Basisstation, während die Übertragung der Nachrichten auf Festnetzleitungen vom Netz aus unverschlüsselt geschieht. Für eine Ende-zu-Ende-Verschlüsselung ist der Teilnehmer selbst verantwortlich. Mannesmann Mobilfunk D2 bietet dieses jedoch als Mehrwertdienst innerhalb seines Funknetzes an. Dazu wird ein Verfahren genutzt, das auch zwischen Mannesmann Mobilfunk selber, seinen Vermittlungsstellen und seinen Partnerunternehmen (Service Provider) in Betrieb ist und nun beschrieben werden soll:[1]

Das Mobilfunknetz wird zentral von einer IBM-Host-Applikation verwaltet und gesteuert. Die Kontakte zum Host laufen über das hauseigene Netz oder aber über das öffentliche Datex-P-Netz in X.25-Konfiguration. Der Host fungiert als Server, die Rechner- und Rechnernetze der Service Provider und Vermittlungsstellen als Clients, die definierte Dienste in verbindlicher und vertraulicher Form abrufen können. Dies geschieht über transaktionsorientierte Protokolle, wobei die Transaktionsdaten mit Hilfe von EDIFACT-Nachrichten (Electronic Data Interchange for Administration, Commerce and Transport) ausgetauscht werden. EDIFACT ist ein UN-genormtes Regelwerk für den elektronischen Austausch von Geschäftsdokumenten. Über EDIFACT-Konverter werden aus internem Datendarstellungsformat die Daten in EDI-Format konvertiert, so daß die Kommunikation trotz der verschiedenen Beteiligten einheitlich erfolgen kann (auch in Hinblick auf künftige Partner und den Datenaustausch mit anderen Netzen).

Für die vertrauliche Kommunikation über öffentliche Netze hat die Firma Kryptokom aus Aachen für Mannesmann Mobilfunk ein Sicherheitskonzept entwickelt. Basierend auf der *Security-Black-Box „Kryptoguard X.25“* wurde ein Mannesmann-spezifisches Modell als Security-Front-End (SFE) – eine Kombination von Black-Box und Gateway – entwickelt, das mit Kryptoguard X.25-Geräten kommunizieren kann. Mit Hilfe des SFE werden die

---

[1] Vgl. Pohlmann, Norbert, Öffentliche Netze, a.a.O., S. 129f.

Rechnernetze transparent entkoppelt, und es ist nicht möglich, auf die Betriebssystemebene des Anwendungsrechners zu kommen. Zudem werden die Sicherheitsdienste Authentikation, Zugangskontrolle, Vertraulichkeit, Urheber- und Empfängernachweis und umfangreiche Protokollauswertungsmechanismen angeboten. Dadurch wird erreicht, daß nur autorisierte Clients Zugriff auf die Mobilfunk-Anwendung haben, keine Daten im Klartext im öffentlichen X.25-Netz vorliegen und alle Transaktionen verbindlich sind. Der SFE ist modular aufgebaut, wobei hier nur das Sicherheitsmodul interessieren soll. Dieses Modul kontrolliert und steuert die Security-Protokolle, die vom Security-Layer abgewickelt werden, der die jeweiligen Netze (LU6.2 / X.25) voneinander trennt. Das Sicherheitsmodul und der gesamte SFE können nur über ein Security-Operator Interface beeinflußt werden, das mit einer Chipkarte geschützt ist. Nach erfolgreicher Authentikation mit der Chipkarte kann der Operator das Security Management der SFE bearbeiten. Hiermit werden Schlüsselsysteme und Zertifikate für alle angeschlossenen Black-Boxes generiert und verwaltet, Konfigurationsdateien installiert, Access-Listen gepflegt und Analysen durchgeführt. Das Sicherheitsmodul ist eine „sichere Hardware“, in der die sicherheitsrelevanten Aktionen geschützt ausgeführt und ihre Daten geschützt gespeichert werden können. Das Modul ist physikalisch gekapselt und mit einer Sensorik ausgerüstet, die evtl. Angriffe erkennt und Alarm gibt (auch automatische Löschungen können eingestellt werden). In ihr sind ein Logbuch, die Access-Listen, Private-Keys und die Kryptoverfahren implementiert.[1]

Zwischen den Black-Boxes wird eine Two Pass Parallel Authentikation durchgeführt, Keyzertifizierung und -management laufen automatisch innerhalb des Sicherheitsmoduls ab. Für die Verschlüsselung wird DES verwendet, für Keymanagement, digitale Signaturen und Authentikation RSA-Algorithmen und Hash-Codes.

Für das hauseigene Netz ist auf dem Host ein Security-Filter implementiert, der die Sicherheitsdienste der SFE softwaremäßig realisiert. Auch zu ISDN ist ein Black-Box-Konzept realisiert.

Man sieht, daß unternehmensweite Sicherheitskonzepte sehr umfassend sein können, zumal sich die beschriebene Konzeption nur auf den Mobilfunkbetrieb von Mannesmann Mobilfunk bezieht und eventuelle interne Verwaltungsnetze und Internetzugänge außen vor läßt.

6 Schlußwort

---

[1] Vgl. Pohlmann, Norbert, Öffentliche Netze, a.a.O., S. 130.

Die in der vorliegenden Arbeit behandelte vielschichtige Thematik der Sicherheitskonzepte für Informationsnetze macht abschließend sowohl eine kurze kritische Würdigung, als auch einen Ausblick auf zukünftige Forderungen und Entwicklungen im Bereich der IT-Sicherheit nötig.

Es konnte gezeigt werden, daß ein nicht unbeachtliches Bedrohungspotential für Informationsnetze besteht, aber gleichzeitig auch ein umfangreiches Angebot an Sicherheitskonzeptionen existiert. Man konnte allerdings auch sehen, daß man „Sicherheit“ nicht einfach plug&play-mäßig anschließen und einschalten kann, sondern eine ausführliche Planung vorausgehen muß – gefolgt von einer dauerhaften intensiven Wartung und Pflege der Sicherheitskomponenten, um „laufende“ Sicherheit zu gewährleisten. Es handelt sich also um einen dynamischen Prozeß.

Das ist vielleicht auch der Grund dafür, daß sich am Markt primär zwei Haltungen polarisieren. Ein Teil der Unternehmen schottet sich gänzlich ab, andere gehen im Extrem vollkommen ungeschützt in das Internet. Viele kleine und mittelständische Unternehmen sind auch einfach überfordert, sich in ihrem IT-Sicherheitsbedarf einzuordnen und die Kosten zu kalkulieren. Das wird sich ändern, wenn zu akzeptablen Preisen umfassende Konzepte und Beratung von speziellen IT-Sicherheits-Dienstleistern (die ja auch gerade erst im Entstehen sind) angeboten werden, womit z.B. über Customizing-Produkte ein flächiger Einsatz möglich wäre.

Des weiteren sollten die Evaluierungsstandards international zusammengefaßt und darauf geachtet werden, daß die Evaluierungen zügig vorgenommen werden, damit die Geräte nicht veraltet sind, wenn sie ihr Zertifikat erhalten. Letztendlich stellt sich die Frage, inwieweit der Markt und der Test im Netz nicht ohnehin die beste Sicherheitseinstufung bieten – „Trockentests“ bringen nur eingeschränkte Sicherheitsbestätigung.

Aber auch der Gesetzgeber ist gefragt, denn es müssen rechtliche Rahmenbedingungen geschaffen und internationale Schranken entfernt werden, um einen umfassenden globalen IT-Sicherheitsbetrieb zu ermöglichen. Vor allem die noch geltenden US-amerika-nischen Exportbeschränkungen für kryptologische Produkte hemmen eine effektive globale Sicherheitsstruktur. Des weiteren ist die Verschlüsselung in manchen Staaten wie z.B. Frankreich auf eine gewisse maximale Krypto-Stärke beschränkt oder in anderen Ländern ganz verboten. In Deutschland wird im Rahmen einer Art „Pionierarbeit“ gerade ein Signaturgesetz[1] erarbeitet, das im Entwurf bereits vorliegt. In einer Stellungnahme des Fachverbandes In-

formationstechnik im VDMA und ZVEI heißt es dazu treffenderweise: „*Die Einführung der geplanten Regelung schafft die Voraussetzungen, um die moderne 1nformations- und Kommunikationstechnik auch für beweisverwertbare und formgerechte Rechtshandlungen (Willenserklärungen, Archivierung von Dokumenten etc.) einzusetzen. Dies erschließt ein erhebliches Rationalisierungspotential in Wirtschaft und Verwaltung, was dem Wirtschaftsstandort Deutschland zugute kommt. Darüber hinaus verbessert die digitale Signatur die Sicherheit bei der Nutzung von Informations- und Kommunikationstechniken entscheidend.*“[2] Um eine erforderliche Rechtssicherheit zu schaffen, ist es in einem zweiten Schritt erforderlich, dem „elektronischen Dokument“ mit digitaler Signatur gesetzlich den gleichen Wert einzuräumen wie der herkömmlichen papiergebundenen Schriftform. Rechtsvorschriften, die bisher die Schriftform vorgeben, sollten künftig auch die digitale Form mit digitaler Signatur zulassen (z.B. Handelsdokumente und Steuerdaten).

Generell wird der Einsatzbereich für IT-Sicherheitstechnologie in den nächsten Jahren eklatant weiter wachsen. Die Entwicklung mobiler Kommunikationsprodukte und die Steigerung der Leistung der Trägernetze läßt das Potential von Telearbeitsplätzen immer mehr steigen. Nach einer Untersuchung der Empirica Gesellschaft für Kommunikations- und Technologieforschung mbH (Stand Mai 1995) sind schon heute 20 - 40 % aller Bürojobs für die Telepräsenz geeignet. Die Interesse für Telepräsenz (von Arbeitnehmern und Entscheidungsträgern) liegt bei ca. 17 % – so daß in Deutschland 2,5 Mio. Menschen gerne telearbeiten würden.[3] In Deutschland sind etwa 150.000 Telearbeitsplätze verwirklicht, was nur einem dritten Platz in Europa entspricht. Für das nächste Jahrtausend wird sogar mit einem Umbruch zu virtuellen Unternehmen gerechnet (Definition:

„*Die virtuellen Organisationen sind Unternehmen oder Betriebe, die nicht mehr als räumlich-organisatorische Einheit existieren, sondern nur noch als elektronisches Netzwerk.*“[4]). Hierbei kann man es als Herausforderung ansehen, Videokonferenzen in Echtzeit zu übertragen, und trotzdem Verschlüsselung nutzen zu können.

Des weiteren wird über kurz oder lang die Briefpost und der Telefaxverkehr durch reine E-Mail-Anwendungen ersetzt werden, so daß evtl. jeder Nutzer / Bürger eine Chipkarte hat,

---

1 Vgl. dazu die Entwürfe von Gesetz und Verordnung unter folgenden URL’s: URL=http://www.telesec.de/siggeset.htm und URL=http://www.telesec.de/sigveror.htm

2 ZVEI-Pressestelle: Stellungnahme des Fachverbandes Informationstechnik im VDMA und ZVEI zum Signaturgesetz vom 25. September 1996, URL=http://www.telesec.de/fvit.htm: 19.11.1996

3 Vgl. Muth, Reinhard / Schäfer, Wolfgang: Telepräsenz. IT-Sicherheitsspezifische Analyse von Telearbeitsplätzen, in: DuD, Jg. 1996, Heft 10, S. 596 - 601, hier S. 597.

4 Stollreither, Konrad: Die Zukunft wird anders sein, in: DuD, Jg. 1996, Heft 5, S. 279 - 285, hier S. 282.

mit der er sich authentisieren und seine Post signieren kann. Dazu könnte der Multimedia- / Internetcomputer der Zukunft standardmäßig einen Kartenleser in der Tastatur integriert haben – wie es heute zum Teil schon in Unternehmen realisiert ist. Solche Lösungen werden auch für ISDN-Telefone immer häufiger genutzt werden.

Weitere künftig wachsende Chipkartenanwendungen sind natürlich der E-Cash-Sektor sowie Abrechnungs- und Authentikationssysteme in den Bereichen TV-On-Demand, Tele-Shopping, Tele-Learning, Krankheitskostenaufzeichnung, Straßenbenutzungsab-rechnung und Verkehrsleitsystemauthentikation.

Es sollte noch erwähnt werden, daß einige Sicherheitskomponenten auch „kriminell“ genutzt werden können. So stellte z.B. der Verfassungsschutz im letzten Jahr fest, daß sowohl rechtsradikale Vereinigungen als auch die PKK (dort sogar als fester Bestandteil ihrer Ausbildung für Guerillakämpfer[1]) PGP als Tarnung ihres Mailverkehrs nutzen.

Im nächsten Jahrtausend wird es auf jeden Fall zu einer immensen Ausweitung der IT kommen, die in bezug auf den Tatbestand der Sicherheit nur in einem synergetischen Kraftakt von Gesellschaft, Politik und Forschung in einem Prozeß der Emergenz zu beherrschen sein wird.

---

[1] Vgl. Fox, Dirk, a.a.O., S. 187.

LITERATURVERZEICHNIS

Monographien

Beutelspacher, A. / Kersten, A.
Chipkarten als Sicherheitswerkzeug, Berlin et al. 1991.

Brobeil H.
Software-Angriffe auf PC's und Netzwerke, Oldenbourg 1992.

Cerny, D. / Kersten, H.
Sicherheitsaspekte in der Informationstechnik, Braunschweig 1991.

Chapman, D. Brent / Zwicky, Elisabeth D.
Einrichten von Internet Firewalls, Bonn 1996.

Cheswick, W. / Bellovin, S.
Firewalls and Internet Security, Reading 1996.

Duelli, H. / Pernsteiner, P.
Alles über Mobilfunk, München 1992.

Eberspächer, J.
Sichere Daten, sichere Kommunikation, Berlin, Heidelberg 1994.

Heldman, Robert K.
Information Telecommunications, 1994.

Kerner, Helmut
Rechnernetze nach OSI, 2. Aufl., Bonn et al. 1993.

Kersten, H.
Sicherheit in der Informationstechnik, 2. Aufl., München 1995.

Kersten, Heinrich
Einführung in die Computersicherheit, München et al. 1991.

Krallmann, Hermann
EDV-Sicherheitsmanagement, Berlin 1989.

Kyas, Othmar
Sicherheit im Internet: Risikoanalyse - Strategien - Firewalls, Bergheim 1996.

Niemeyer, Joachim
Mobile Computing, München 1994.

Oppliger, Rolf
Computersicherheit: Eine Einführung, Braunschweig / Wiesbaden 1992.

Plattner, B. / Lanz, C. et al.
Elektronische Post und Datenkommunikation, 1. Aufl., Bonn, München et al. 1989.

Pohl, Hartmut
Sicherheit der Informationstechnik, Köln 1989.

Preneel, Bart
Computer Security and Industrial Cryptography, Berlin 1991.

Rihaczek, Karl
Datenverschlüsselung in Kommunikationssystemem, DuD-Fachbeiträge 6, Braunschweig 1984.

Rihaczek, Karl
Datenschutz und Kommunikationssysteme, DuD-Fachbeiträge 1, Braunschweig 1981.

Ruland, Christoph
Informationssicherheit in Datennetzen, Bergheim 1993.

Ruland, Christoph
Datenschutz in Kommunikationssystemen, Pulheim 1987.

Russell, Deborah / Gangemi Sr., G. T.
Computer Security Basics, 1. Aufl., Sebastopol 1991.

Siyan, Karanjit / Hare, Chris
Internet Firewalls und Netzwerksicherheit, 1995.

Stahlknecht, **Peter**
Einführung in die Wirtschaftsinformatik, 7. Aufl., Berlin, et al. 1995.

Stallings, William
Sicherheit im Datennetz, München, London, et al. 1995.

Stallings, William
Network and Internetwork Security, Englewood Cliffs 1995.

Thaller, Georg Erwin
Computersicherheit, DuD-Fachbeiträge 18, Braunschweig / Wiesbaden 1993.

Wähner, Gerd W.
Datensicherheit und Datenschutz, Düsseldorf 1993.

Weck, Gerhard
Datensicherheit, Stuttgart 1984.

Zentralstelle für Sicherheit in der Informationstechnik:
IT-Sicherheitskriterien - Kriterien für die Bewertung der Sicherheit von Systemen der IT vom 11.01.1989, Köln 1989.

Festschriften, Sammelwerke, Zeitschriften

Abel, H.G. / Ermer, D. J.
Sicherheitsmaßnahmen bei Vernetzung, in: Sichere EDV, Band 2, Hrsg.: Wißner, B., Augsburg 1996, Abschnitt 5/5.

Abel, Horst / Schoberth, Andreas
Effektive und sichere Nutzung von Internet-Diensten, in: KES, 12. Jg. (1996), Heft 4, S. 32 - 42.

Albert, Bodo
Authentisierung, digitale Unterschrift und Chipkarte, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 331 - 350.

Alles, Peter / Hueske, Thomas
Netzwerksicherheit und Chipkarteneinsatz, in: DuD, Jg. 1993, Heft 4, S. 214 - 219.

Bauer, Peter / Peuckert, Heribert
Chipkarten mit Kryptographie erschließen neue Anwendungsfelder, in: DuD, Jg. 1994, Heft 7, S. 380 - 384.

Bauspieß, Fritz; Horster, Patrick; Stempel, Steffen Weck, G.
Netzwerksicherheit durch selektiven Pakettransport, in Verläßliche Informationssysteme, Proceedings VIS `93, Hrsg.: Horster, P., Braunschweig 1993, S. 395 - 415.

Becker, K. / Beutelspacher, A.
Hinter Schloß und Riegel ?, in: MC-Magazin, Jg. 1994, Heft 5, S. 88 - 95.

Becker, Lutz / Ehrhardt, Johannes
Die Datenautobahnen: Die Sicherheit der Highways, in: Datacom, 12. Jg. (1995), Heft 4, S. 126 - 129.

Beheim, Johannes
Sicherheit und Vertraulichkeit bei europaweiter Mobilkommunikation, in: DuD , Jg. 1994, Heft 6, S. 327 - 331.

Birkelbach, Jörg
Safer Banking, in: c’t Magazin für Computertechnik, Jg. 1996, Heft 12, S. 104 - 108.

Blab, Herbert A.
Chipkarten und Kryptosysteme in digitalen Kommunikationsanlagen, in: Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 11-13.11.1992, Hrsg.: ITG, Berlin 1993, S. 291 - 301.

Borowka, Petra
Sicherheit durch Netzwerkmanagement, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’93, Hrsg.: Lippold, Heiko / Schmitz, Paul u.a., Braunschweig 1992, S. 137 - 170.

Brandl, Hans
CRYPSET 300, in: Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 11-13.11.1992, ITG Fachbericht 121, Hrsg.: ITG, Berlin 1993, S. 283 - 290.

Damker, Herbert / Federrath, Hannes / Schneider, Michael J.
Maskerade-Angriffe im Internet, in: DuD, Jg. 1996, Heft 5, S. 286 - 294.

Dienst, Detlef / Fox, Dirk
Transparente Sicherheitsmechanismen für ISDN-Anwendungen, in: Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 09-10.11.1994 , ITG Fachbericht 131, Hrsg.: ITG, Berlin 1994, S. 81 - 95.

Dürr, Helmut
Kommunikationsfunktionen im OSI-Management, in: Datacom, 10. Jg. (1993), Heft 8, S. 88 - 92.

Eisele, Raymund
Sicherheit und Elektronische Unterschriften - SmartDisk, in: DuD, Jg. 1995, Heft 7, S. 401 - 406.

Engler, Tobias
Der gläserne Web-User, in: c’t Magazin für Computertechnik, Jg. 1996, Heft 12, S. 94 - 99.

Ermer, Dieter
Grundsätze für Benutzerrichtlinien für das Internet, in: KES, 12. Jg. (1996), Heft 4, S. 37 - 42.

Fischer, Ralf
Sichere Nachrichten aus dem All, in: KES, 12. Jg. (1996), Heft 1, S. 8 - 15.

Fox, Dirk
DSS: Aufwand, Implementierung und Sicherheit, in: Verläßliche Informationssysteme, Proceedings VIS `93, Hrsg.: Horster, P., Braunschweig 1993, S. 333 - 352.

Fox, Dirk
Schlüsseldienst. Private Kommunikation mit PEM und PGP, in: c’t Magazin für Computertechnik, Jg. 1995, Heft 9, S.184 - 187.

Fuhrberg, Kai
Gefährdungen bei der Benutzung des Internets, in: BSI-Forum, 3. Jg. (1995), Heft 6, S. 41 - 45.

Fumy, Walter
Network Security, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 211 - 225.

Gefrörer, Stanislaus
Chipkarten in Sinix-Netzen, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 257 - 274.

George, Gerhard
Extended Authentication mit dem Securid-Token, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET ’92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 115 - 126.

Gilge, Michael
Standards und Trends in der Bildkommunikation, in: Codierung für Quelle, Kanal und Übertragung: Vorträge der ITG-Fachtagung vom 26-28.10.1994, ITG Fachbericht 130, Hrsg.: ITG, Berlin 1994, S. 211 - 224.

Goebel, Jürgen W. / Scheller, Jürgen
Elektronische Unterschriftsverfahren in der Telekommunikation, Braunschweig 1991.

Grimm, Rüdiger
Kryptoverfahren und Zertifizierungsinstanzen, in: DuD, Jg. 1996, Heft 1, S. 27 - 36.

Hagemann, Hagen / Rieke, Andreas
Datenschlösser. Grundlagen der Kryptologie , in: c’t Magazin für Computertechnik, Jg. 1994, Heft 8, S. 230 - 238.

Hammerer, Charlie
Vermittlung der Problematik des sicheren Schlüssel-Verteilens als Lehrprogramm, in: DuD, Jg. 1993, Heft 1, S. 33 - 39.

Hange, Michael
Die Rolle der Kryptologie im Rahmen der „IT-Sicherheit“, in: Sicherheit in Informationssystemen, Proceedings SECUNET ’91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 15 - 21.

Hartleif, Siegfried
Multifunktionale Chipkarten an Kommunikationsendgeräten, in: Nutzung und Technik von Kommunikationsendgeräten: Vorträge der ITG-Fachtagung vom 11-13.11.1992, Hrsg.: ITG, Berlin 1993, S. 303 - 313.

Heinrich, Wilfried
Es lebe das Hoffnungsprinzip, in: Datacom, 13. Jg. (1996), Heft 1, S. 58 - 60.

Hembach, Friedrich
IT-Sicherheitspolitik im Datex-P, in: BSI-Forum, 2. Jg. (1994), Heft 3, S. 56 - 58.

Horster, P. / Knobloch, H.-J.
Protokolle zum Austausch authentischer Schlüssel, in: Verläßliche Informationssysteme, Proceedings VIS'91, Hrsg.: Pfitzmann, A. / Raubold, E., Berlin et al., S. 321 - 328.

Horster, Patrick; Portz, Michael
Privacy Enhanced Mail: Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet, in: DuD , Jg. 1994, Heft 8, S. 434 - 442.

Jacobson, Gunnar
Grenzenlose Sicherheit, in: Datacom, 13. Jg. (1996), Heft 1, S. 48 - 56.

Janson, Phil / Waidner, Michael
Electronic Payment Systems, in: DuD, Jg. 1996, Heft 6, S. 350 - 359.

Kauffels, F.-J.
Netzsicherheit, in: Datacom, 10. Jg. (1993), Heft 1, S. 96 - 103.

Kauffels, Franz-J.
Schwachstellen der Informationssicherheit in Netzen, in: DuD im Wandel der Informationstechnologien, Hrsg.: Spies, P. P., Berlin 1985, S. 51 - 69.

Kersten, Heinrich
Evaluierung und Zertifizierung von IT-Systemen, in: Sicherheit in Informationssystemen, Proceedings SECUNET '91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 333 - 348.

Keus, Klaus
Aktuelle IT-Sicherheitskriterien, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '93, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1993, S. 171 - 200.

Kiranas, Argiris
Technische Sicherheitsmechanismen in POS-Systemen, in: DuD, Jg. 1996, Heft 7 u. 8, S. 413 - 420 u. 472 - 478.

Klein, Stefan
Informationssicherheit bei der Kommunikation von Versicherungen mit Dritten, in: Sicherheit in Informationssystemen, Proceedings SECUNET '91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 169 - 183.

Klein, Stefan / Weller, Stefan
EDI ? Aber sicher, in: KES, 9. Jg. (1993), Heft 2, S. 52 - 60.

Klein, Stefan / Weller, Stefan
Sicherheismechanismen für EDIFACT und X.400, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 43 - 60.

Klute, Rainer
Verschlußsache - Sicherheit im WWW, in: iX Multiuser, Multitasking Magazin, Jg. 1995, Heft 12, S. 132 - 145.

Knobloch, Hans-Joachim / Horster, Patrick
Eine Krypto-Toolbox für Smartcards, in: DuD , Jg. 1992, Heft 7, S. 353 - 361.

Koritnik, Andreas
Firewalls für's Internet - Alle Schotten dicht ?, in: KES, 11. Jg. (1995), Heft 3, S. 36 - 42.

Koritnik, Andreas
Firewalls - Welche Bastion für welchen Dienst ?, in: KES, 11. Jg. (1995), Heft 6, S. 31 - 38.

Kossel, Axel
Innere Sicherheit. Sichere Intranet-Lösungen, in: c't Magazin für Computertechnik, Jg. 1996, Heft 10, S. 332 - 334.

Kowalski, B.
Telesec, in: Secure Information, Hrsg.: Eberspächer, J., Berlin u.a. 1994, S. 134 - 166

Kruse, Dietrich
Sicherheitszertifikat für Chipkarten, in: DuD, Jg. 1995, Heft 9, S. 537 - 542.

Kruse, Dietrich / Peuckert, Heribert
Chipkarte und Sicherheit, in: DuD, Jg. 1995, Heft 3, S. 142 - 149.

Kunze, Michael
Privatsphäre im Datennebel, in: c't Magazin für Computertechnik, Jg. 1996, Heft 12, S. 100 - 102.

Leiberich, Otto
Verschlüsselung und Kriminalität, in: BSI-Forum, 3. Jg. (1995), Heft 1, S. 60 - 61.

Lennox, Gordon
EDI Security, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 235 - 243.

Lipp, Michael
Kommunikationsnetze für große verteilte Client/Server-Architekturen, in: KES, 11. Jg. (1995), Heft 5, S. 70 - 80.

Lippold, Heiko
Management der Informationssicherheit, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 17 - 40.

Luckhard, Norbert
Kryptologische Begriffe und Verfahren, in: c't Magazin für Computertechnik, Jg. 1996, Heft 12, S. 110 - 113.

Mackenbrock, Markus
ITSEC Funktionalitätsklasse für die Sicherheit von digitalen TK-Anlagen, in: BSI-Forum, 3. Jg. (1995), Heft 3, S. 47 - 51.

Meyer, M. / Rannenberg, K.
Eine Bewertung der ITSEC, in: VIS'91 Verläßliche Informationssysteme (Proceedings), Informatik-Fachberichte 271, Hrsg.: Pfitzmann, A., Berlin u.a. 1991, S. 133 - 145.

Michel, U.
Sicherheitsfunktionen im paneuropäischen Mobilfunknetz, in: Verläßliche Informationssysteme, Proceedings VIS'91, Hrsg.: Pfitzmann, A. / Raubold, E., Berlin et al. 1991, S. 133 - 145.

Moayeri, Behrooz
Netzwerk-Koppelelemente im Dienste der Sicherheit, in: Datacom, 13. Jg. (1996), Heft 1, S. 68 - 73.

Mund, Sibylle / Rieß, Hans Peter
Kryptographische Protokolle für Sicherheit in Netzen, in: DuD, Jg. 1992, Heft 2, S. 72 - 80.

Munzert, Michael / Wolff, Christian
Firewalls - Schutz vor Angriffen aus dem Internet, in: DuD, Jg. 1996, Heft 2, S. 89 - 93.

Muth, Reinhard / Schäfer, Wolfgang
Telepräsenz. IT-Sicherheits-spezifische Analyse von Telearbeitsplätzen, in: DuD, Jg. 1996, Heft 10, S. 596 - 601.

Papst, Markus
OSI und Security, in: Datacom, 10. Jg. (1993), Heft 3, S. 112 - 115.

Pfitzmann, Andreas
Technischer Datenschutz in öffentlichen Funknetzen, in: DuD, Jg. 1993, Heft 8, S. 451 - 463.

Pohl, Hartmut
Sicherheit in Client/Server-Architekturen und internationalen Netzen, in: Datacom, 12. Jg. (1995), Heft 6, S. 58 - 63.

Pohlmann, Norbert
Corporate Networks, in: KES, 12. Jg. (1996), Heft 3, S. 56 - 60.

Pohlmann, Norbert
Bausteine für die Sicherheit: Chipkarten und Sicherheits-Module, in: KES, 11. Jg. (1995), Heft 5, S. 16 - 22.

Pohlmann, Norbert
Durch die Maschen geschlüpft - Risiken im Netz, in: KES, 11. Jg. (1995), Heft 4, S. 13 - 21.

Pohlmann, Norbert
Schutz von LAN's und LAN-Kopplung über öffentliche Netze, in: Datacom, 12. Jg. (1995), Heft 6, S. 50 - 56.

Pohlmann, Norbert
Vertrauliche Kommunikation über öffentliche Netze, in: Datacom, 11. Jg. (1994), Heft 8, S. 126 - 130.

Pohlmann, Norbert
Sicherheit in UNIX-Netzen, in: Datacom, 10. Jg. (1993), Heft 12, S. 122 - 129.

Pohlmann, Norbert
Das RSA-Verfahren und dessen Anwendung, in: DuD, Jg. 1990, Heft 1, S. 14 - 22.

Pohlmann, Norbert
Sicherheitsdienste in Paket-Netzen, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 473 - 490.

Popp, Ralf
A Security Architecture for Mobile Personal Communication Services, in: Mobile Kommunikation: Vorträge der ITG-Fachtagung vom 26-28.09.1995, ITG Fachbericht 135, Hrsg.: ITG, Berlin 1995, S. 423 - 432.

Pütz, Stefan
Lösungsansätze für Authentikation in künftigen Mobilfunksystemen, in: Mobile Kommunikation: Vorträge der ITG-Fachtagung vom 26-28.09.1995, ITG Fachbericht 135, Hrsg.: ITG, Berlin 1995, S. 411 - 422.

Racke, Wilhelm F.
Netzarchitekturen, in: Lexikon der Wirtschaftsinformatik, Hrsg.: Mertens Peter, 2. Aufl., Berlin, Heidelberg 1990, S. 292 - 294.

Raubold, Eckart
Sicherheitsaspekte in der „offenen" Telekommunikation, in: Entwicklungslinien der Telekommunikation: Vorträge der ITG-Fachtagung vom 21-22.01.1993, ITG Fachbericht 123, Hrsg.: ITG, Berlin 1993, S. 75 -81.

Reif, Holger
Netz ohne Angst. Sicherheitsrisiken im Internet, in: c't Magazin für Computertechnik, Jg. 1995, Heft 9, S. 174 - 183.

Reimer, Helmut
Vertrauenswürdige Kommunikation in offenen IT-Systemen, in: KES, 11. Jg. (1995), Heft 5, S. 24 - 29.

Rinderknecht, H. / Ilg, H. / Schäfer, W.
Sicherheitssystem: Biometrische Techniken, in: DuD, Jg. 1992, Heft 5, S. 241 - 243.

Roberts, D. W.
Evaluation Criteria For IT-Security, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 151 - 161.

Roßnagel, Alexander / Bizer, Johann
Multimediadienste und Datenschutz, in: DuD, Jg. 1996, Heft 4, S. 209 - 217.

Rothe, Joachim
Anwendungsaspekte von Hash-Funktionen, in: DuD, Jg. 1993, Heft 7, S. 401 - 410.

Rudeloff, Roger
IT-Sicherheitsfunktionen im ISDN, in: BSI-Forum, 2. Jg. (1994), Heft 3, S. 53 - 55.

Rueppel, Rainer A.
Clipper - Der Krypto-Konflikt am Beispiel der Amerikanischen ESCROW Technologie, in: DuD, Jg. 1994, Heft 8, S. 443 - 451.

Ruland, Christoph
Sichere Kommunikation zwischen ISDN-Endgeräten, in: Datacom, 12. Jg. (1995), Heft 1, S. 108 - 116.

Schläger, Uwe
Datenschutz in Netzen, in: DuD, Jg. 1995, Heft 5, S. 270 -275.

Schlette, Joachim
Internet - Sicherheit durch Firewalls, in: Datacom, 13. Jg. (1996), Heft 1, S. 62 - 66.

Schmidt, Werner
Datenschutz und ISDN, in: Sicherheit in Informationssystemen, Proceedings SECUNET ’91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 111 - 122.

Schopka, Klaus
Die Bedeutung der IT-Sicherheit aus betriebswirtschaftlicher Sicht, in: KES, 11. Jg. (1995), Heft 6 , S. 64 - 70.

Seidel, Ulrich
Gesetzeskonforme elektronische Unterschrift, in: Sicherheit in Informationssystemen, Proceedings SECUNET ’91, Hrsg.: Lippold, Heiko u. a., Braunschweig 1991, S. 301 - 311.

Stang, David / Becker, Lutz
Flächenbrände im Netz ?, in: Datacom, 12. Jg. (1995), Heft 6, S. 66 - 76.

Staudinger, Bernd
Anforderungen an eine zukunftsorientierte Informationssicherheit, in: BSI-Forum, 3. Jg. (1995), Heft 1, S. 62 - 64.

Staudinger, Bernd
Sicherer Datentransfer in heterogenen Netzen, in: KES, 10. Jg. (1994), Heft 2, S. 12 - 16.

Stempel, Steffen / Knobloch, Hans-Joachim
Netzwerksicherheit durch Authentifikationsverfahren, in: Spektrum der Wissenschaft, Jg. 1994, Heft 5, S. 70 - 71.

Stiegler, H. G.
Welche Sicherheit bietet ein evaluiertes System ?, in: Verläßliche Informationssysteme, Proceedings VIS'91, Hrsg.: Pfitzmann, A. / Raubold, E., Berlin et al., S. 277 - 288.

Stiel, Hadi
Löcher im Netz, in: Datacom, 13. Jg. (1996), Heft 1, S. 42 - 46.

Stiel, Hadi
Achillesferse Netzwerke, in: Datacom, 12. Jg. (1995), Heft 6, S. 44 - 48.

Stollreither, Konrad
Die Zukunft wird anders sein, in: DuD, Jg. 1996, Heft 5, S. 279 - 285.

Strohmeyer, Rolf
Die strategische Bedeutung des elektronischen Datenaustausches, dargestellt am Beispiel von VEBA Wohnen, in: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung, 44.Jg. (1992), H. 5, S. 462-475.

Ungerer, Bert
Knackfreundlich. Schnelle Online-Plattenverschlüsselung birgt Risiken, in: c't Magazin für Computertechnik, Jg. 1994, Heft 6, S. 184 - 190.

van der Giet, Gerhard
Informationssicherheit und Dienstvereinbarung beim Einsatz ISDN-fähiger Systeme, in: DuD, Jg. 1992, Heft 1, S. 21 - 26.

Vedder, Klaus
Security Aspects of Mobile Communication, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 193 - 210.

Verschuren, Jan
ISO-OSI Security Architecture, in: Computer Security and Industrial Cryptography, ESAT Course, Hrsg.: Preneel, Bart / Govaerts, René, Berlin 1993, S. 179 - 192.

Wagner, Markus
Evaluierung von IT-Systemen und Produkten nach den ITSEC, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '92, Hrsg.: Lippold, H. / Schmitz, P., Braunschweig 1992, S. 151 - 172.

Wallich, Paul
Piraten im Datennetz, in: Spektrum der Wissenschaft, Jg. 1994, Heft 5, S. 64 - 70.

Weck, Gerhard
Sicherheit von Client/Server-Systemen, in: DuD, Jg. 1995, Heft 3 - 5, S. 156 - 163, 224 - 231 u. 276 - 283.

Weimann, Jürgen
Chipkarten: Realisierungs- und Anwendungsmöglickeiten, in: DuD im Wandel der Informationstechnologien, Hrsg.: Spies, P. P., Berlin 1985, S. 26 - 32.

Widmer, Walter
Banken: Durchsetzung von Sicherheitsstandards, in: DuD, Jg. 1992, Heft 5, S. 237 - 240.

Wirtz, Brigitte
Automatische Unterschriftsverifikation, in: DuD, Jg. 1994, Heft 7, S. 385 - 395.

Witt, Martin
Heterogene Netze und Sicherheit, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET'92, Hrsg.: Lippold, Heiko / Schmitz, Paul, Braunschweig 1992, S. 443 - 458.

Wolfenstetter, Klaus-Dieter
TeleSec und Sicherheit in Telekommunikationssystemen, in: Sicherheit in netzgestützten Informationssystemen, Proceedings SECUNET '93, Hrsg.: Lippold, Heiko u. a., Braunschweig 1993, S. 445 - 462.

Publikationen im World Wide Web

Hinter dem URL (= Uniform Resource Locator) ist der Tag angegeben, an dem der Verfasser die angeführte Publikation unter der Adresse vorgefunden hat.

Brickell, E. / Denning, D. u.a.
SKIPJACK Review: The skipjack algorithm, Interim Report, 28.07.93,
URL=http:// www.cis.ohio-state.edu/hypertext/books/usenet/sj-report/sj-itrep.html:
24.11.1996

Bundesministerium für Inneres
Signaturgesetz (SigG), URL=http://www.telesec.de/siggeset.htm: 19.11.1996

Bundesministerium für Inneres
Signaturverordnung (SigV), URL=http://www.telesec.de/sigveror.htm: 19.11.1996

Chaum, David
Prepaid Smart Card Techniques, Digicash,
URL=http://www.digicash.com/publish/sciam.html: 09.02.1997

Ellermann, Uwe
Firewalls - Klassifikation und Bewertung, DFN-CERT Workshop
URL=http://www.cert.dfn.de/team/ue/fw/workshop/: 15.12.1996

Freier, Alan O. / Karlton, Philip
The SSL Protocol Version 3.0, Netscape Communications, (Expires 9/96)
URL=http://www.uni-siegen.de/security/internet/ssl.draft-freier-ssl-version3-01.txt:
19.01.1997

Gaissmaier Karl
Sicherheitsaspekte bei Dial-In Zugängen, CERT: DFN-Bericht Nr. 81,
URL=http://www.cert.dfn.de/dfn/berichte/db081/dialin/home.html: 23.11.1996

Gaissmaier, Karl
Implementation eines Firewalls unter Verwendung frei verfügbarer Software,
CERT: DFN-Bericht Nr. 78,
URL:http://www.cert.dfn.de/dfn/berichte/db078/firewall/: 23.11.1996

Litterio, Francis
Cryptography, PGP, and Your Privacy,
URL=http://world.std.com/~franl/crypto.html: 17.11.1996

RSA Laboratories
The RC5(R) Encryption Algorithm, General Information
URL=http://www.uni-siegen.de/security/krypto/rc5-rsainfo.txt: 17.11.1996

RSA Laboratories
Crypto-Challenge RSA-Wettbewerbsauschreibung
URL= http://www.rsa.com/rsalabs/97challenge/ : 09.02.1997

Schiffman, A. / Rescorla, E.
The Secure HyperText Transfer Protocol, Enterprise Integration Technologies, (Expires Jan-96), URL=http://www.uni-siegen.de/security/internet/shttp.draft-ietf-wts-shttp-00.txt: 19.01.1997

Schuhmacher, Staale
PGP, Programmbeschreibung und aktuelle Version PGP 2.6.2i
URL=http://www.ifi.uio.no/ staalesc/PGP/home.html

Telekom-Produktzentrum Telesec
Produktübesicht, Deutsche Telekom AG, Telesec,
URL=http://www.telesec.de/produkte.htm: 17.11.1996

Universität-Gesamthochschule Siegen
Data Encryption Standard, Security Server,
URL=http://www.uni-siegen.de/security/krypto/des.html: 17.11.1996

Universität-Gesamthochschule Siegen
RC5, Security Server,
URL=http://www.uni-siegen.de/security/krypto/rc5.html: 17.11.1996

Universität-Gesamthochschule Siegen
ECC, Security Server,
URL=http://www.uni-siegen.de/security/krypto/ecc.html: 17.11.1996

Universität-Gesamthochschule Siegen
Hash-Codes, Security Server,
URL=http://www.uni-siegen.de/security/krypto/shs.html: 17.11.1996

Universität-Gesamthochschule Siegen
LUC, Security Server,
URL=http://www.uni-siegen.de/security/krypto/luc.html: 17.11.1996

Universität-Gesamthochschule Siegen
IDEA, Security Server,
URL=http://www.uni-siegen.de/security/krypto/idea.html: 17.11.1996

US-Commerce Department
Export Administration Regulations, Iterim Rules
URL=http://www.eff.org/pub/Privacy/ITARexport/961230_commerce.regs: 02.02.1997

ZVEI-Pressestelle
Stellungnahme des Fachverbandes Informationstechnik im VDMA und ZVEI zum Signaturgesetz vom 25. September 1996, URL=http://www.telesec.de/fvit.htm: 19.11.1996

SELBSTÄNDIGKEITSERKLÄRUNG

„Ich versichere, daß ich die vorstehende Arbeit selbständig
und ohne fremde Hilfe angefertigt und mich anderer als der im beigefügten
Verzeichnis angegebenen Hilfsmittel nicht bedient habe.
Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen
entnommen wurden, sind als solche kenntlich gemacht."

Hamburg, 25. Februar 1997 _____

(Sönke Volquartz)