Diplomarbeit

Sichere Transaktionen für Intranet Verbindungen über das Internet durch local-Server/remote-Server Kommunikation

Diplomarbeit am Fachbereich Informatik der Universität Dortmund Lehrstuhl Informatik I

Betreuer: Dipl.-Inform. Sascha Dierkes & Prof. Dr. Bernd Reusch

Christian Fiebig

Juni 1998

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AH Authentication Header

ARP Adress Resolution Protocol

ARPA Advanced Research Projects Agency

ATM Asynchronous Transfer Mode

CA Certification Authority

CIDR Classless Internet Domain Routing

CPS Certificate Policy Statement

CRL Certificate Revocation List

DARPA Defense ARPA

DES Data Encryption Standard

DN Distinguished Name

DNS Domain Name System

DoD Department of Defense

ESP Encapsulated Security Payload

E-Mail Electronic Mail

FTP File Transfer Protocol

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

IAB Internet Architecture Board

IDEA International Data Encryption Algorithm

IEC International Electrotechnical Committee

IETF Internet Engineering Task Force

IPSP IP Security Protocol

IP Internet Protocol

ISDN Integrated Services Digital Network

ISO International Standard Organisation

IT Informationstechnik

ITU International Telecommunication Union

ITU-T ITU - Telecommunication Standardization Sector

JTC Joint Technical Committee

LAN Local Area Network

MAC Message Authentication Code

MIME Multipurpose Internet Mail Extension

NFS Network File System

NIS Network Information Service

OSI Open Systems Interconnection

PCA Policy Certification Authority

PCT Private Communication Technology

PDU Protocol data unit

PEM Privacy Enhanced Mail

PGP Pretty Good Privacy

PPP Point-to-Point Protocol

RFC Request For Comment

RSA Rivest, Shamir, Adleman

SC Sub Committee

SET Secure Electronic Transactions

S-HTTP Secure-HTTP

SMTP Simple Mail Transfer Protocol

SSL Secure Socket Layer

TCP Transmission Control Protocol

TCSEC Trusted Computer System Evaluation Criteria

TLS Transport Layer Security

TLSP TLS Protocol

UDP User Datagram Protocol

URL Uniform Resource Locator

VPN Virtual Private Network

WAN Wide Area Network

WG Working Group

WWW World Wide Web

Kapitel 1

Einleitung

Das Internet erfuhr in den letzten Monaten und Jahren einen enormen Aufschwung, der auch immer stärker durch kommerzielle Interessen geprägt wird. Mit dieser Entwicklung hat sich auch das Sicherheitsbedürfnis der angeschlossenen Organisationen stark verändert. Die Anbindung eines Systems oder auch eines Netzwerkes (bspw. Intranet) an das Internet hat aber zur Folge, daß allen Internet-Benutzern ein mehr oder weniger eingeschränkter Zugriff auf die eigenen Systeme ermöglicht wird [kyas97]. Der Dienstanbieter im Internet muß seine Systeme wenigstens teilweise zugänglich machen, um eine Nutzung der Dienste zu ermöglichen. Damit ist aber auch die Gefahr gegeben, daß Einbruchsversuche und Manipulationen an Daten von außen gegen die eigenen angeschlossenen Rechner stattfinden können. In dem Maße, wie das Internet wächst und wie es als Wirtschaftsfaktor Bedeutung erlangt, wächst auch das Gefährdungspotential durch unerwünschte Aktivitäten.

Einen Schwerpunkt des Interesses bildet dabei das WWW, da es im Vergleich zu anderen Diensten wie Gopher oder ftp relativ einfach zu bedienen ist und so von einer großen Anzahl Nutzern verwendet werden kann. Immer mehr werden so auch kostenpflichtige oder sensible Daten über das WWW weitergeleitet. Hier werden an die Kommunikation besondere Bedingungen verknüpft. Ein denkbares Szenario ist z.B. das Verbinden von mehreren Standorten einer Firma über das Internet. Da das Internet eine weltweite Infrastruktur zur Verfügung stellt, ist es als Medium zunächst gut geeignet. Es gibt ebenso kommerzielle Intranet Systeme, die auf die WWW-Technik aufsetzen und auf lokale Netze übertragen. Durch geeignete Server kann dann ein transparentes weltweites Netz realisiert werden, das die einzelnen Firmenstandorte miteinander verbindet, ohne daß dies für einen Benutzer sichtbar wäre. Dies hat den Vorteil, daß firmeneigene Informationsdienste weltweit zur Verfügung stehen, für den Benutzer allerdings keine Probleme hinsichtlich der Bedienung auftreten. Eine solche weltweite Vernetzung über das Internet ist mit großen Sicherheitsrisiken behaftet. Dazu gehört das

Abhören von Information, das unerlaubte Eindringen in das Firmennetz, sowie das Vortäuschen eines Firmenservers über das Internet. Ähnliche Probleme treten auch beim Anbieten kostenpflichtiger Daten auf. Beim Abhören von Verbindungen, können andere Parteien an kostenpflichtige Information[1] gelangen, ohne dafür zu bezahlen, oder durch Vortäuschen eines Informationsdienstes durch Dritte kann gezielt falsche Information weitergegeben und so u.a. auch das Vertrauen in den Anbieter erschüttert werden. Ebenso könnte ein Angreifer versuchen die Identität eines Kunden vorzutäuschen, um so auf dessen Kosten an die Datenbestände zu gelangen. Ein weiterer Punkt ist die Sicherheit eines Abrechnungssystems. Es muß gewährleistet sein, daß weder der Anbieter dem Kunden nicht geleistete Dienstleistungen in Rechnung stellt, noch daß der Kunde in Anspruch genommene Dienstleistungen leugnen kann.

Ziel dieser Arbeit ist es ein Konzept für einen modularen Server zu entwickeln und diesen in seinen Grundzügen zu realisieren, um einerseits eine größtmögliche Sicherheit gegenüber den unterschiedlichen Angriffsarten zu ermöglichen und andererseits die Kosten dafür durch ein globales Konzept möglichst gering zu halten.

Im folgenden Kapitel 2 werden technologische Ursprünge erläutert, die maßgeblich an der Entwicklung des Internet bzw. Intranet beigetragen haben. Über die Darstellung des OSI-Referenzmodells und die Erläuterung der Protokollfamilie TCP/IP werden gängige Dienste im Internet wie das World Wide Web angesprochen. In Kapitel 3 werden Grundlagen aufgezeigt, die sich mit allgemeinen Sicherheitsproblemen in IT-Systemen befassen. Hier werden speziell Angriffspunkte und Schwachstellen aufgezeigt. Ferner werden erste Lösungsansätze, wie Firewallsysteme und kryptographische Grundlagen erläutert. Im folgenden Kapitel 4 wird über den Entwurf eines modularen Servers diskutiert, der gewisse Sicherheitsdienste und Sicherheitsmechanismen betrachtet. Kapitel 5 zeigt dann eine mögliche technische Realisierung dieses Konzeptes, wobei hier speziell auf den Server Jigsaw eingegangen wird. Im abschließenden Kapitel 6 wird eine Zusammenfassung der betrachteten Materie und ein kleiner Ausblick gegeben.

[1] Da Information keine exakt quantifzierbare Größe ist, gibt es auch den Plural „Informationen“ nicht. Es gibt nur mehr oder weniger Information [fuhr96].

Kapitel 2

Ursprünge

2.1 Historie

Das heute bekannte Internet nahm seinen Ursprung im Jahre 1957 [hobb98]. Damals gründete das US Verteidigungsministerium (Department of Defense, DoD) die Advanced Research Projects Agency (ARPA), um die Führung in Wissenschaft und Technologie im militärischen Bereich zu gewährleisten. Die Aufgabe der ARPA (seit 1972 Defense ARPA (DARPA)) bestand darin, ausgewählte Forschungsprojekte durch Zuteilung finanzieller Mittel zu fördern.

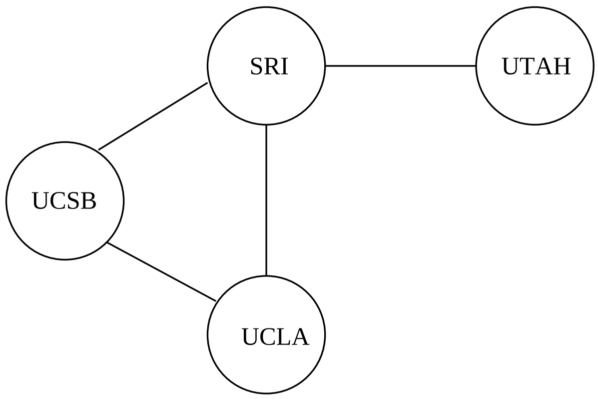

Abbildung 2.1: ARPANET, Dezember 1969

Eines dieser Forschungsprojekte war ein Programm namens *Recource Sharing Computer Networks* des IPTO (Information Processing Techniques Office), also die mögliche gemeinsame Nutzung aller im Netz vorhandenen Ressourcen. Man erkannte schnell das militärische Potential von Computernetzen und es entstand das ARPANET, welches den ältesten Bestandteil des Internet darstellt. Wie in Abbildung 2.1 zu erkennen ist, startete das ARPANET mit vier Knoten [ahuj96], das zunächst die Universitäten von Los Angeles (UCLA), Santa Barbara (UCSB) und Utah, sowie das Standford Research Institute (SRI) miteinander verband.

Nachdem das Netz 1972 der Öffentlichkeit vorgestellt wurde, schlossen sich viele Universitäten und Forschungseinrichtungen an das ARPANET an, aus dem sich im weiteren Verlauf das Internet entwickelte. Eine direkte Folge der Entstehung aus dem ARPANET ist auch die Robustheit des Internet. Das ARPANET wurde dezentral organisiert, damit es beim Ausfall von Teilen (aus militärischer Sicht z.B. durch einen Atomschlag) als Ganzes immer noch funktionstüchtig war.

Einen weiteren Meilenstein in der Entwicklung des Internet stellte 1982 die Einführung einer neuen Generation von Netzwerkprotokollen, u.a. der beiden Protokolle TCP (Transmission Control Protocol) und IP (Internet Protocol), dar. Da alle Spezifikationen in frei zugänglichen Dokumenten, den sogenannten RFCs (Request For Comment) beschrieben sind, stellt es für einen Programmierer kein Problem dar, eigene Netzwerk-Anwendungen auf der Basis von TCP/IP zu entwickeln. Zudem wurde bei der Spezifikation auf ein Höchstmaß an Portabilität geachtet, so daß TCP/IP nicht auf einen bestimmten Rechnertyp beschränkt ist.

Der Name Internet entstand 1983 als das ARPANET in zwei Teile unterteilt wurde, das ARPANET und das MILNET. Die zentrale Koordination liegt beim NOC (Network Operation Center).

Das WWW (World Wide Web) entstand am Europäischen Forschungszentrum für Teilchenphysik, CERN (Center of Nuclear Research), in Genf unter der Leitung des britischen Informatikers Dr. Tim Berners-Lee [klut96]. Die Projektplanung begann im März 1989 und sah ursprünglich ein Hypertextsystem für Hochenergiephysiker in aller Welt vor. Diese sollten die Möglichkeit erhalten, beispielsweise ihre Forschungsberichte per WWW ihren Kollegen in aller Welt verfügbar zu machen und sie über Hypertextlinks mit anderen Dokumenten verknüpfen zu können (siehe auch Kapitel 2.5). Gegen Ende 1990 konnte das Entwicklungsteam um Berners-Lee einen Prototypen für NEXTStep sowie eine einfache zeilenorientierte Anwendung im CERN vorstellen.

Nachdem die Leitung des CERN im März 1994 das WWW als offizielles CERN-Projekt anerkannt hatte, kam es Ende Juli 1994 zur Gründung der W3-Organisation (W3 Consortium: http://www.w3.org), die für die Standardisierung und weitere Entwicklung des WWW verantwortlich ist.

Das öffentliche Internet, auf dessen Basis sich die heutigen Intranets entwickelten, ist ein Datennetz mit weltweiter Ausdehnung, bestehend aus hierarchisch strukturierten Datenmietleitungen. Transkontinentalkabel (Seekabel) und Satelliten verbinden dabei die Hauptverbindungswege (Backbones) der Kontinente, an welche sich nationale und regionale Internetdienstleister (Provider) anschließen. Die Internetprovider stellen für Internetkunden Einwahlknoten (POP: Point of Presence) zur Verfügung, über die der eigentliche Anschluß an das Internet erfolgt. Das Transportprotokoll im Internet ist einheitlich TCP/IP, auf dessen Basis die unterschiedlichen Anwendungsprogramme realisiert sind. Die Funktionen, die den einzelnen Benutzern heute im Internet zur Verfügung stehen, reichen von elektronischer Post (E-Mail) bis hin zu Echtzeit-Audio und -Video.

2.2 Technische Grundlagen des Internet

Allgemein spricht man von einem Rechnernetz, wenn mehrere unabhängige Rechner so miteinander verbunden sind, daß sie Information austauschen können [barz91]. Um erfolgreich Information austauschen zu können, ist es notwendig, daß jeder Rechner eine eindeutige Adresse besitzt, mittels der er angesprochen werden kann. Zudem muß innerhalb des Rechnernetzes ein Protokoll festgelegt werden, das die Kommunikation zwischen den einzelnen Rechnern regelt. Als Internet wird die Verbindung all jener Computer bezeichnet, die über das Protokoll TCP/IP miteinander kommunizieren [maie95]. Die zentrale Vergabe der Internet-Adressen geschieht dabei durch den InterNIC Registration Service bzw. durch einen regionalen Unterverteiler. Nach [sand96] muß ein Rechner (Host) drei Kriterien erfüllen, damit er zum Internet gehört:

1. Er muß in der Lage sein, mit anderen Rechnern mittels TCP/IP zu kommunizieren.

2. Er muß eine, ihm vom InterNIC Registration Service zugewiesene Internet-Adresse besitzen.

3. Er muß mit allen Rechnern kommunizieren können, die eine, ihnen vom InterNIC Registration Service zugewiesene Internet-Adresse besitzen.

Der Anschluß von Rechnernetzen an das Internet erfolgt über einen einzelnen Rechner, der schon Bestandteil des Internet ist und Gateway (engl.: Einfahrt) genannt wird. Hierbei muß vorher für jeden in diesem Rechnernetz vorhandenen Rechner eine eigene Internet-Adresse beantragt worden sein.

Das Internet ist somit weniger eine Verbindung zwischen einzelnen Rechnern, sondern vielmehr eine Verbindung zwischen unabhängigen Teilnetzen, daher wird das Internet auch als „Netz der Netze“ bezeichnet.

Da es sich bei TCP um ein verbindungsorientiertes Protokoll handelt, muß vor dem Datenaustausch eine logische Verbindung zwischen den beiden kommunizierenden Rechnern aufgebaut werden.

Abbildung 2.2 zeigt die Anschlußmöglichkeiten von Rechnern bzw. Rechnernetzen an das Internet.

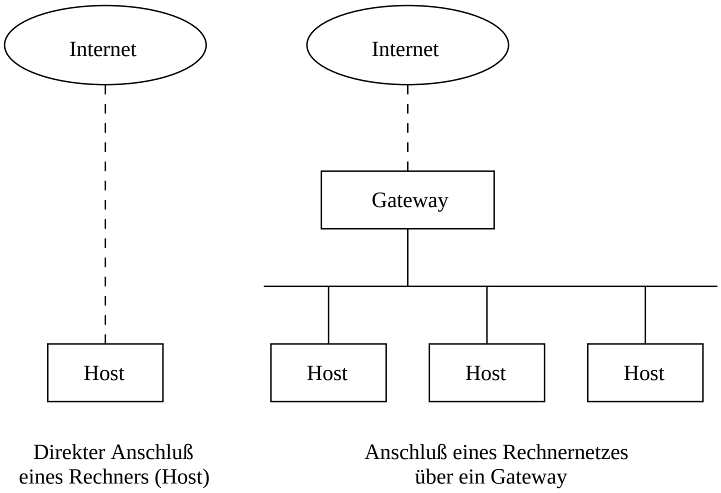

Abbildung 2.2: Anschluß von Rechnernetzen an das Internet

2.3 Datenübertragung im Internet

Eine genauere Betrachtung der Bezeichnung Internet stellt einen guten Einstieg zum Verständnis der technischen Hintergründe des weltweiten Netzwerkverbundes dar. Der Begriff weist bereits darauf hin, daß das Internet nicht mit einem bestimmten Datenübertragungsverfahren oder einer bestimmten Netzwerkarchitektur gleichzusetzen ist. Ziel des Internet ist vielmehr, die Basis für weltweiten Zugriff auf Dienste und für den Austausch von Information, aufbauend auf bestehende Telekommunikationsinfrastrukturen zu bieten. Diese grundlegende Idee der Internet-Technik wird durch einen beispielhaften Ausschnitt aus einer Netzwerk-Infrastruktur in Abbildung 2.3 illustriert.

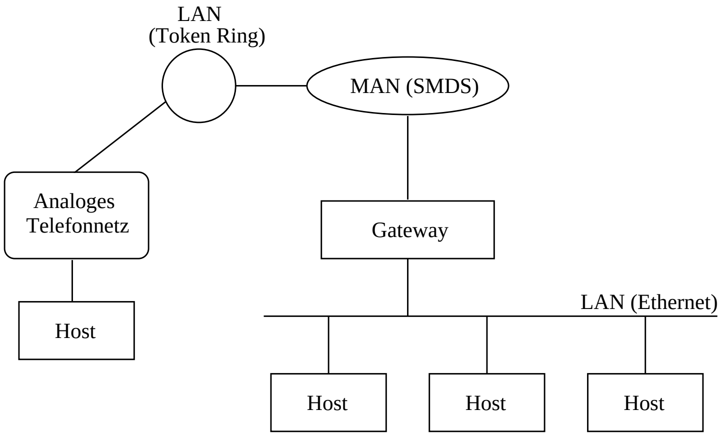

Abbildung 2.3: Datenübertragung im Internet

Abbildung 2.3 zeigt, in welcher Form die diversen Datenübertragungsverfahren in unterschiedlichen Anwendungsgebieten zum Einsatz kommen können. Der hier dargestellte Ausschnitt umfaßt zwei lokale Netze, die durch ein öffentliches Netzwerk miteinander verbunden sind. Dabei kommen unterschiedliche Verfahren zum Einsatz. Im lokalen Bereich werden die LAN-Protokolle Ethernet und Tokenring verwendet. Im Weitverkehrsbereich bedient man sich eines öffentlichen Telekommunikationsnetzes auf der Basis des Standards SMDS (Switched Multimegabit Data Service). Solche Netze werden typischerweise von großen Telekommunikationsfirmen betrieben, welche unterschiedliche Zugänge zur Netzwerkinfrastruktur als Dienstleistung an ihre Kunden verkaufen.

Eines der beiden in Abbildung 2.3 skizzierten lokalen Netze bietet außerdem einen Zugang über das öffentliche Fernsprechnetz an. Der Einsatz von Modems auf beiden Seiten ermöglicht die Übertragung von digitaler Information auch über das analoge Telefonnetz. Diese Technik wird in der beschriebenen Form von Internet-Providern eingesetzt, um private Haushalte sowie Unternehmen einen Zugang zum Internet zu ermöglichen.

Alle diese Übertragungstechniken weisen unterschiedliche Charakteristika auf. Sie unterscheiden sich in Parametern wie der maximal überbrückbaren Distanz, der erzielbaren Übertragungsgeschwindigkeit, der Auswirkung von hohem Verkehrsaufkommen im Gesamtnetz auf die Transferrate einer einzelnen Verbindung oder der Geschwindigkeit des Verbindungsaufbaus (vgl. [hans96, fitz95]).

Auf eine genauere Beschreibung der Eigenschaften von Telekommunikationsdiensten und LAN-Protokollen gehen [ehle94, cont97, kern89] ein. Die erwähnten Übertragungsverfahren stellen ein Transportmittel für die Internet-Protokolle dar; diese können losgelöst vom zugrundeliegenden Übertragungsmechanismus betrachtet werden.

2.4 Datenübertragung und das OSI-Referenzmodell

Offene Systeme zeichnen sich durch normierte Schnittstellen, Dienste und Protokolle aus. Aufgrund ihrer Vorteile in Bezug auf Konnektivität, Interoperabilität und Benutzerfreundlichkeit ist heute ein starker Trend hin zu offenen Systemen spürbar. Allerdings stehen diesen Vorteilen auch Nachteile in Bezug auf die Sicherheit gegenüber. Der Konflikt zwischen Offenheit und Sicherheit liegt auf der Hand und ist in der Regel nur schwer aufzulösen [shaf94].

Im Bereich der IT arbeiten die International Organization for Stadardization (ISO) und das International Electrotechnical Committee (IEC) im Rahmen eines Joint Technical Committees 1 (JTC1) eng zusammen. Innerhalb des ISO/IEC JTC1 befassen sich verschiedene Unterkomitees (sub committees, SCs) und Arbeitsgruppen (working groups, WGs) mit Fragen der IT-Sicherheit [ford94].

2.4.1 Grundlagen von Netzwerkprotokollen

Schon vor der Veröffentlichung des OSI-Referenzmodells sprach man im Zusammenhang mit der Architektur von Netzwerkprotokollen oft von Schichten (engl.: Layer) [hals88]. So ist es einsichtig, daß gewisse Teile, der zur Datenübertragung notwendigen Software, Bestandteil des Betriebssystems sind, während andere, anwendungsspezifische Teile, in die einzelnen Netzwerkapplikationen integriert sind. Eine E-Mail-Software integriert beispielsweise zwar die notwendige Funktionalität, um eine Nachricht nach den am Internet gültigen Konventionen aufzubauen, die Fragmentierung der Nachricht in Pakete übernimmt jedoch die Netzwerksoftware.

Zur Übertragung dieser in Pakete zerstückelten Nachricht bedarf es ferner eines *Kommunikationspartners*. Bei diesem findet der im letzten Absatz beschriebene Vorgang in umgekehrter Reihenfolge statt. Die einzelnen Pakete werden von der Netzwerksoftware defragmentiert, in der ursprünglichen Reihenfolge wieder zusammengesetzt und dann der E-Mail-Software übergeben. Diese wiederum ist in der Lage, die empfangene Nachricht in ihre Bestandteile zu zerlegen und diese Information – Absender, Empfänger, Datum und Nachricht – auf benutzerfreundliche Art und Weise zu präsentieren.

Man kann erkennen, daß sich die Funktionalität der Datenübertragung in Schichten einteilen läßt. An oberster Stelle befindet sich die Anwendung mit ihren konkreten Kommunikationsanforderungen, an unterster Stelle befindet sich das Übertragungsmedium, das physische Netzwerk. Beim Sendevorgang bedient sich jede Schicht der Funktionalität der darunterliegenden Ebene. Beim Empfangsvorgang werden die empfangenen Daten durch die Schichten nach oben weitergereicht.

Ein *Netzwerkprotokoll* legt die Regeln für die Kommunikation zwischen den Teilnehmern fest. Solche Standards beinhalten typischerweise das Format der übertragenen Daten und die exakte Beschreibung des Auf- und Abbaus der Verbindung [gasm94].

Diese Definitionen gelten jeweils für eine bestimmte Schicht. Betrachtet man wiederum das Beispiel der E-Mail-Software, so sind zur Übertragung einer Nachricht mehrere Protokolle erforderlich. Auf Anwendungsebene wird das Format der Nachricht definiert, auf der Ebene der Netzwerksoftware werden der Aufbau und die Länge der Pakete standardisiert und auf der untersten Schicht beispielsweise die konkreten Spannungsunterschiede des Übertragungsmediums festgelegt. Bedenkt man, daß auf all diesen Ebenen Hard- und Software unterschiedlicher Hersteller zum Einsatz kommen können, so wird die Bedeutung von Netzwerkprotokollen klar. Der große Vorteil der konsequenten Trennung der Netzwerkfunktionalität in unterschiedlichen Ebenen liegt in der Unabhängigkeit der anwendungsnahen Software von Änderungen in der Übertragungstechnik. Wann immer also von einem Netzwerkprotokoll die Rede ist, dann ist es unumgänglich, auch die entsprechende Ebene anzugeben, auf der dieses Protokoll das Zusammenspiel der Kommunikationspartner standardisiert.

Das Beispiel der E-Mail-Applikation zeigt bereits drei mögliche Ebenen. Im Zusammenhang mit den Internet-Protokollen spricht man üblicherweise von vier Schichten (vgl. Kapitel 2.4.5), während das im folgenden Abschnitt kurz vorgestellte OSI-Referenzmodell sieben Schichten umfaßt.

2.4.2 OSI-Referenzarchitektur

Das von der ISO 1977 in Zusammenarbeit mit nationalen Normungsgremien entwickelte Modell zur Rechnerkommunikation war als Basis für zukünftige Implementierungen gedacht. Obwohl es heute einige Protokolle gibt, die sich strikt am Aufbau des Open Systems Interconnection (OSI) Referenzmodells orientieren, fand das Konzept keine weitläufige Verbreitung. Insbesondere lassen sich auch die bereits vor der Veröffentlichung des OSI-Modells entstandenen Internet-Protokolle nicht reibungslos in das Schema einordnen. Grund für die mangelhafte Akzeptanz der OSI-Standards war wohl die hohe Komplexität der einzelnen Spezifikationen und der langsame Standardisierungprozeß.

Das OSI-Referenzmodell setzt sich aus sieben Schichten zusammen, die jeweils für bestimmte Aufgaben zuständig sind und der nächst höheren Schicht an definierten Schnittstellen entsprechende Dienstprimitive (engl.: service primitives) zur Verfügung stellen.

In Abbildung 2.4 sind die sieben Schichten des OSI-Referenzmodells schematisch dargestellt. Die Aufgaben der Schichten lassen sich folgendermaßen zusammenfassen:

1. Auf der Bitübertragungsschicht (engl.: physical layer) findet die eigentliche Übertragung der elektrischen und optischen Signale über die physikalischen Medien statt.

2. Die Sicherungsschicht (engl.: data link layer) ist für die Aufteilung der Daten in Blöcke und für die sichere und fehlerfreie Übertragung dieser Blöcke zuständig.

3. Die Vermittlungsschicht (engl.: network layer) ist sowohl für die Wegwahl als auch für die Flußkontrolle in Überlastsituationen zuständig.

Abbildung 2.4: Das OSI-Referenzmodell

4. Die Transportschicht (engl.: transport layer) bietet einen von den Übertragungsmedien und -netzen unabhängigen Übertragungsdienst an.

5. Die Sitzungsschicht (engl.: session layer) ist für den Aufbau, die Durchführung und Synchronisation, sowie den Abbau von Sitzungen zuständig.

6. Die Darstellungsschicht (engl.: presentation layer) regelt die systemweite einheitliche Darstellung von Daten.

7. Schließlich laufen auf der Anwendungsschicht (engl.: application layer) die eigentlichen Applikationsprozesse.

Zwei Systeme kommunizieren „schichtweise“ miteinander, d.h. die Schicht N von System A kommuniziert mit Schicht N von System B (N=1,...,7). Ein Protokoll beschreibt dabei die Syntax und Semantik der dabei ausgetauschten Daten, sowie die Art und Weise, wie dieser Austausch zu erfolgen hat. Jede Nachricht, die im Rahmen eines (N)-Protokolls übertragen wird, wird als (N)-Protokolleinheit (protocol data unit, PDU) bezeichnet [oppl97].

Ein Vorteil des OSI-Modells ist die Schaffung einer international klar abgegrenzten Terminologie und eines Rahmens, der eine eindeutige Diskussion über die Architektur unterschiedlicher Netzwerkprotokolle ermöglicht.
Aus diesem Grund wird auch in der vorliegenden Arbeit die Funktionalität der Internet-Protokolle und deren abgesicherter Erweiterungen anhand des OSI-Referenzmodells beschrieben.

2.4.3 UNIX und das Kommunikationsprotololl TCP/IP

Als im Jahr 1969 das ARPANET in Betrieb ging, begann im AT&T Forschungszentrum Bell-Laboratories die Entwicklung eines neuen Betriebssystems, das sich vor allem durch Multi-User-Fähigkeit von bisherigen Betriebsystemen unterschied: UNIX. Ursprünglich als Programmierumgebung für Softwareentwickler gedacht, stellte die Universität von Kalifornien in Berkeley die Version 4.2 ihrer UNIX-Implementation vor (4.2 BSD UNIX), die erstmals als integraler Bestandteil auch das im selben Jahr im Internet eingeführte Kommunikationsprotokoll TCP/IP enthielt. Diese Version war frei kopierbar und erlangte nicht zuletzt deshalb eine sehr weite Verbreitung. Daten konnten nun nicht mehr nur mit Hilfe von Modems ausgetauscht werden, sondern wesentlich schneller und zuverlässiger mit dem Protokoll TCP/IP über das Internet oder über lokale Netzwerke.

2.4.4 Protokollfamilie TCP/IP

Wie bereits erwähnt werden mit dem Begriff Internet all diejenigen Rechner bezeichnet, die in der Lage sind, mit Hilfe der Netzwerkprotokolle TCP/IP zu kommunizieren. Die Bezeichnug weist bereits auf die zentrale Rolle des Internet Protocol (IP) und des Transmission Control Protocol (TCP) hin. Der Großteil der Internet-Dienste bedient sich dieser beiden Nertzwerkprotokolle als Grundlage, weswegen die darauf aufbauenden Protokolle der Anwendungsebene auch oft als Protokollfamilie TCP/IP oder TCP/IP-Protokolle bezeichnet werden. Im weiteren Verlauf dieser Arbeit ist mit dem Begriff Internet-Protokolle stets die gesamte Protokollfamilie gemeint.

Um den konzeptionellen Aufbau der Internet-Protokolle zu verstehen, ist es wichtig, die Zielsetzung beim Entwurf dieser Technik zu betrachten. Der Zweck, den die Entwickler der Internet-Protokolle verfolgten, war die Verbindung von Rechnern unterschiedlicher, paketorientierter Netzwerke. Daraus ergeben sich bereits wichtige Charakteristika der Protokollfamilie TCP/IP [come93].

- Unabhängigkeit vom physischen Übertragungsmedium und dem eingesetzten Protokoll auf der Sicherungsebene. Die Internet-Protokolle können über Kupferkabel oder Glasfaserkabel genauso betrieben werden wie über Satellitenfunk oder Richtfunkstrecken. TCP/IP läßt sich sowohl über die LAN-Protokolle Ethernet und Token-Ring als auch über zahlreiche WAN-Protokolle einsetzen. Diese Eigenschaft hat es den Internet-Protokollen erlaubt, von der Vielzahl von Neuentwicklungen im Bereich der Datenübertragung profitieren zu können.

- Grundlage der Internet-Protokolle sind offene Standards, die unabhängig von spezieller Hardware oder einem bestimmten Betriebssystem entwickelt wurden. Auch wenn mittlerweile kommerzielle Internet-Dienste diesen Trend nicht mehr unbedingt Folge leisten, so kann doch der Kern der Internet-Protokolle ohne Lizenzgebühren von jedem Hersteller implementiert werden. Folglich gibt es mittlerweile TCP/IP-Software für nahezu alle Betriebssysteme. Gleiches gilt auch für die zugrundeliegende Hardware. Vom Netzwerkdrucker über den Arbeitsplatzrechner bis hin zur Multiprozessor-Workstation finden heute die Internet-Protokolle ihren Einsatz bei allen Komponenten, die in ein Netzwerk integrierbar sind. Folglich ist TCP/IP eine gute Ausgangsbasis zur Verbindung von heterogenen Systemen.

- Teil des Internet-Protokolls ist ein weltweit einheitlicher Adressierungsmechanismus. Dieser erlaubt es, jedem Rechner mit Internet-Anschluß mit jedem anderen Rechner des Netzwerkes kommunizieren zu können.

- Schließlich beinhaltet die Protokollfamilie TCP/IP bereits zahlreiche Protokollstandards der Anwendungsebene. Diese bilden eine konsistente Grundlage für die gängigsten Internet-Dienste. Die meisten Implementierungen der Internet-Protokolle enthalten daher auch Programme zur Abwicklung von E-Mail oder elektronischen Dateitransfer, die durch die frühzeitige Standardisierung der Protokolle weltweit Interoperabilität bieten.

Die im kommerziellen Einsatz auftretenden Ansprüche an die Übertragungssicherheit waren bei der Entwicklung der Internet-Technik kein vorrangiger Aspekt. Zwar wurde auf die Ausfallsicherheit der Technik großes Augenmerk gelegt, verschlüsselte Übertragung oder verläßliche gegenseitige Identifizierung war bei der Entwicklung der Internet-Protokolle noch kein Thema von Bedeutung.

2.4.4.1 Standardisierungsprozeß

Die Weiterentwicklung der Internet-Technik wird von einem zentralen Gremium, dem *Internet Architecture Board (IAB)*, koordiniert. Die Hauptrolle bei der Entwicklung und Standardisierung neuer Techniken übernimmt die *Internet Engineering Task Force (IETF)*. Der Standardisierungsprozeß selbst findet in Form von Arbeitsgruppen (engl.: Working Groups, WG) statt. Der Zugang zu diesen Arbeitsgruppen ist nicht beschränkt, Teilnehmer können Vertreter von Unternehmen oder Universitäten sein. Die Koordination der Aktivitäten einer Arbeitsgruppe kann beispielsweise über E-Mail und mit Hilfe sogenannter Internet-Drafts erfolgen.

Diese *Internet-Drafts* sind formlose schriftliche Entwürfe, die den entsprechenden Arbeitsgruppen als Diskussionsgrundlage dienen. Als Folge sind Internet-Drafts häufig Änderungen unterworfen und das Spektrum möglicher Inhalte reicht von zukünftigen Standards bis zu Ideen, die eventuell wieder verworfen werden.

Das IAB übernimmt ferner auch die Wartung und Herausgabe der zentralen Standarddokumente des Internet: Die *Requests For Comments (RFC)*. Diese Dokumente definieren Protokolle, Verfahren oder auch Leitfäden für bestimmte Problembereiche. Ein RFC kommt erst zustande, nachdem ein entsprechender Entwurf eine Begutachtungsperiode überdauert hat [hobb98]. Nahezu alle Schlüsseltechniken des Internet sind in Form von RFCs definiert – als Beispiel definiert RFC 791 das Internet-Protokoll selbst [post81].

2.4.5 Aufbau der Internet-Protokolle

Während das im vorrangegangenen Abschnitt beschriebene OSI-Referenzmodell in sieben Schichten aufgebaut ist, werden die Internet-Protokolle üblicherweise anhand von drei bis fünf Schichten dargestellt. In dieser Arbeit wird das vierschichtige Modell von Hunt eingesetzt, um den Aufbau der Protokolle zu illustrieren [hunt92].

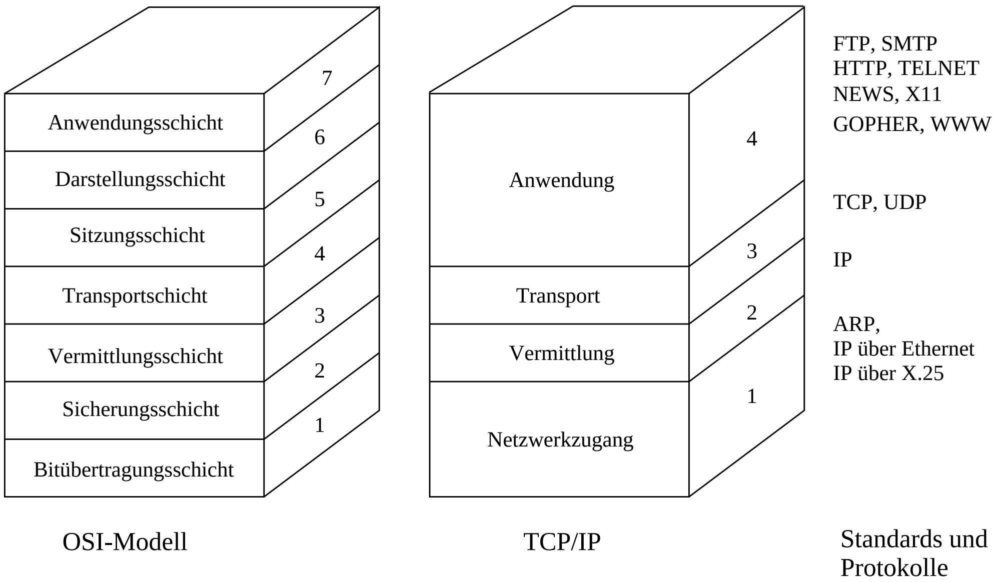

Abbildung 2.5: TCP/IP und das OSI-Referenzmodell

Eine Gegenüberstellung zu den sieben Schichten zeigt Abbildung 2.5. Man erkennt, daß die Internet-Protokolle in den zwei Randbereichen des Schichtenmodells weniger ausführlich sind als das OSI-Modell.

Dies entspricht durchaus der Realität: Im Bereich der Bitübertragungsschicht gibt es keine Standards der Protokollfamilie TCP/IP, da eben diese Unabhängigkeit von der eingesetzten Übertragungstechnik ein wesentliches Ziel bei der Entwicklung der Internet-Protokolle war. Die Verbindung von unterschiedlichen Netzen ist, wie bereits erwähnt, der zentrale Gegenstand der Protokolle.

Im oberen Bereich des OSI-Schichtenmodells wäre auch für die Internet-Protokolle, die einige Jahre später von der ISO vorgeschlagene Schichtenaufteilung, von Vorteil gewesen. Der vorgesehene Funktionsumfang muß im Fall der Internet-Dienste von den Anwendungen selbst übernommen werden. Beispielsweise definieren sowohl die Terminalemulation TELNET als auch FTP (File Transfer Protocol), ein eigenes Sitzungsmanagement und müssen somit die Funktionalitäten der OSI-Ebene fünf als Bestandteil der Applikationssoftware implementieren.

In weiterer Folge werden die Funktionalität des Transportsystems der Internet-Protokolle, also der drei unteren Schichten, beschrieben und die inhärenten Sicherheitsrisiken aufgezeigt. Im nächsten Abschnitt geht es um das Internet-Protokoll selbst, den Kernbestandteil des Protokoll-Stacks TCP/IP.

2.4.6 Internet-Protokoll (IP)

Das Internet-Protokoll ist die unterste einheitliche Schicht jeder Kommunikation über das Internet. Abbildung 2.5 zeigt die zentrale Stellung von IP als Protokoll auf der Vermittlungsebene. In dem entsprechenden Standard werden mehrere bedeutsame Aspekte des Internet in seiner heutigen Form festgelegt.

- Die Gestalt der Internet-Adresse und damit die Größe des verfügbaren Adreßraumes wird durch die Struktur des IP-Datagrammes determiniert.
- Die Integration der Netzwerk-Adresse in die IP-Adresse ist die Grundlage der Routenwahl des Internet-Protokolls, die der zentrale Gegenstand der Vermittlungsschicht ist.
- Es ist Aufgabe des Internet-Protokolls, Datagramme, deren Größe das maximale Ausmaß eines Rahmens des darunterliegenden Protokolls der Datensicherungsschicht überschreitet, in kleinere Einheiten zu fragmentieren. Auf diese Weise werden die Eigenschaften der darunterliegenden Ebene möglichst gut vor den darüberliegenden Schichten verborgen.
- Die verbindungslose Natur des Internet-Protokolls wird durch das Fehlen jeglicher Spezifikation zum Verbindungsaufbau (engl.: Handshake) oder zur Fehlerkontrolle unterstrichen. Diese oft benötigte Funktionalität wird jedoch von TCP, dem darüberliegenden Protokoll der Transportschicht, zur Verfügung gestellt. Aus dieser häufigen Kombination resultiert auch der Name der Protokollfamilie: TCP/IP.

Aus dem Blickwinkel der Sicherheit sind vor allem zwei Aspekte von Bedeutung: Der Aufbau eines IP-Datagrammes sowie der Vorgang der Routenwahl.

2.4.6.1 IP-Datagramm

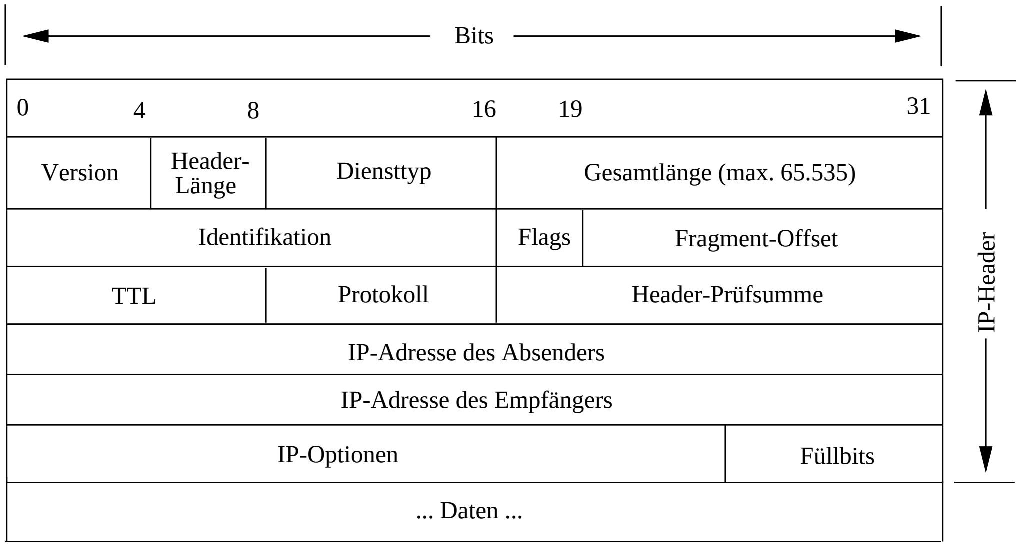

Abbildung 2.6: IP-Datagramm

Da das Internet-Protokoll kein verbindungsorientiertes Netzwerkprotokoll ist, müssen in jedem Datagramm die gesamten Adreßinformationen enthalten sein, die notwendig sind, um den Zielrechner zu erreichen. Abbildung 2.6 zeigt den Aufbau eines IP-Datagramms, wobei einige Felder besonders hervorgehoben sind. Jedes Datagramm beginnt mit Protokollinformation, die als Protokollkopf (engl.: Header) bezeichnet werden. Dieser besteht aus sechs Wörtern zu je vier Byte. Aus den Feldern eines Datagrammes kann man die Version des Internet-Protokolls ebenso ersehen wie die Gesamtgröße des Datagrammes. Letztere ist wegen des dafür vorgesehenen Platzes auf etwa 64 KB (Kilo Byte) beschränkt.

Ein weiterer Bestandteil ist das TTL-Feld (Time-To-Live). Der in diesem Feld enthaltene Wert wird von jedem Router, der an der Weiterleitung des Datagrammes beteiligt ist, dekrementiert. Wird der Wert Null erreicht, so kommt es zur automatischen Vernichtung des Datagrammes. Auf diese Weise kann verhindert werden, daß Datagramme aufgrund von Konfigurationsfehlern ewig im Internet kreisen.

Das Protokoll-Feld legt schließlich fest, wie die im Datagramm enthaltenen Daten interpretiert werden, also welchem Protokoll der Transport-Ebene das Datagramm angehört – in den meisten Fällen handelt es sich dabei um die Protokolle TCP oder UDP (User Datagram Protocol).

Abschließend folgen die IP-Adressen des Absenders und des Empfängers, die zur korrekten Zustellung des Paketes notwendig sind. Die hier nicht näher beschriebenen Felder bestehen aus einigen Flags, einer zur Refragmentierung not-

Adress-klasse	Größe der Netzwerk-adresse	Größe der Benutzer-adresse	Anzahl der Netzwerke (theoretisch)	Anzahl der Benutzer pro Netzwerk
A	7 Bits	24 Bits	128	16.777.214
B	14 Bits	16 Bits	16.384	65.534
C	21 Bits	8 Bits	2.097.152	254

Tabelle 2.1: Adreßklassen im Internet

wendigen Kennung, einer Prüfsumme über den Header, sowie einem Feld mit der Header-Länge, die unter gewissen Umständen von dem in Abbildung 2.6 dargestellten Umfang abweichen kann [bada94].

2.4.6.2 Internet-Adresse

Die Gestalt der Internet-Adresse oder IP-Adresse geht bereits auch aus Abbildung 2.6 hervor. Im Header jedes Datagrammes sind jeweils vier Byte für die Adressen des Absenders und Empfängers vorgesehen, eine IP-Adresse entspricht somit vier Zahlen in der Größenordnung zwischen 0 und 255. Diese Adresse läßt sich in drei Komponenten unterteilen.

Die *Netznummer* gibt während des Routing-Vorgangs Aufschluß darüber, wo sich das gesuchte Zielnetz befindet. Die Netznummer wird von der zuständigen Vergabestelle auf Antrag zugewiesen, was im kommerziellen Einsatz zumeist einer Zuteilung durch den Internet-Provider gleichkommt. Netznummern gibt es in drei verschiedenen Klassen, die sich in der maximalen Anzahl von Rechnern unterscheiden, an die eine gültige IP-Adresse vergeben werden kann. Wie in Tabelle 2.1 zu erkennen, unterscheidet man die Klassen A, B und C [birm96].

- Adressen der *Klasse A* ermöglichen den Anschluß von über 16 Millionen Rechnern. Weltweit gibt es 126 derartige Adressen, die bereits alle vergeben sind.

- Adressen der *Klasse B* unterstützen etwa 65.000 Rechner mit gültigen IP-Adressen. Solche Adressen sich mittlerweile auch nicht mehr verfügbar, weltweit gibt es nur 16.382 derartige Netznummern.

- Adressen der *Klasse C* erlauben die Bildung von maximal 254 gültigen Internet-Adressen. Weltweit gibt es über zwei Millionen derartige Netznummern, die auch noch erhältlich sind.

Der verbleibende Adreßbestandteil – ein, zwei oder drei Byte der gesamten Internet-Adresse – steht dem Antragstellenden zur Verfügung, der nach eigenem Ermessen bis zur maximalen Anzahl gültige IP-Adressen vergeben kann.

Dies kann für einige Antragsteller nicht immer befriedigend sein, da die solchermaßen addressierten Rechner innerhalb eines physikalischen Netzes liegen müssen. Die Netznummer muß im Internet stets den Weg bis zum Zielnetz weisen. Erst bei der Ankunft im Zielnetz wird die Host-ID ausgewertet und auf eine Adresse der Sicherungsschicht übersetzt. Größere Unternehmen verfügen oftmals über eine Netzwerk-Infrastruktur, die aus mehreren Netzen im Sinne der OSI-Ebene zwei bestehen. Da die Unternehmen nicht auf den Vorteil einer einzigen Internetadresse verzichten wollen, wird ein Teil der verfügbaren Benutzeridentifikation dazu verwendet, die Internetadresse in mehrere Subnetzwerke zu strukturieren. Ein Netzwerk mit der Klasse-B-Adresse 128.69 könnte so beispielsweise in die Subnetzwerke A und B aufgeteilt werden, so daß Subnetz A nur den Adressenbereich 128.69.1.1 bis 128.69.1.254 benutzt, und Subnetz B den Bereich 128.69.2.1 bis 128.69.2.254. Die Verbindungskomponente zwischen beiden Netzwerken, ein Router (siehe Kapitel 2.4.7), kann nun mit Hilfe einer sogenannten Subnet-Adreßmaske feststellen, ob ein Datenpaket des Netzwerkes ein lokales Ziel besitzt, in das zweite Subnetzwerk vermittelt (geroutet) oder überhaupt in ein anderes Internet-Netzwerk übertragen werden soll. Die Subnet-Adreßmaske ist beispielsweise 255.255.255.0. Sie ist nichts anderes als eine Bitmaske, die Nullen für den Adressenbereich enthält, der für den lokalen Subnetzbereich vorgesehen ist, und Einsen für alle anderen Bits.

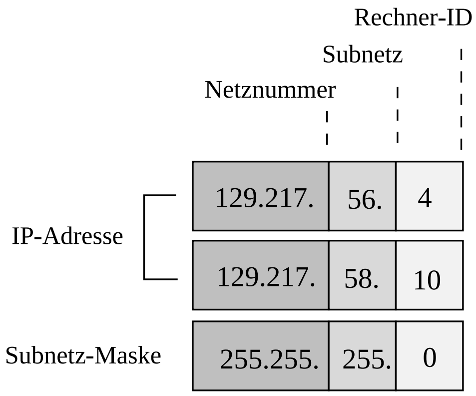

Abbildung 2.7: Aufbau einer Internet-Adresse

Abbildung 2.7 zeigt zusammenfassend die Struktur einer Internet-Adresse anhand eines Beispiels aus dem Adressraum der Universität Dortmund am Lehrstuhl Informatik. Die ersten zwei Stellen (129.217) bilden die Netznummer, das gesamte dritte Byte ist die Subnetzadresse (am Beispiel des Lehrstuhls sind es zwei). Bei den abgebildeten IP-Adressen handelt es sich somit um die Rechner, mit den Adressen 4 und 10 in den Subnetzen 56 und 58 des Adreßbereiches.

Wie in Tabelle 2.1 zu erkennen ist, sind die Adreßbereiche der einzelnen Klassen beschränkt. Jede Netzidentifikation der Internet-Adreßklasse A beinhaltet 2^{21} (da 21 Bit dafür zur Verfügung stehen) oder 2.097.152 Benutzeridentifikationen. Allerdings stehen weltweit nur 126 Klasse-A-Adressen zu Verfügung. Die 16.384 Klasse-B-Adressen beinhalten dementsprechend 65.536 Benutzeradressen, die 2.097.152 Klasse-C-Adressen je 254 Benutzeridentifikationen. Die Zahl der zu vergebenen 32-Bit-Internetadressen wird aufgrund des starken Wachstums des Internet in absehbarer Zeit erschöpft sein [birm96].

Aus diesem Grund wurde im November 1991 vom IAB (Internet Activities Board) die ROAD-Gruppe (Routing and Addressing) gegründet, die die Aufgabe hatte, das Internetprotokoll zu überarbeiten. 1995 wurde diese verbesserte Internetprotokoll-Version (IPv6 oder IPng next generation) vom IETF beschlossen, und löst seitdem (die Kompatibitlität zur bestehenden IP-Version IPv4 ist gewährleistet) zunehmend die bestehende Internet-Protokollversion ab. Der Adreßraum von IPv6 umfaßt aufgrund von 128 Bit langen Adressen 2^{128} oder 10^{38} Adressen, womit das Problem der Adressenknappheit gelöst ist [deer95].

Ferner stehen noch Adressen der Klassen D und E zur Verfügung. Die 32-Bit-Internetadressen der Klasse D werden als Multicast-Adressen bezeichnet. Mit ihrer Hilfe können Datenpakete an bestimmte Gruppen von Empfängern gesendet werden. Bestimmte Multicast-Adressen werden dabei wie alle anderen Internetadressen zentral vergeben, andere sind zur vorübergehenden Benutzung frei verfügbar. Multicast-Adressen können allerdings ausschließlich als Zieladresse verwendet werden, niemals als Senderadresse. Adressen der Klasse E sind für zukünftigen Verwendungen reserviert [birm96].

Die in diesem Abschnitt beschriebene Adreßstruktur ist auch Grundlage der IP-Routenwahl, die für die Zustellung eines Datagrammes zwischen zwei unterschiedlichen Netzen verantwortlich ist.

2.4.7 Routenwahl

Unter *Routenwahl* (engl.: Routing) versteht man den Vorgang, durch den zwei Rechner den optimalen Weg zur Kommunikation in einem verteilten Netz finden.

Jede Implementierung des Internet-Protokolls besitzt die notwendige Funktionaliät, um auf der Basis der Adreßinformation entscheiden zu können, ob eine gewünschte Zieladresse im eigenen Subnetz liegt. Liegt dieser Fall vor, so wird das Datagramm mit Hilfe des entsprechenden Netzwerkprotokolls der Sicherungsschicht direkt an den Zielrechner gesandt. Wird beispielsweise innerhalb einer Arbeitsgruppe, die durch ein Netzwerk auf Ethernet-Basis verbunden ist, eine E-Mail verschickt, so erzeugt die Netzwerksoftware des Senders einen Ethernet-Rahmen, der das IP-Datagramm zum gewünschten Empfänger überträgt [denn98].

Geht aus den Netz- und Subnetzkomponenten der Zieladresse jedoch hervor, daß der Empfänger des Datagrammes nicht im selben Netz zu finden ist, so muß das Datagramm an einen Router weitergeleitet werden.

Ein *Router* (auch als Gateway bezeichnet), ist eine auf OSI-Ebene drei operierende Netzwerkkomponente, die auf Basis der Transportadressen die Routenwahl durchführt.

Als Router kommt folglich jeder Rechner mit mehr als einer Netzwerkschnittstelle und geeigneter Software in Frage. Heutzutage sind Router in den meisten Fällen speziell für diesen Zweck geschaffene Netzwerkkomponenten, deren Software auf den Vorgang der Routenwahl hin optimiert ist [perl94]. Sie sind typischerweise modular aufgebaut und können mit Netzwerkschnittstellen der unterschiedlichsten Protokolle der Sicherungsschicht ausgestattet werden. Router unterstützen daher die gängigen Protokolle der Transportschicht, sowie die gewählten Netzwerkprotokolle der Sicherungsschicht.

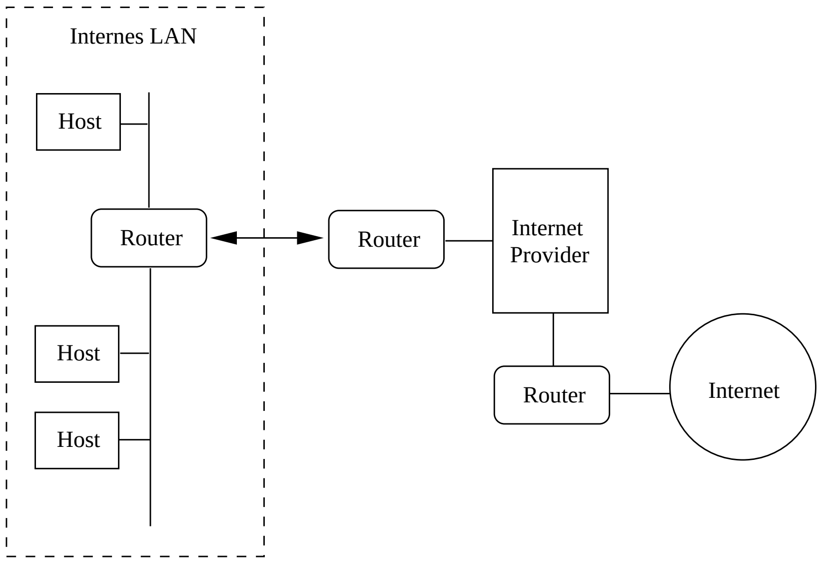

Abbildung 2.8: Routenwahl

Abbildung 2.8 zeigt symbolisch zwei getrennte Netze, die durch einen IP-Router verbunden sind.

Jedes Datagramm, dessen Zieladresse nicht im lokalen Netz liegt, wird von den angeschlossenen Rechnern zum Router weitergeleitet. Dieser determiniert ausgehend von der Zieladresse, über welchen seiner Netzwerkanschlüsse das Zielnetz zu erreichen ist. Anschließend wird das entsprechende Protokoll der Sicherungsschicht eingesetzt, um das Datagramm zu übertragen. Vermittelt der Router lediglich zwischen den beiden Teilnetzen, so wird das Datagramm in der Form eines

Ethernet-Rahmens zum Zielrechner gesandt.

Anders verhält es sich, wenn ein IP-Datagramm an einen Rechner im globalen Internet adressiert ist. Der Router verfügt über keine globale Adreßtabelle aller Netze im weltweiten Internet. Vielmehr leitet er alle Pakete mit ihm unbekannten Zielnetzen in das Netz des Internet-Providers weiter. Wiederum bedient er sich dazu des erforderlichen Protokolls der Sicherungsebene um den Transfer des Datagrammes durchzuführen. Über ISDN-Verbindungen kann beispielsweise das Protokoll *PPP* (Point-to-Point Protocol) zum Einsatz kommen [gasm94].

Im Netz des Zugangsanbieters wiederholt sich der gleiche Vorgang unter Einsatz eines größer dimensionierten Routers. Dieser verwaltet eine Adreßtabelle, in der alle über diesen Zugangsanbieter direkt erreichbaren Netzadressen enthalten sind. Ist die gesuchte Zieladresse auch in dieser Liste nicht zu finden, wird das Datagramm über die Infrastruktur des Providers weitergeleitet.

Neben diesen Grundlagen der Routenwahl sind es im wesentlichen zwei Mechanismen, die den Aufbau des Internet zum weltumspannenden Netzwerk ermöglicht und die Integration der stark steigenden Anzahl von Rechnern erlaubt haben [perl94].

- Die von den Routern verwaltete Adreßtabelle kann dynamisch aufgebaut werden. Durch den Einsatz von sogenannten *Routingprotokollen* tauschen Router auf standardisierte Art die ihnen bekannten Netzadressen aus. Dieser Mechanismus ist vor allem an den stark belasteten Knotenpunkten der globalen Infrastruktur von Bedeutung. Ein Beispiel für solch einen zentralen Konten wäre ein Router, der die Netze zweier Internet-Provider verbindet.

- Ein großes Problem war jedoch das starke Anwachsen der auf diese Art propagierte Routing-Information. Dies steht in Zusammenhang mit der Erschöpfung des IP-Adreßraumes. Mit der zunehmenden Vergabe von mehreren Adressen der Klasse C, anstelle von einer Adresse der nicht mehr verfügbaren Klasse B, stieg die von den Routern zu propagierende Adreßinformation sprunghaft an [denn98]. Ein unter dem Namen CIDR (Classless Internet Domain Routing) bekanntes Verfahren, ermöglicht die Aggregation unterschiedlicher Netzwerkadressen zu einem *Supernetz* (engl.: Supranetting). Auf diese Weise können beispielsweise alle über den gleichen Internet-Provider angeschlossenen Netze mit einer einzigen Adresse von den Routingprotokollen nach außen propagiert werden. Erst innerhalb der eigenen Infrastruktur ist schließlich der Einsatz der Netzwerkadresse erforderlich. Das hier angewandte Prinzip ist das gleiche wie im Fall der Subnetzbildung (vgl. Kapitel 2.4.6.2).

2.4.8 Sicherheitsüberlegungen zum Internet-Protokoll

Bei der Entwicklung der Internet-Protokolle stand der kommerzielle Einsatz dieser Architektur nicht im Vordergrund. Überlegungen wie Ausfallsicherheit oder flexible Einsatzbarkeit bestimmten den Aufbau des Internet-Protokolls.

Der Vorgang der Übertragung von Datagrammen über mehrere autonome Netze verdient unter dem Blickwinkel des kommerziellen Einsatzes dieser Protokoll-Architektur besondere Beachtung. Darin liegt ein wesentlicher Unterschied zwischen dem Internet und alternativen Telekommunikationsdiensten begründet: Das Internet wird in hohem Ausmaß *dezentral administriert.* Daraus ergeben sich einige im kommerziellen Einsatz bedeutsame Aspekte:

- Ein Unternehmen, das sich des Internet als Infrastruktur bedient, hat keinerlei Gewährleistungsansprüche, wenn ein IP-Paket nicht vollständig oder überhaupt nicht beim Adressaten ankommt [amor94]. In der Regel hört die Einflußnahme beim eigenen Zugangsanbierter auf, dessen Infrastruktur in manchen Fällen jedoch nur in geringem Ausmaß die Grundlage der tatsächlichen Datenübertragung ist. Wird das Internet als Marketingmedium eingesetzt, so ist der Kundenkreis naturgemäß offen. Dementsprechend schwer abschätzbar sind auch die an einer Datenübertragung beteiligten Netzanbieter.

- Aufgrund der dynamischen Routenwahl ist die von einem IP-Paket verwendete Route nicht vorhersehbar. Die Überlastung einer Strecke oder der Ausfall einer Leitung kann zur Übertragung von Paketen auf alternativen Routen führen. Die Absicherung der Datenübertragung kann daher nicht darauf beruhen, daß die beteiligten Netzbetreiber sorgfältig ausgewählt werden.

- Nicht nur die fehlende Übertragungsgarantie, auch die Qualität der benutzten Infrastruktur ist für den kommerziellen Einsatz von großer Bedeutung. Darunter ist im Zusammenhang mit der Übertragungssicherheit in erster Linie die Qualität der Systemadministration zu verstehen [ches96]. Von der Konfiguration und Wartung der komplexen Routerprodukte bis zur Durchsetzung von Sicherheitsmaßnahmen im Bereich der Netzwerkknoten ist der Internet-Benutzer den Betreibern der Netze ausgeliefert. Bei jedem Netzbetreiber können die übertragenen Pakete eingesehen, abgefangen oder modifiziert werden.

Die IP-Adresse scheint bei oberflächlicher Betrachtung als Mittel zur weltweit eindeutigen Identifikation der beiden Kommunikationsparteien naheliegend. Dieser Eindruck ist jedoch bei näherer Betrachtung trügerisch – mehrere Angriffe auf geschützte Netze nutzen die Tatsache aus, daß die Verbindungen zwischen der IP-Adresse im Protokollkopf und einem physischen Rechner keine zuverlässige ist.

Mit geeigneter Software besteht die Möglichkeit, daß IP-Datagramme gezielt mit falscher Absender-Adresse verschickt werden können. Dieses als *„Internet Adress Spoofing“* bezeichnete Verfahren, wird häufig dazu benutzt, um Firewall-Systeme zu umgehen, die mit Paketfiltern arbeiten (siehe Kapitel 3.6). Einen Überblick zu Angriffsmethoden und entsprechenden Gegenmaßnahmen bietet das Kapitel 3.5.

2.4.9 OSI-Sicherheitsarchitektur

So grundlegend wie das OSI-Referenzmodell für die Architektur von offenen Systemen ist, so wichtig ist die OSI-Sicherheitsarchitektur auch für die Integration von Sicherheitsdiensten in diese Systeme. In der OSI-Sicherheitsarchitektur sind Sicherheitsdienste (security services) und Sicherheitsmechanismen (security mechanism) aufgeführt, sowie deren mögliche Einbettung in die sieben Schichten des OSI-Referenzmodells diskutiert. Weil im OSI-Referenzmodell Dienste zwischen zwei Schichten als angebotene Dienstprimitive (service primitives) verstanden werden, wird anstelle von Sicherheitsdiensten auch etwa von Sicherheitsfunktionen (security functions) gesprochen [oppl97] (vgl. Kapitel 4.5 und 4.6).

2.5 Dienste im Internet

Das Internet stellt den Benutzern auf der Basis von TCP/IP als Transportprotokoll eine Vielzahl von Dienstleistungen zur Verfügung [hahn94]. Diese Dienste sind normalerweise unter Verwendung weiterer Protokolle realisiert, die wiederum auf TCP/IP aufsetzen. Im folgenden werden einige zur Verfügung stehenden Dienste im Internet näher beschrieben.

2.5.1 Client/Server Prinzip

Das Client/Server Prinzip ist eigentlich kein Dienst, den man als Anwender in Anspruch nehmen kann. Es handelt sich hierbei vielmehr um ein grundlegendes Prinzip, auf dem wichtige Dienste wie Gopher oder das Word Wide Web aufbauen.

Der Begriff Client/Server-Computing wird in unterschiedlicher Weise verwendet. Für eine Erklärung sind zumindest zwei Perspektiven zu unterscheiden: die *hardware-orientierte* und die *software-orientierte* Sichtweise [rued95].

Die PC-Netzwerkbetriebssysteme der 80er Jahre, wie *Netware* und *LAN-Manager*, prägten die hardware-orientierte Interpretation des Client/Server-Begriffs. Diese Sichtweise ist sehr an den beteiligten Rechnern orientiert. Desktop-Systeme sind über lokale Netzwerke mit speziellen Hintergrundsystemen verbunden, die beispielsweise als Datei-Server oder Druck-Server genutzt werden. Bei einer hardware-orientierten Sichtweise bezeichnet der Sprachgebrauch die Desktop-Systeme als Clients und die Hintergrundsysteme als Server.

Die alleinige Beschränkung des Begriffs Client/Server-Computing auf bestimmte Hardware-Konfigurationen greift deutlich zu kurz. Die Vorteile des Client/Server-Computing liegen bei der Software-Architektur.

Die zugrundeliegende Konzeption wird verständlich, wenn man sich die Blockstruktur moderner Programmiersprachen vor Augen hält. Diese kennen eine Unterscheidung von Hauptprogrammen und Unterprogrammen. Das Aufbauprinzip für Unterprogramme wird beim Client/Server-Ansatz erweitert, und zwar auf Programme, die auf unterschiedlichen Rechnern ablaufen, sowie auf asynchrone Aufrufe. Das aufrufende Programm wird als Auftraggeber oder Client und das aufgerufene Programm als Auftragnehmer oder Server bezeichnet. Client- und Server-Programme können prinzipiell sowohl auf einem Rechner, als auch über entsprechende Kommunikationsprotokolle miteinander verbunden werden und auf unterschiedlichen Rechnern installiert werden.

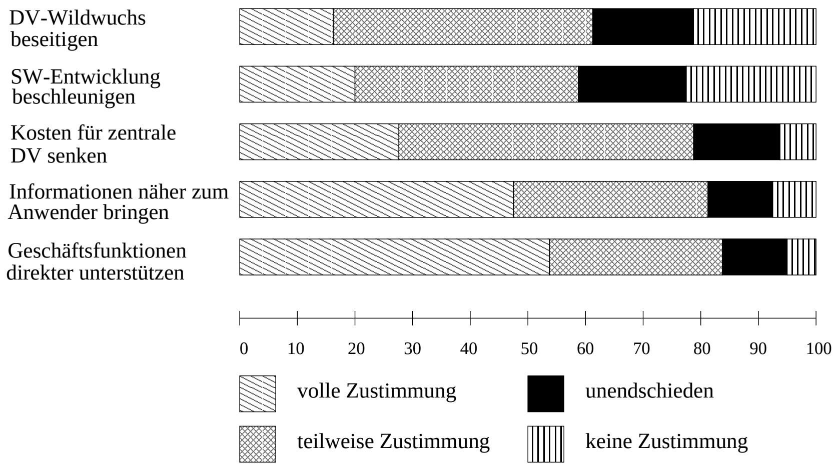

Abbildung 2.9: Zielsetzungen von Client/Server-Strategien

Client/Server-Computing als Software-Architektur bildet die Basis für eine kooperative Verarbeitung (Cooperative Processing) und kann sowohl zentralistisch im Verbund mit speziellen Präsentationsrechnern als auch in hochgradig verteilten, vernetzten Installationen mit einer Vielzahl unterschiedlicher Server realisiert werden.

In einer Umfrage der Computerwoche (*CW93a*) unter 60 deutschen Großanwendern zu den Zielsetzungen der hauseigenen Client/Server-Strategie wurden überwiegend die Anliegen

- Geschäftsfunktionen direkter zu unterstützen und
- Information näher zum Anwender zu bringen

genannt [niem95].

Wie in Abbildung 2.9 zu erkennen ist, stehen diese Zielsetzungen sehr viel stärker im Mittelpunkt der Überlegungen als das Thema der Kosteneinsparung.

2.5.2 Telnet

Telnet ermöglicht es, eine Verbindung zu einem fernen System aufzubauen, als würde dies von einem direkt angeschlossenen Terminal aus geschehen. Man benutzt also den lokalen Bildschirm und die lokale Tastatur, arbeitet aber mit dem entfernten Computer (Remote Terminal). Die Internet-Dienste, die im allgemeinen über Telnet angeboten werden, unterscheiden sich nicht von Diensten, die durch direktes Einwählen in ein System über ein Modem zugänglich sind. Demnach kann ein Dienst, der über Modem verfügbar ist, auch über Telnet in Internet angeboten werden.

Verwendet wird der Dienst Telnet zum Beispiel von Systemadministratoren, um entfernte Computer zu konfigurieren und zu warten. Es wird dazu beispielsweise ein Konfigurationsprogramm auf dem entfernten Computer gestartet.

Eine weitere Anwendung ist die Benutzung sehr leistungsfähiger Computer für rechenintensive Aufgaben. Der Benutzer stellt eine Telnet Verbindung zu einem leistungsstarken Computer her und startet dort sein Programm. Das Ergebnis der Berechnungen wird auf dem lokalen Bildschirm angezeigt. In einem firmeninternen LAN genügt es beispielsweise einige wenige sehr leistungsstarke Computer zu installieren, da dann die Möglichkeit besteht, zeitkritischen Programme auf diesen Rechnern auszuführen.

2.5.3 E-Mail

E-Mail steht für electronic mail (elektronische Post) und ist ein häufig verwendeter Dienst im Internet. Heutzutage werden täglich sehr viele elektronische Briefe über das Internet verschickt. Mittels E-Mail kann man jedem Benutzer des Internet binnen kürzester Zeit einen elektronischen Brief zukommen lassen; ein entsprechender konventioneller Brief würde für die gleiche Entfernung einige Tage oder noch länger benötigen. Mail-Systeme bieten auch die Möglichkeit beliebige Daten, wie zum Beispiel Bilder oder Programme zu versenden.

E-Mails haben ein standardisiertes Format und bestehen im wesentlichen aus zwei Teilen: einem Vorspann (header) und der Nachricht selbst (body). Im Header werden Informationen wie die Adresse des Senders, die Adresse des Empfängers, die Absendezeit, das Absendedatum, die Überschrift der Nachricht usw. übertragen.

Die Übertragung von Mails im Internet geschieht mit einem speziellen Protokoll der TCP/IP Familie, dem SMTP (Simple Mail Transfer Protocol). Es beschreibt das Format von E-Mails und die Art und Weise wie E-Mails von einem Computer zum anderen weitergeleitet werden. Für diesen Zweck ist in jedem Computernetz ein Programm installiert, welches die Weiterleitung der E-Mails verwaltet. Dieses Programm nennt man *transport agent*. Auf UNIX Rechnern heißt dieses Programm meist *sendmail* und es kann auch direkt zur Erstellung von E-Mails verwendet werden. Mail-Programme für Benutzer kommunizieren auf UNIX Rechnern ebenfalls über SMTP mit den transport agents.

Um auch die Übertragung von binären Daten, wie Bildern oder Musikdateien zu ermöglichen, wurde ein erweitertes Nachrichtenformat, genannt MIME (Multipurpose Internet Mail Extension), entwickelt. Dabei werden binäre Daten in reine ASCII Daten umgesetzt und in einer Kopfzeile vermerkt. Die E-Mail, die nun nur aus ASCII Daten besteht, wird ebenfalls mit mit SMTP übertragen.

2.5.4 FTP

Ein weiterer wichtiger Dienst im Internet ist FTP. FTP steht für File Transfer Protocol und bezeichnet ein weiteres Protokoll für die Übertragung von Dateien im Internet. Mit Hilfe des Dienstes FTP können im Internet Dateien von einem Computer auf einen anderen Computer übertragen werden.

Wie auch viele andere Internet Dienste basiert FTP auf dem Client/Server Prinzip; jedoch werden beim Aufbau einer FTP Verbindung zwei verschiedene Ports verwendet. Über das Port mit der Nummer 21 werden nur die Befehle für die Datenübertragung gesendet. Die angeforderten Daten werden dann über Port 20 übertragen.

Auch bei diesem Dienst benötigt man wie bei Telnet eine Zugangsberechtigung zum Computer, von dem man Dateien laden will. Jedoch gibt es im Internet eine riesige Anzahl von FTP-Servern, von denen man auch ohne Zugangsberechtigung Daten beziehen kann. Diese Art von FTP-Servern werden *anonymous* FTP-Server genannt, da sie für jeden Benutzer auch ohne eine spezielle Berechtigung zugänglich sind. Am Anfang bei der Abfrage des User Namens gibt man entweder ftp oder anonymous ein. Als Paßwort muß meist die eigene E-Mail Adresse angegeben werden.

2.5.5 Usenet

Der Dienst Usenet ist die Abkürzung für Users Network und stellt eine große Ansammlung von Diskussionsgruppen zur Verfügung. In den mehr als 10.000 existierenden Newsgruppen diskutieren Millionen von Menschen überall auf der Welt. Beinahe für jedes Thema existiert eine Newsgruppe.

Technisch gesehen werden die Artikel der verschiedenen Diskussionsgruppen mit dem Network News Transfer Protocol (NNTP) übertragen. Dabei tauschen benachbarte News-Server immer die neuesten Artikel miteinander aus. Nach einer bestimmten Ausbreitungszeit befindet sich ein neuer Artikel auf allen News-Servern im Internet. Es gibt auch lokale Diskussionsgruppen, die nicht über das ganze Internet verbreitet werden.

2.6 Die Schlüsselstrategie: World Wide Web

Obwohl das Internet als solches bereits seit mehr als 25 Jahren besteht, wurde seine heutige Popularität erst durch die Einführung der graphischen Benutzeroberfläche World Wide Web (WWW) im Jahr 1993 möglich. Das Prinzip des World Wide Web basiert auf der Verknüpfung von elektronischen Dokumenten über Schlüsselbegriffe oder Symbole (Links). Textdokumente, die solche Verknüpfungen beinhalten, werden als Hypertextdokumente bezeichnet (vgl. [berg96]).

Das World Wide Web ist kein Programm, sondern ein Konzept. Es besteht aus folgenden Komponenten:

- *Client-Server-Architekturen:* WWW-Server stellen Information zur Verfügung; WWW-Clients rufen sie ab und zeigen sie an.
- *HTML:* Die Hypertext Markup Language für strukturierten Hypertext.
- *HTTP:* Das Hypertext Transfer Protocol als Kommunikationsprotokoll zwischen WWW-Client und WWW-Server.
- *Multimedia:* WWW erlaubt die Integration von Text, Bild, Ton, Video und beliebigen weiteren Dokumentarten.
- *URI:* Uniform Resource Identifier ermöglicht die Integration bestehender Internet-Ressourcen durch ein einheitliches Adressierungsschema.

2.6.1 Adressierungsschema im WWW

Die Adressierung von Objekten im WWW erfolgt im URL-Format. URLs können beliebige Dateiformate spezifizieren. Ein URL (Uniform Resource Locator) be-

Schlüsselwort	Dienst
file	Lokales Dateisystem
telnet	Telnet
mailto	E-Mail
ftp	FTP
news	Usenet
http	World Wide Web

Tabelle 2.2: WWW-Protokolle

steht aus drei Komponenten, die zur eindeutigen Bezeichnung eines Objektes im Internet notwendig sind:

- das Protokoll (Dienst), das benutzt werden muß, um auf das betreffende Objekt zugreifen zu können,
- die Internetadresse und Portnummer des Serversystems, auf dem sich das Objekt befindet,
- dem Pfad und Dateinamen des betreffenden Objektes.

Aus dieser Information ergibt sich folgender Aufbau der Adresse:

Dienst://Serveradresse:Port/Pfad/Dokument

Im folgenden werden die einzelnen Komponenten näher beschrieben.

2.6.1.1 Protokoll/Dienst

Dieser Parameter gibt den gewünschten Dienst an. Der Browser benötigt diese Angabe, um daraus das geeignete Übertragungsprotokoll und den richtigen Port zu bestimmen. Die folgende Tabelle 2.2 zeigt die Schlüsselwörter für einige Dienste im Internet.

2.6.1.2 Serveradresse

Die Serveradresse gibt die Internet-Adresse des Servers an. Es kann dabei der Name des Servers oder direkt seine IP-Adresse angegeben werden. Außerdem ist eine explizite Angabe der gewünschten Portnummer möglich, da ein Server an einem beliebigen Port arbeiten kann. Die Portnummer wird dabei mit einem Doppelpunkt getrennt an die Adresse des Servers angehängt.

2.6.1.3 Pfad

Der Pfad gibt, wie bei einem lokalen Dateisystem den Pfad zu einem bestimmten Dokument von der Wurzel aus an. Dabei ist zu beachten, daß das UNIX konforme Divisionszeichen „/“ (Slash) als Trennzeichen für die Pfadangabe verwendet wird.

2.6.1.4 Dokument

Dokument bezeichnet irgendeine beliebige Datei. Für die Dateierweiterungen gelten dabei die gleichen Regeln wie bei lokalen Dateisystemen. Index.html bezeichnet zum Beispiel ein HTML Dokument.

Eine Dokumentadresse sieht zum Beispiel folgendermaßen aus:

```
http://www.w3.org/pub/WWW/Jigsaw/User
```

2.6.2 Das Übertragungsprotokoll HTTP

Für den Transport der Daten ist das Hypertext Transfer Protocol (HTTP) zuständig. Es ist auch auf dem Client/Server Prinzip aufgebaut und die Kommunikation zwischen Client und Server erfolgt über Port 80 [gett96].

2.6.2.1 Request-Line oder Status-Line

Die erste Zeile bei einer Anfrage eines Browsers besteht aus der Anfrage-Zeile (Request-Line). Sie enthält die Methode, den Namen des Dokuments mit Pfad und die verwendete HTTP Protokoll Version. Die am häufigsten verwendete Methode ist GET. Sie dient zur Anforderung des adressierten Dokuments. Zum Beispiel:

```
GET /PEOPLE/index.html HTTP/1.0
```

Der Antwort des Servers beginnt mit der Status-Zeile (Status-Line). Sie enthält den Rückgabewert der Antwort und zeigt, ob die Anfrage beantwortet wurde oder ob ein Fehler aufgetreten ist. Das folgende Beispiel zeigt den Statuscode für eine erfolgreiche Bearbeitung der Anfrage:

```
HTTP/1.0 200 OK
```

2.6.2.2 Header

Nach der Request-Line folgen die sogenannten Header (Kopfzeilen). Sie dienen zur Beschreibung der Daten im Message Body und enthalten Informationen über

Typ, Sprache, Zeichensatz, Kodierung, usw.

In jeder Zeile befindet sich genau ein Header. Nach dem Namen des Headers folgt ein Doppelpunkt und dann dessen Wert. CONTENT-TYPE: image/jpg zeigt zum Beispiel an, daß es sich bei den Daten um ein Bild im JPEG Format handelt.

2.6.2.3 Entity Body

Nach einer Leerzeile folgen am Ende der Nachricht schließlich die in den Headern beschriebenen Daten. Mit diesem System ist eine Übertragung aller beliebigen Datenformate möglich. Es muß nur der Wert des Headers CONTENT-TYPE: richtig gesetzt sein, da sonst vom Browser ein falsches Programm zur Bearbeitung der Daten gestartet wird.

2.7 Corporate Intranets

Unter dem Übergriff Corporate Intranets versteht man die Gesamtheit der internen Unternehmensapplikationen, die über moderne WWW-Browser unter einer einheitlichen Benutzerschnittstelle zur Verfügung gestellt werden. Intranets benutzen die Transportmechanismen und Darstellungsformate des Internet als universelle Plattform für die unternehmensinternen Datenkommunikation, sowohl im lokalen (LAN, Local Area Network) als auch im Weitverkehrsbereich (WAN, Wide Area Network). Die Basis von Intranets stellen World Wide Web-Server und -Clients, sowie ein leistungsfähiges Messagingsystem dar. Die Funktionen der WWW-Intranetserver gehen dabei weit über die von Internet-Web-Servern der ersten oder zweiten Generation hinaus und umfassen Funktionen wie

- Dokumentenmanagement,
- Replikation,
- Groupware-Anwendungen,
- Datenbankzugriffe,
- Zugriff auf unternehmensspezifische Anwendungen,
- Multimedia-Erweiterungen (Nutzung als Audio-/Videoserver),
- Authentifikation/Kryptographie und die,
- Integration in Netzwerkmanagement-Systeme (SNMP).

Dasselbe gilt für Messagingsysteme, wie sie in Intranets genutzt werde. Dabei kommen Systeme auf der Basis von HTML-Mail zum Einsatz, die in der Lage sind, multimediale Inhalte zu übertragen und darüber hinaus mit Funktionen wie Verschlüsselung, Empfangsbestätigung und Zeitmarken die Grundlage für

- Workflow-Systeme,
- Terminplanungsapplikationen,
- Diskussionsforen,
- Fax-/Voice-Mailsysteme und
- Electronic-Commerce-Anwendungen

bilden.

Kapitel 3

Grundlagen zur Sicherheit

3.1 Warum Sicherheit ?

Was ist *„Computersicherheit"?* Allgemein gesprochen, die Verhinderung unbefugter Aktivitäten an, mit oder durch einen Computer und der zugehörigen Peripherie.

Die verstärkte kommerzielle Internetnutzung und die zunehmende einfache Zugangsmöglichkeiten führten in den letzten Jahren zu einem starken Anstieg von gezieltem Mißbrauch und kriminellen Handlungen innerhalb des Internet. Bei der Frage, ob und wie für ein Unternehmen ein Internetzugang eingerichtet werden soll, gilt es daher in besonderem Maße, die Risiken der jeweiligen Optionen abzuwägen. Ein Internetanschluß ohne entsprechende Sicherheitsmaßnahmen, kann eine nicht zu unterschätzende Gefahr bedeuten. Nahezu jedes Unternehmen ist heute auf das reibungslose Funktionieren der EDV-Infrastruktur angewiesen. Ein Teil- oder sogar Totalausfall der Informationssysteme, verursacht durch Sicherheitsprobleme im Internet, bedeutet zwangsläufig einen enormen finanziellen Schaden, der den möglichen Nutzen eines Internetzuganges bei weitem übertreffen kann. Sicherheitsmaßnahmen haben zunächst nur einen gewissen *Verhinderungsnutzen*, eine Investition in entsprechende Sicherheitskonzepte scheinen zunächst nicht plausibel. Eine Investition impliziert einen indirekten Nutzen für ein Unternehmen.

3.1.1 Sicherheit allgemein

IT-Sicherheit ist das Fachgebiet, das sich mit der Sicherheit in der IT, d.h. mit der sicheren Speicherung, Verarbeitung und Übertragung von informationstragenden Daten, befaßt [oppl97].

Nach [pfle97] unterteilt man den allgemeinen Begriff der Sicherheit eines IT-Systems in drei Bereiche. Dabei geht man von der Sicherstellung der *Verfügbarkeit*, der *Integrität* und der *Vertraulichkeit* eines IT-Systems, bzw. der in einem IT-System gespeicherten, verarbeiteten und übertragenen Daten aus. Abbildung 3.1 zeigt die Zusammensetzung dieser drei Bereiche.

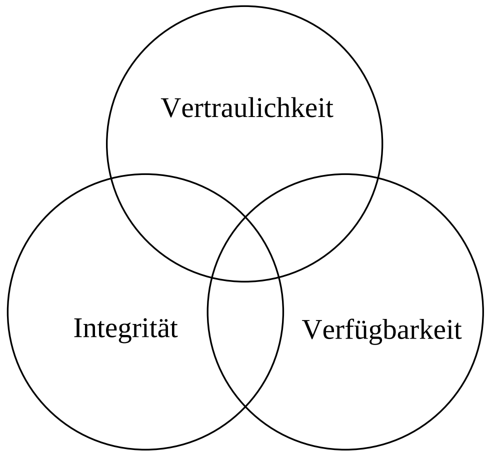

Abbildung 3.1: Sicherheitsziele

Die einzelnen Begriffe lassen sich wie folgt erklären:

1. Die Vertraulichkeit (engl.: confidentiality oder secrecy) bezeichnet die Eigenschaft eines IT-Systems, gespeicherte, verarbeitete oder übertragene Information nur berechtigten Personen oder -gruppen zugänglich zu machen. Eine Information ist dabei vertraulich, wenn sie nur berechtigten Personen oder -gruppen zugänglich ist.

2. Die Integrität (engl.: integrity) bezeichnet die Eigenschaft eines IT-Systems, nur erlaubte und beabsichtigte Veränderungen an gespeicherte, verarbeitete oder übertragene Information zuzulassen. Die Information ist integer, wenn an ihr nur zulässige Veränderungen vorgenommen worden sind.

3. Die Verfügbarkeit (engl.: availibility) bezeichnet die Eigenschaft eines IT-Systems, bestimmte Dienstleistungen in zugesicherter Form und Qualität erbringen zu können. Die Verfügbarkeit von Information ist darin enthalten. Sie besagt, daß Information in entsprechender Frist und in erwarteter oder geforderter Form und Qualität zur Verfügung stehen muß. Erwähnt sei hier das Beispiel einer Notaufnahme in einem Krankenhaus, wo der Zugriff auf eine Blutdatenbank für den Patienten existentiell sein kann.

Alle drei Sicherheitsanforderungen gewähren erst zusammen den sicheren Betrieb eines IT-Systems. Entsprechend können sie nicht unabhängig und losgelöst voneinander betrachtet werden (siehe: Bild 3.1). Im Zusammenhang mit offenen Systemen werden neben Vertraulichkeits-, Integritäts- und Verfügbarkeitsaspekten auch Authentizitäts-, Verbindlichkeits- und Anonymitätsaspekte diskutiert [hoff95].

3.1.2 Sicherheitsrisiko Internet

Eine Studie der *National Computing Security Association (NCSA)* vom Mai 1995 ergab, daß Unternehmen mit Internetzugang im Durchschnitt acht Mal so häufig Angriffen ausgesetzt sind wie vergleichbare Unternehmen ohne Internetanschluß. Demnach sind nur drei Prozent der Unternehmen ohne Internet, jedoch 24 Prozent der Unternehmen mit Internetanbindung, Opfer von externen Mißbrauchversuchen (Hacking). Weitere risikoerhöhende Faktoren sind Datenverbindungen zu anderen Unternehmen, sowie eine Infrastruktur, die es Mitarbeitern erlaubt, sich per Modem in das Unternehmensnetzwerk einzuwählen [kyas97].

Die potentiellen Risiken für das interne Unternehmensnetzwerk durch einen Internetanschluß stellen sich durch folgende Szenarien dar:

- Eindringen von nichtautorisierten Personen von außen in das Informationsnetzwerk.
- Einschleusen von Trojanischen Pferden und Viren durch Datenübertragungen aus dem Internet.
- Vortäuschung falscher Identität (Mißbräuchliche Verwendung der eigenen Internet-Adresse durch dritte (Adress Spoofing), Täuschung durch von Dritten simulierte Identifikationen, etc.).

Daraus können sich für ein Unternehmen

- Verlust von Daten (einfügen, löschen, verfälschen),
- Verlust von vertraulicher Information (Öffentlichkeit, Wettbewerb),
- Störung der Netzverfügbarkeit (Viren, Sabotage),
- Imageverlust in der Öffentlichkeit

als Folge ergeben.

Allgemein unterscheidet man Bedrohungsformen in *aktive* und *passive*, wobei im Rahmen eines passiven Angriffs die Vertraulichkeit der auf einem Kanal übertragenen Daten bedroht. Wie in Abbildung 3.2 dargestellt ist, kann sich ein passiver Angreifer zwischen Sender und Empfänger schalten, ohne den eigentlichen Datenfluß zu beeinträchtigen. Der Angreifer spielt lediglich die Rolle eines Beobachters.

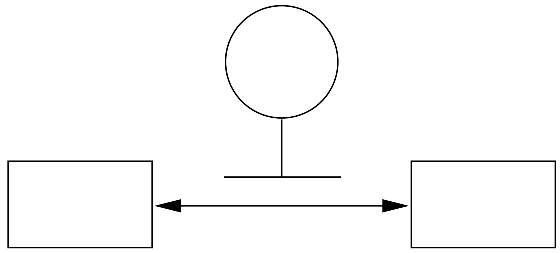

Abbildung 3.2: Prinzip eines passiven Angriffs

Grundsätzlich ist zu unterscheiden, ob ein Angreifer aus den übertragenen Daten *Nutz-* oder nur *Verkehrsinformationen* extrahieren kann. Entsprechend werden passive Abhorchangriffe und Verkehrsanalysen unterschieden.

- Im Rahmen eines passiven Abhorch- oder Lauschangriffs (passive wiretapping oder eavesdropping) kann ein Angreifer aus passiv abgehorchten Daten auf die entsprechenden Nutzinformationen schließen.
- Im Rahmen einer Verkehrsanalyse (traffic analysis) kann der Angreifer zwar aufgrund der Verkehrsdaten auf Herkunft, Ziel, Frequenz und Umfang von Nachrichten schließen, er kann daraus aber keine Nutzinformation ableiten. Verkehrsanalysen erlauben Rückschlüsse, ob überhaupt und wie stark zwischen den einzelnen Netzteilnehmern kommuniziert wird.

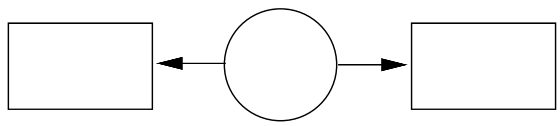

Abbildung 3.3: Prinzip eines aktiven Angriffs

Im Vergleich zum passiven Angriff richtet sich ein aktiver Angriff in erster Linie gegen die Integrität oder Verfügbarkeit der auf einem Kanal übertragenen Daten. Wie in Abbildung 3.3 dargestellt ist, kann sich ein aktiver Angreifer direkt in den Datenfluß zwischen Sender und Empfänger einschalten. Er hat dabei grundsätzlich zwei Möglichkeiten, einen aktiven Angriff zu verüben:

- Er kann übertragene Daten stören, verändern, erweitern, verzögern, vervielfältigen oder früher aufgezeichnete Daten wieder in den Kanal einspielen. Zudem kann er autorisierte Zugriffe auf Betriebsmittel verhindern oder zeitkritische Operationen verzögern.

- Der Angreifer kann aber auch versuchen, Kommunikationsbeziehungen unter falscher Identität aufzubauen und nach dem Vortäuschen von falschen Identitäten fremde Betriebsmittel in unerlaubter und nicht zulässiger Form benutzen. Um einen solchen Angriff zu verüben, muß er entweder früher abgehorchte Verbindungsaufbausequenzen wieder in den Kanal einspielen oder direkt unter falschen Identitäten auftreten (siehe hierzu auch Kapitel 3.5).

3.2 Potentielle Angreifer

Erkenntnisse über die mögliche Identität von potentiellen Angreifern können einen ersten Anhaltspunkt für die Dimensionierung des Sicherheitssystems liefern. Folgende Personengruppen können unterschieden werden:

- Mitarbeiter des eigenen Unternehmens,
- Studenten/Teenager aus dem Universitäts- und Schulenumfeld,
- Personen aus dem Konkurrenz/Wettbewerbs-Umfeld,
- Hacker/Cracker aus der Computer-Untergrund-Szene,
- professionelle Hacker/Industriespione.

3.3 Angriffspunkte und Schwachstellen

Aufgrund der Größe sowohl des Internet insgesamt, als auch der Hard- und Softwarekomponenten, aus denen es im einzelnen besteht, ist das Gesamtsystem Internet von Programm- und Funktionsfehlern durchsetzt. Damit besteht auch für jede kommerziell erstellte Software das potentielle Sicherheitsrisiko einer mißbräuchlichen Nutzung von Programmfehlverhalten. Sind die betreffenden Komponenten über ein Datennetz einer großen Zahl von Benutzern zugängig, so erhöht sich die Wahrscheinlichkeit, daß auch vereinzelte Schwachstellen mißbräuchlich genutzt werden.

Ein Beispiel aus der Vergangenheit zeigte Schwachstellen in der Software des Internet-Providers T-Online auf. Hier wurde ein sogenanntes Trojanisches Pferd[1] so platziert, so daß persönliche Daten eines T-Online Benutzers, sowie Paßwörter unbemerkt einer dritten Person zugänglich gemacht wurden.

[1] Trojanische Pferde sind ausführbare Programme, die neben ihren eigentlichen Funktionen noch absichtlich eingebaute Zusatzmechanismen enthalten, die gegen die Interessen des Anwenders gerichtet sind [heid96].

3.4 Internet: Mangelndes Programmdesign

Eine Hauptursache für die Vielzahl an Sicherheitsproblemen im Internet stellt die prinzipielle Architektur der Kommunikationsprotokolle TCP/IP und UDP dar. Keines dieser Protokolle wurde ursprünglich mit der Intention entwickelt, wirklich sichere Kommunikationspfade zu garantieren. So läßt sich bei der Datenübertragung mit Hilfe von TCP/IP im Internet nicht vorhersagen, über welche Vermittlungsknoten die Übertragung der Pakete erfolgt. Gelingt es Hackern, sogenannte *Sniffer*-Programme auf einem oder mehreren Vermittlungsknoten zu installieren, können z.B. die im Klartext übertragenen Paßwörter enttarnt werden.

Ein anderer Grund für erfolgreiche Einbruchsversuche sind mangelhafte Systemkonfigurationen sowie teilweise oder ganz fehlende Sicherheitsvorkehrungen an den Internet-Zugangssystemen. Folgende fünf Punkte zeigen technisch gesehen Schwachstellenbereiche auf:

- Fehlende Sicherheitsmaßnahmen (Keine Firewalls),
- Mangelhaft konfigurierte und administrierte Systeme,
- Prinzipielle Sicherheitsprobleme der Kommunikationsprotokolle (IP, TCP, UDP),
- Fehlerhafte Dienstprogramme,
- Prinzipielle Sicherheitsprobleme der Dienstprogramme (WWW, FTP, etc.).

3.5 Angriffsmethoden

Stellvertretend für eine Vielzahl von Methoden soll an dieser Stelle eine der häufigsten, zum Einbruch in Datennetze aus dem Internet beschrieben werden: Internet Adress Spoofing sowie der darauf aufsetzende TCP-Sequenznummern-Angriff. Einen detailierteren Überblick bieten [beye89, kers91, oppl97].

3.5.1 Internet Address Spoofing

Beim Internet Address Spoofing werden vom Angreifer synthetische Datenpakete mit gefälschter IP-Sendeadresse erzeugt, die das Paket einer internen Station vortäuschen. Gefährlich ist diese Form des Angriffs, wenn als Firewallsysteme Paketfilter zum Einsatz kommen (vgl. Kapitel 3.6), die lediglich in der Lage sind, am Ausgangsport von zu übertragenen Datenpaketen eine Filterung durchführen. Dabei geht die Information, ob es sich bei dem betreffenden Datenpaket tatsächlich um ein internes, oder aber um ein externes, gefälschtes handelt, verloren. Es wird, sobald die Sendeadresse als aus dem eigenen Adressbereich stammend erkannt wird, als Bestandteil von internen Kommunikationsbeziehungen behandelt, und entsprechend weitervermittelt. Abbildung 3.4 illustriert das Prinzip des IP-Adress-Spoofing.

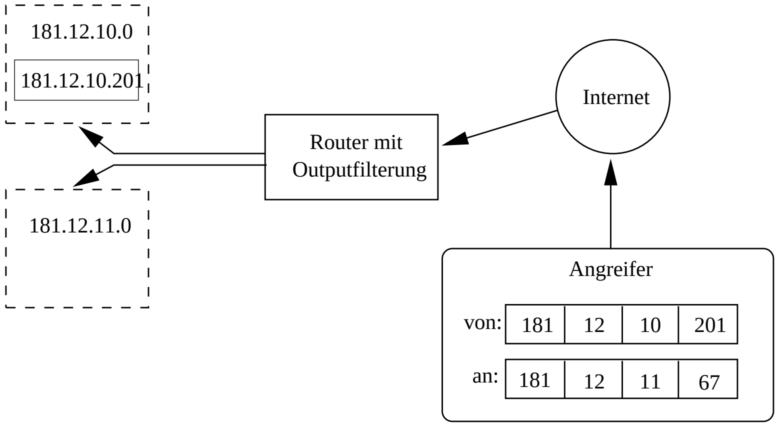

Abbildung 3.4: Prinzip des Internet Adress Spoofing

Der Angreifer aus dem Internet erzeugt dabei ein „Spoofing"-Paket mit der Sendeadresse 181.12.10.201. Als Zieladresse benutzt er die Adresse des Opfers, das sich im Netzwerk 181.12.11.0 befindet. Der Firewall Router vermittelt zunächst das synthetische Paket an das gewünschte Ausgangsport (181.12.11.0) und überprüft erst hier anhand der Filtertabelle die Sendeadresse. Das Paket wird dabei vermeintlich als von einem aus dem internen Netzsegment 181.12.10.0 stammenden System behandelt und weitervermittelt. Können von einem Angreifer mittels Adress Spoofing erfolgreich IP-Pakete von außen durch das Firewall-System hindurch in das interne Datennetz gesendet werden, kann dies als Ausgangspunkt zu einer Reihe von Angriffsarten wie Source-Routing-Angriffen, RIP-Angriffen, ICMP-Angriffen, NTP-Angriffen oder TCP-Angriffen genutzt werden.

3.5.2 Der TCP-Sequenznummern-Angriff

Der TCP-Sequenznummern-Angriff ist eine der gefährlichsten und wirksamsten Methoden, um auf Paketfiltertechniken basierende Firewall-Systeme zu überwinden. Der Ansatzpunkt dieses Angriffs liegt in der aus drei Schritten bestehenden Handshake-Sequenz (aus dem engl.: Handschlag) während eines TCP-Verbindungsaufbaus. Voraussetzung ist, daß, wie beschrieben, mit Hilfe von IP-Address-Spoofing gefälschte IP-Pakete von außen in das interne Datennetz gesendet werden können.

Eine TCP-Handshake-Sequenz arbeitet folgendermaßen: Soll von Client A eine Verbindung zum Remote-Server B aufgebaut werden, so wird dies mit dem Datenpaket

$$\boxed{\text{A > B: SYN, A\_SNa}}$$

eingeleitet, in dem von A das Synchronisationsbit SYN gesetzt wird und B die Anfangs-Sequenznummer der aufzubauenden TCP-Verbindung A_SNa mitgeteilt wird. Server B antwortet darauf mit

$$\boxed{\text{B > A: SYN, A\_SNb}}$$

Dabei wird die eigene Anfangssequenznummer A_SNb an den Client A übermittelt, und gleichzeitig dessen Sequenznummer A_SNa bestätigt. A beendet mit der Bestätigung

$$\boxed{\text{A > B: ACK(A\_SNb)}}$$

die Handshake-Sequenz. Die Wahl der Anfangssequenznummern erfolgt dabei nicht zufällig, sondern durch einen einfachen Algorithmus. Dazu wird festgelegt, daß ein 32-Bit-Zähler an der niederwertigsten Stelle alle 4 μs um den Wert 1 erhöht werden muß. In der Berkeley-TCP-Implementierung erfolgt die Erhöhung jedoch nur jede Sekunde um den Wert 128 innerhalb einer Verbindung und um den Wert 64 für jede neue Verbindung. Damit ist es möglich, mit einer hohen Wahrscheinlichkeit vorauszusagen, welche Sequenznummer ein System für seinen nächsten Verbindungsaufbau benutzen wird. Dies wird beim Sequenznummern-Angriff ausgenutzt. Vom Angreifer X wird zunächst (unter Benutzung einer beliebigen Sendeadresse X) eine Vorbereitungs-Verbindung zum Zielsystem Z aufgebaut:

$$\boxed{\text{X > Z: SYN, A\_SNx}}$$

Das Zielsystem Z antwortet mit

$$\boxed{\text{Z > X: SYN, A\_SNz, ACK(A\_SNx)}}$$

Nun täuscht der Angreifer die Identität eines internen Systems A vor (IP-Spoofing; Sendeadresse A) und sendet

$$\boxed{\text{A > Z: SYN, A\_SNx}}$$

worauf Z mit

$$\boxed{\text{Z > A: SYN, A\_SNz+, ACK(A\_SNx)}}$$

antwortet. Obwohl diese Nachricht an die interne Station A gerichtet ist und für den externen Angreifer nicht sichbar ist, kann dieser die Anfangssequenznummer A_SNz+ des Zielsystems, ausgehend vom Wert A_SNz der Vorbereitungsverbindung, errechnen und, wieder das interne System A simulierend, mit

$$\boxed{\text{A > Z: ACK(A\_SNz+)}}$$

antworten. Das Zielsystem geht nun von einer gesicherten Verbindung zu der internen Station A aus. Der Angreifer kann weiter als Station A auftreten und auf dem Zielsystem beliebige Operationen durchführen. Einzige Einschränkung ist, daß die jeweiligen Antworten des Zielsystems für den Angreifer nicht sichtbar sind, da diese ja an den internen Client A gesendet werden (vgl. [kyas97]).

3.5.3 URL-Spoofing

Weder das Protokoll HTTP noch die Beschreibungssprache HTML besitzen besondere Mechanismen um WWW-Server gegen Angriffe zu schützen. Eine weitere Methode, um in WWW-Serversysteme einzubrechen, ist URLs so zu modifizieren, daß der Server veranlaßt wird, Systemdateien zu übertragen (wie etwa Passwortdateien). URLs, die als Gateway zu Diensten wie FTP oder Gopher dienen, sind ebenfalls Ziel von Einbruchsversuchen. Durch Veränderungen der Portnummer, auf welche der URL verweist, kann beispielsweise versucht werden, die auf dem betreffenden Port befindliche Applikation zu einer unerwarteten Reaktion zu bringen und so eine Sicherheitslücke zu öffnen.

3.6 Firewalls

> *„Die meisten Hosts genügen unseren Anforderungen nicht: Sie fahren zu viele, zu große Programme. Die einzige Lösung ist daher, sie mit einer Firewall abzuschotten, wenn sie überhaupt irgendwelche Programme benutzen wollen.“ [ches96]*

Aufgrund der Größe des Internet und den damit verbundenen Gefahren wird meist empfohlen, ein IT-System nur über ein Firewall-System an das Internet anzuschließen. Ähnlich wie eine Brandschutzmauer in einem Haus die Ausbreitung von Feuer verhindert, soll ein Firewall-System vor An- und Übergriffen aus dem Internet schützen [siya95].

Man bezeichnet ein Firewall-System als eine Menge von speziell geschützten Komponenten, die an einem Übergang zwischen zwei Netzen installiert sind, um diesen Übergang zu kontrollieren. Alle zwischen den Netzen ausgetauschten Daten müssen die Firewall passieren und können dabei – in Einklang mit einer explizit formulierten Sicherheitsstrategie – durchgelassen oder abgewiesen werden. Die Firewall etabliert somit *Filter* (auch als *Screens* bezeichnet) zwischen den beiden Netzen, wobei das verwendete Gateway auch als *demilitarisierte Zone (DMZ)* bezeichnet wird. Abbildung 3.5 zeigt exemplarisch das Schema einer Firewall.

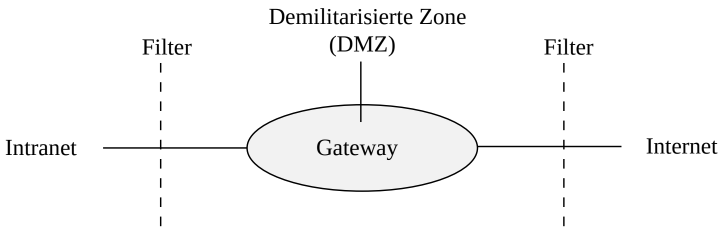

Abbildung 3.5: Schema einer Firewall

Die zwei angesprochenen Netze müssen nicht notwendigerweise das Internet sein. Der Einsatz von Firewalls läßt sich auch auf X.25 oder ATM-Netze übertragen. Ebenfalls möglich ist der Einsatz von firmeninternen Firewalls, um z.B. verschiedene Organisationseinheiten gegenseitig abzuschotten.

Eine explizit formulierte Sicherheits- oder Firewall-Strategie kann z.B. festlegen, daß bestimmte Anwendungsprotokolle und Dienste, wie NFS (Network File System) oder NIS (Network Information Service), nicht, bzw. nur in einer Richtung oder nur zwischen bestimmten Rechnern zu unterstützen sind. Sie kann auch festlegen, daß IP-Pakete mit Source Routing in jedem Fall abzuweisen sind. Systeme, die diese Funktionen realisieren, werden als Zugriffskontrollsysteme bezeichnet.

Damit ein Firewall-System eine Sicherheitsstrategie umsetzen kann, braucht es Information. Die für ein Firewall-System aus Datenpaketen ersichtliche Information hängt in erster Linie von der Schicht ab, auf der es arbeitet. Im Rahmen von Firewalls können drei unterschiedliche Zugriffskontrollsysteme unterschieden werden, die alleine oder in Kombination eingesetzt werden können.

3.6.1 Paketfilter

Paketfilter sind Systeme, die in der Lage sind, Datenpakete nach Kriterien wie

- Sende-, Empfangsadresse,

- Protokolle,
- Protokoll-Ports und
- benutzerdefinierten Bitmasken

zu filtern. Damit kann bei korrekter Konfiguration der Filter ein erster Schutz des Netzwerks erzielt werden. Paketfilter werden mit Hilfe von Filtertabellen realisiert, die bei großen Netzwerken leicht unübersichtlich und fehlerhaft werden können. Paketfilter werden vielfach als Vorfilter für weitere Firewall-Komponenten nach dem Circuit- oder Application-Relay-Prinzip benutzt. Bild 3.6 zeigt unter anderem die Funktion von Paketfiltern anhand des OSI-Referenzmodells. Die Wirkungsweise beschränkt sich demnach im wesentlichen auf die Filterung des Datenstromes der Netzwerkschicht bzw. der Vermittlungsschicht.

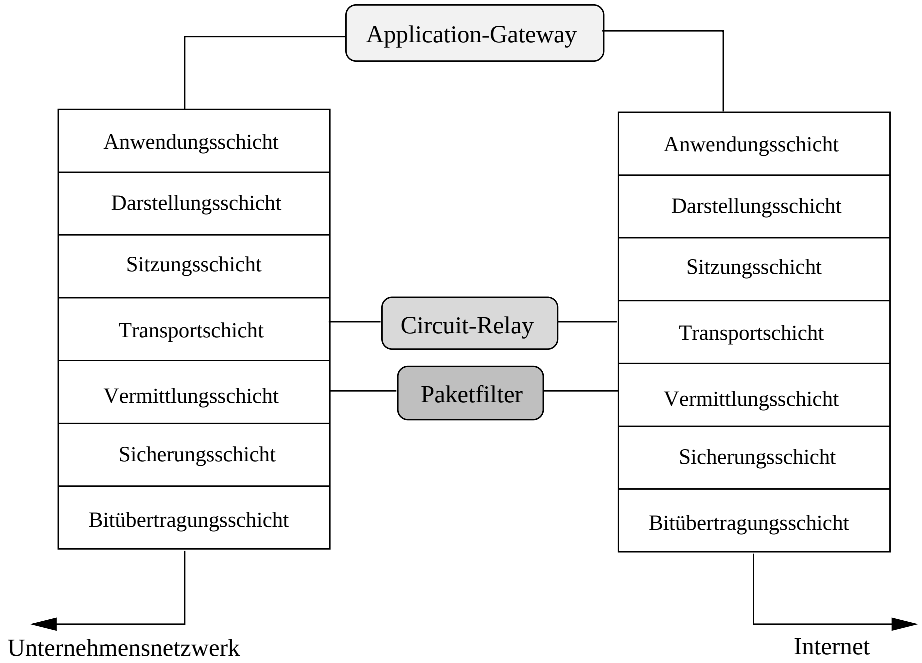

Abbildung 3.6: Zugriffskontrollsysteme

3.6.2 Circuit Relays

Eine deutliche Erhöhung der Netzwerksicherheit wird durch den Einsatz von auf Circuit Relays basierenden Firewall-Komponenten erreicht. Circuit Relays ermöglichen den Betrieb von auf den Kommunikationsprotokollen TCP oder UDP aufsetzenden Applikationen wie WWW, Gopher oder Telnet, ohne eine durchgehende Kommunikationsverbindung auf Protokollebene zuzulassen. Das

Circuit Relay fungiert quasi als Vermittlungsstelle für das betreffende Protokoll. Alle eingehenden Verbindungen enden hier und werden am gegenüberliegenden Ausgang neu aufgebaut. Ein Nachteil dieser Systeme besteht darin, daß die Client-Applikationen, um mit dem jeweiligen Circuit Relay zusammenarbeiten zu können, angepaßt werden müssen (Bild 3.6).

3.6.3 Application Relays

Application Relays gehen noch einen Schritt über die Funktionsweise von Circuit Relays hinaus. Auch sie ermöglichen die Nutzung von Anwendungen, ohne eine das Firewall-System durchbrechende darunterliegende Kommunikationsverbindung auf Protokollebene zulassen zu müssen. Darüber hinaus verhalten sie sich aus Sicht der Client-Programme wie ein Server-System des jeweiligen Dienstes. Die Client-Systeme müssen daher nicht modifiziert werden (Bild 3.6).

3.6.4 Topologie von Firewallsystemen

Grundsätzlich kann zwischen den folgenden Firewall-Architekturen unterschieden werden:

- Begrenzungs-Router,
- Begrenzungs-Router mit abgesichertem Zwischennetz (Screened Subnet, Secure Subnet),
- Dual-Home-Bastion-Host mit Paketfilter,
- Dual-Home-Bastion-Host mit Circuit-Relay,
- Dual-Home-Bastion-Host mit Application-Relay.

Einfache Begrenzungs-Router stellen im Vergleich eine geringere Sicherheitsstufe dar, kaskadierte Dual-Home-Bastion-Hosts bieten einen größeren Schutz.

3.6.4.1 Begrenzungs-Router

Begrenzungs-Router bestehen entweder aus Router-Systemen mit aktivierter Paketfilterfunktion oder aus einem Dual-Home-Host mit installierter Paketfilter-Software. Firewalls, die ausschließlich aus einem Begrenzungs-Router bestehen, sind kostengünstig, stellen allerdings einen geringeren Schutz dar [full97].

3.6.4.2 Begrenzungs-Router mit abgesichertem Zwischennetz

Mit Hilfe eines abgesicherten Zwischennetzes kann der durch Begrenzungs-Router gewährleistete Schutz erhöht werden. Der Begrenzungs-Router wird dabei so konfiguriert, daß lediglich Verbindungen von bzw. zu dedizierten und gesicherten internen Systemen möglich sind. Diese besonders gesicherten Systeme werden als abgesichertes Zwischennetz bezeichnet.

3.6.4.3 Dual-Home-Bastion-Hosts

Auf Dual-Home-Bastion-Hosts aufbauende Firewall-Systeme sind in der Lage, einen wesentlich höheren Schutz zu bieten. Bastion-Hosts sind in der Lage, interne und externe Netzwerke auf Applikationsebene miteinander zu koppeln, ohne auf Protokollebene eine Verbindung zuzulassen (einzige Ausnahme bieten Bastion-Hosts mit Paketfiltern) [full97].

Ein Bastion-Host ist ein Computer-System, das physikalisch zwischen dem internen Netzwerk und dem nicht vertrauenswürdigen Netzwerk (Internet, Anbindung an Partnerfirmen etc.) plaziert ist. Bastion-Hosts können als Paketfilter, als Circuit-Relay oder als Application-Relay konfiguriert werden. Sie stellen die zentrale Komponente eines Firewall-Systems dar [siya95].

3.6.5 Die Grenzen von Firewalls

Firewallsysteme 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 eventuell in Form von Viren oder auf andere Art und Weise (Protocol Tunneling) das interne Netzwerk bedrohen, können nicht blockiert werden. Zu vielfältig sind die Möglichkeiten Dateninhalte zu kodieren, um auch diese Art der Bedrohung ausfiltern zu können.

Es werden aber inzwischen kommerzielle Anwendungen eingesetzt, die entsprechend die beschriebene Problematik aufgreifen und beispielsweise versuchen sogenannte Viren zu erkennen und zu filtern.

3.7 Kryptographie

Die *Kryptographie* ist jenes Teilgebiet der *Kryptologie*, das sich mit dem Ver- und Entschlüsseln von Nachrichten befaßt. Für alle der in diesem Kapitel vorgestellten kryptographischen Verfahren gilt, daß deren Sicherheit sich nicht aus der

Verschleierung des Verfahrens, sondern aus der Qualität des Algorithmus ergibt. Mathematische Grundlagen zur Kryptologie wie beispielsweise die Faktorisierung, die Modularisierung, die Erzeugung von Primzahlen oder die Moduloexponentiation werden in [baur:93, denn82, smit97, schn96]

Eine Nachricht in ihrer Originalform wird *Klartext* genannt, die transformierten Daten werden als *Schlüsseltext* bezeichnet. Die Transformation vom Klartext zum Schlüsseltext nennt man *Verschlüsselung*, die inverse Transformation *Entschlüsselung*.

In einem Verfahren nach Abbildung 3.7 liegt die Sicherheit nur in der Verwendung des Ver- bzw. Entschlüsseln der Daten. Dieses Verschlüsselungsprinzip ist in der Praxis nicht sehr brauchbar, da einerseits jedes Verfahren nach einer bestimmten Zeit durchschaut wird, und andererseits alle Kommunikationspartner ein eigenes Verschlüsselungsverfahren entwickeln müßten. In Abbildung 3.7 und in den folgenden Abbildungen bezeichnet M den Klartext, der verschlüsselt werden soll. Ferner bezeichnen die Funktionen $E(M)=C$ und $D(C)=M$ die Verschlüsselungsfunktion (engl.: encode) bzw. die Entschlüsselungsfunktion (engl.: decode). Der Schlüsseltext wird C genannt.

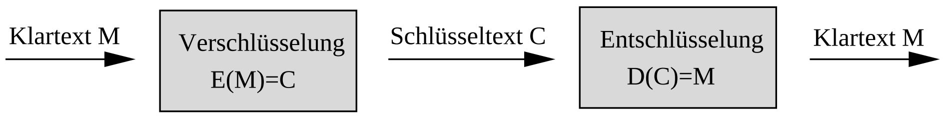

Abbildung 3.7: Prinzip der Verschlüsselung

Um dieses Problem zu lösen, bieten sich sogenannte *Schlüssel* (engl.: Key) an, die als Parameter an die jeweilige Verschlüsselungsfunktion übergeben werden. Abbildung 3.8 stellt dieses Prinzip exemplarisch dar, wobei der Schlüssel von $E(M)$ mit K_E und der Schlüssel von $D(C)$ mit K_D bezeichnet wird.

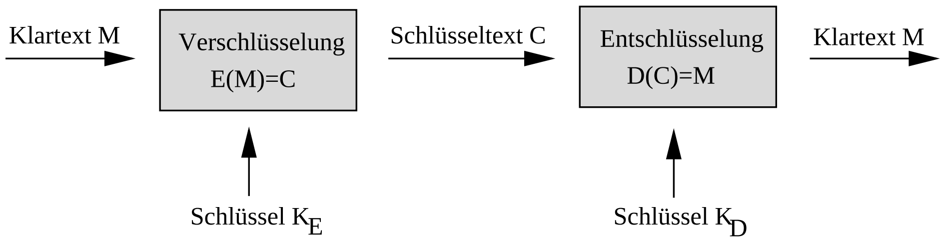

Abbildung 3.8: Schlüsselgesteuerte Verschlüsselung

Unter einem Schlüssel versteht man in diesem Zusammenhang eine sehr große Zahl. Werte für einen Schlüssel sind zum Beispiel 64 oder 128 Bit Schlüssellängen für symmetrische und 512, 1024 oder 2048 Bit für asymmetrische Verfahren.

Alle in diesem Kapitel beschriebenen Verschlüsselungsverfahren sind bekannt und wurden geprüft und getestet. Den Vorgang, den Versuch, eine konzeptionelle

Schwachstelle in einem Verschlüsselungsverfahren zu finden, nennt man *Kryptoanalyse*. Ziel der Kryptoanalyse ist es, den gesuchten Schlüssel schneller zu finden, als dies durch ein konsequentes Testen aller möglichen Schlüssel der Fall ist, ein sogenannter Brute-Force-Angriff (engl.: Exhaustive Search oder Brute Force Attack).

Mit Hilfe von Verschlüsselungsmechanismen können Daten in eine für jeden unverständliche Form transformiert werden, der nicht in Besitz des geheimen Entschlüsselungscodes ist. Damit können sensitive Daten auf Speichermedien für mögliche Einbrecher unleserlich gemacht oder über ungesicherte Netzwerke wie das Internet übertragen werden.

Neben der Vertraulichkeit durch die Verschlüsselung des Klartextes kann mit den Methoden der Kryptographie auch die Authentizität einer Nachricht sowie die Integrität einer Datei sichergestellt werden.

Die Kryptographie kennt verschiedene Methoden der Verschlüsselung:

- Symmetrische Verschlüsselung
- Hash-Verfahren
- Asymmetrische Verschlüsselung

3.7.1 Symmetrische Verschlüsselung

Die Gruppe der symmetrischen Alogorithmen zeichnet sich dadurch aus, daß zur Entschlüsselung der gleiche Schlüssel verwendet wird wie zur Verschlüsselung: $K_E = K_D = K$

Symmetrische Verschlüsselungsverfahren (engl.: Single-Key Cryptography oder Secret-Key Cryptography) teilen alle denselben Problembereich – die Übergabe des geheimen Schlüssels von Absender zu Empfänger. Vor allen bei einer großen Anzahl von Teilnehmern, die alle verschlüsselt miteinander kommunizieren, ist die sichere Übertragung des geheimen Schlüssels ein bedeutsames Problem aller symmetrischen Verfahren. Dieser Vorgang – das Erzeugen, Übertragen und die Speicherung von Schlüsseln – wird in weiterer Folge auch als Schlüsselverwaltung (engl.: Key Management) bezeichnet.

Eines der bekanntesten symmetrischen Verfahren ist der amerikanische Verschlüsselungsstandard DES (Data Encryption Standard), der bereits seit 1976 als Regierungsstandard für nichtklassifizierte Kommunikation dient [schn96]. DES verwendet in seiner ursprünglichen Form einen 56 Bit langen Schlüssel, der Suchraum für einen reinen Brute-Force-Abgriff beträgt in diesem Fall folglich 2^{56} Möglichkeiten. Die Funktionsweise des DES-Algorithmus besteht in der wiederholten Anwendung einer Reihe von logischen Operationen auf 64-Bit-Daten-

Schlüssellänge	Maximale Zeit für Brute-Force-Angriff
40 Bit	0,4 Sekunden
56 Bit	7 Stunden
64 Bit	74 Stunden, 40 Minuten
128 Bit	157.129.203.952.300.00 Jahre

Tabelle 3.1: Zeit für Brute-Force-Angriff auf DES

Schlüssellänge	Maximale Zeit für Brute-Force-Angriff
40 Bit	15 Tage
56 Bit	2.691,49 Jahre
64 Bit	689.021,57 Jahre
128 Bit	12.710.204.652.610.000.000.000.000 Jahre

Tabelle 3.2: Zeit für Brute-Force-Angriff auf RC4

Blöcke. Aus diesem Grund wird DES auch den sogenannten Block-Algorithmen zugeordnet (engl.: Block Ciphers).

Die Sicherheit von DES ist in den letzten Jahrzehnten wiederholt diskutiert worden, auch einige für die Praxis bedeutungslose analytische Angriffspunkte wurden entdeckt. Ein interessanter Aspekt ist in diesem Zusammenhang die maximale Dauer eines Brute-Force-Angriffs. Tabelle 3.1 zeigt Werte für diese Zeitspanne bei unterschiedlichen Schlüssellängen [star97].

DES unterliegt in vollem Ausmaß den gegenwärtigen geltenden amerikanischen Exportbeschränkungen, die den Export von kryptographischen Produkten genehmigungspflichtig machen. Exportgenehmigungen für DES wurden nahezu nie erteilt [rsa98].

RC2 und RC4 sind symetrische Verschlüsselungsverfahren, die beide von dem amerikanischen Wissenschaftler Ron Rivest für die Gesellschaft RSA Data Security entwickelt wurden. Die Details der Algorithmen wurden von der Gesellschaft bisher nicht veröffentlicht.

Beide Verfahren sind – im Gegensatz zu DES – unabhängig von einer bestimmten Schlüssellänge und können daher unterschiedlichen Sicherheitsanforderungen angepaßt werden. Sie sind schneller in der Durchführung der Ver- und Entschlüsselungsoperationen als DES [rsa98] und gegenüber einem Brute-Force-Angriff widerstandsfähiger. Tabelle 3.2 zeigt Werte für die maximale Dauer eines solchen Angriffs bei unterschiedlichen Schlüssellängen [star97].

Der Vergleich der Tabelle 3.1 und der Tabelle 3.2 zeigt, daß RC4 schon bei einer Schlüssellänge von 40 Bit wesentlich sicherer als DES ist. Ferner sind bei diesen Vefahren die Exportbeschränkungen nicht so drastisch wie bei DES. Bei einer Schlüssellänge bis zu inklusive 40 Bit werden RC2 und RC4 üblicherweise genehmigt.

Andere häufig genannte Verfahren sind der von Bruce Schneier entwickelte Block-Algorithmus *Blowfish* sowie das von Xuejia Lai und James Massey entworfene Verschlüsselungsverfahren IDEA (International Data Encryption Algorithm) [schn96].

3.7.2 Hash-Verfahren

Eine Hash-Funktion $H(M)=h$ erzeugt aus binären Daten unterschiedlicher Länge eine Zeichenkette fixer Länge, die auch als digitaler Fingerabdruck bezeichnet wird (engl.: digital fingerprint). Das Hash-Verfahren muß eine Einweg-Funktion darstellen, der Vorgang darf also nicht umkehrbar sein. Darüber hinaus gilt noch die Anforderung, daß bei gegebenen digitalen Fingerabdruck die Ermittlung einer zweiten Nachricht, welche den gleichen Fingerabdruck aufweist, hinreichend schwer ist. Schwer bedeutet in diesem Zusammenhang, daß es keinen Algorithmus gibt, der das Finden der Lösung vereinfacht, als das Durchprobieren aller Möglichkeiten. Abbildung 3.9 zeigt die prinzipielle Idee zur Bildung eines Hash-Wertes.

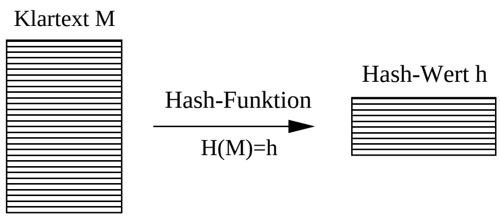

Abbildung 3.9: Berechnung eines Hash-Wertes

Einweg-Hash-Funktionen müssen folgende drei Eigenschaften erfüllen:

- ist M gegeben, so ist die Berechnung von h einfach
- ist h gegeben, so ist es schwer M zu berechnen, so daß H(M)=h
- ist M gegeben, so ist es schwer ein M' zu finden , so daß H(M)=H(M')

Eine Hash-Funktion ist öffentlich und jeder der den Algorithmus kennt, kann jederzeit den Hash-Wert berechnen. Ein wichtiges Anwendungsgebiet des digitalen Fingerabdrucks liegt in der Möglichkeit der Erzeugung von digitalen Unterschriften (siehe Kapitel 3.7.4).

3.7.3 Asymmetrische Verschlüsselung

Ein Paradigma der symmetrischen Kryptographie änderte sich im Jahr 1976 auf grundlegende Art und Weise: Whitfield Diffie und Martin Hellman beschrieben erstmals ein kryptographisches Verfahren, das auf den Einsatz von zwei einander zugeordneten Schlüsseln beruhte. Zwei Jahre später wurde ein – auf dem gleichen Prinzip basierendes – komplettes Verfahren publiziert, das nach den Initialen der drei Entwickler Ron Rivest, Adi Shamir und Leonard Adleman *RSA-Verfahren* genannt wurde. Nach deren bedeutender Eigenschaft, dem Einsatz von zwei unterschiedlichen Schlüsseln zur Ver- und Entschlüsselung, bezeichnet man diese Verfahren auch als *asymmetrisch* oder *Public-Key-Verfahren*. Abbildung 3.10 zeigt den Einsatz eines asymmetrischen Verfahrens zur Übertragung einer verschlüsselten Nachricht. Um den Klartext zu kodieren, wird der öffentliche Schlüssel K_O des Empfängers eingesetzt, dieser wiederum kann die Nachricht mit dem zugehörigen privaten Schlüssel K_G entschlüsseln. Ein wesentliches Charakteristikum vollständiger Public-Key-Verfahren ist die Tatsache, daß beide Schlüssel die Eigenschaften aufweisen, daß die mit dem einen Schlüssel verschlüsselte Nachricht nur mit dem zugehörigen zweiten Schlüssel entschlüsselt werden kann. Während einer der Schlüssel an möglichst alle potentiellen Sender einer Nachricht verteilt und dadurch zum öffentlichen Schlüssel wird, muß der andere unter allen Umständen geheimgehalten werden.

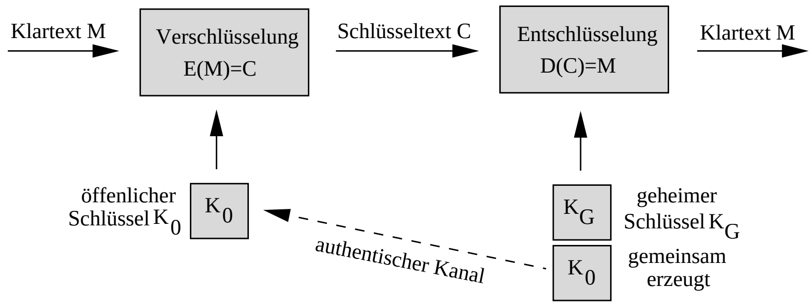

Abbildung 3.10: Public-Key-Kryptographie

Beide Schlüssel werden gemeinsam bei der Schlüsselgenerierung erzeugt und es ist unmöglich, von einem der beiden Schlüssel direkt auf den anderen zu schließen. Öffentliche Schlüssel können auf mehrere Arten verteilt werden. Eine Möglichkeit bieten Key-Server, eine Art Telefonbuch für öffentliche Schlüssel, aber auch Webseiten oder Signaturen von E-Mails können für diesen Zweck verwendet werden.

Wird zur Kommunikation zwischen mehreren Teilnehmern ein asymmetrisches Verfahren eingesetzt, so ändert sich auch die Anforderung an das Schlüsselmanagement. Die Übertragung des öffentlichen Schlüssels ist nicht mehr der zentrale Problembereich, da dieser nicht zum Lesen der verschlüsselten Nachrichten ermächtigt. Von Bedeutung ist aber die Frage, ob tatsächlich der gewünschte Empfänger der Nachricht im Besitz des zugehörigen privaten Schlüssels ist. Der kritische Aspekt beim Einsatz von Public-Key-Kryptographie ist es, eine zuverlässige Zuordnung zwischen der Identität des Empfängers der Nachricht und dessen öffentlichen Schlüssel zu erhalten.

Der öffentliche Schlüssel muß über einen authentischen Kanal übertragen werden, um eine eindeutige Zuordnung zwischen Kommunikationspartnern und öffentlichen Schlüssel gewährleisten zu können.

Es wurde bereits erwähnt, daß konzeptionell kein Unterschied zwischen den beiden Schlüsseln besteht; folglich ist auch der umgekehrte Vorgang möglich: Eine mit dem privaten Schlüssel kodierte Nachricht kann von allen Personen entschlüsselt werden, die sich im Besitz des zugehörigen öffentlichen Schlüssels befinden. Dieser Vorgang wird auch als die Erstellung einer *digitalen Unterschrift* bezeichnet. Nur der Besitzer des privaten Schlüssels kann ein Dokument auf diese Weise unterschreiben, die digitale Unterschrift kann aber von allen Inhabern des öffentlichen Schlüssels verifiziert werden.

Der RSA-Algorithmus ist heute eines der am meisten eingesetzten Public-Key-Verfahren, das sowohl zur Verschlüsselung als auch zur Erzeugung von digitalen Unterschriften verwendet werden kann.

Allen asymmetrischen Verfahren liegt das Konzept der Einweg-Funktion zugrunde, die ohne eine zusätzliche Information nicht oder nur sehr schwer reversiert werden kann. Im Fall des RSA-Algorithmus handelt es sich bei dieser Einweg-Funktion um das Produkt zweier großer Primzahlen. Zur Umkehrung dieser Funktion ist es folglich notwendig, dieses Produkt – den sogenannten Modulus – zu faktorisieren. Die Komplexität dieses Vorgangs ist die Grundlage der Sicherheit des RSA-Algorithmus. Ein Angreifer, der in der Lage wäre, die Faktorisierung schnell genug durchzuführen, um den gesamten Suchraum in vertretbarer Zeit abdecken zu können, wäre in der Lage, aus dem öffentlichen den privaten Schlüssel abzuleiten [schn96].

Da eine größere Zahl schwieriger zu faktorisieren ist, hängt die Sicherheit von RSA von der Größe des Modulus ab. Nach eigenen Angaben der RSA Data Security [rsa98] dauert die vollständige Faktorisierung eines 512-Bit-Schlüssels gegenwärtig acht Monate bei einem Aufwand von unter einer Million US-Dollar. Die von RSA empfohlenen Schlüssellängen liegen bei 768 Bit für den persönlichen Gebrauch, 1024 Bit im kommerziellen Einsatz und 2048 Bit für sensitive Situationen.

Hinsichtlich der benötigten Rechenleistung besteht ein großer Unterschied zwischen Verschlüsselungsoperationen mit symmetrischen und asymmetrischen Verfahren – letztere sind etwa um den Faktor 100 langsamer als erstere.

3.7.4 Digitale Unterschriften

Wie bereits in Kapitel 3.7.3 erwähnt, können Nachrichten mit digitalen Unterschriften versehen werden. Will der Autor einer Nachricht beweisen, daß diese von ihm verfaßt wurde, so führt er eine Verschlüsselung mit seinem geheimen Schlüssel durch. Wegen der Äquivalenz zur Unterschrift spricht man hier von einer digitalen oder elektronischen Unterschrift.

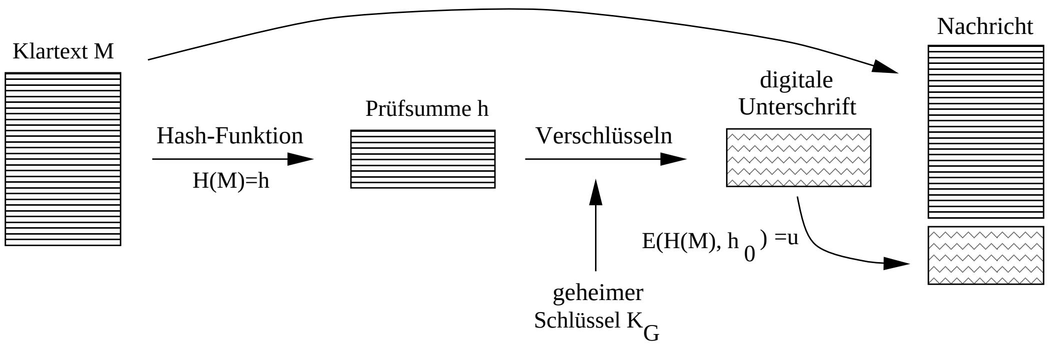

Abbildung 3.11: Erstellen einer digitalen Unterschrift

In der Praxis wird jedoch nicht die gesamte Nachricht verschlüsselt. Statt dessen wird aus der Nachricht mit einer Hashfunktion eine Prüfsumme fixer Länge gebildet, die dann mit dem geheimen Schlüssel verschlüsselt wird. Abbildung 3.11 stellt diesen Vorgang exemplarisch dar.

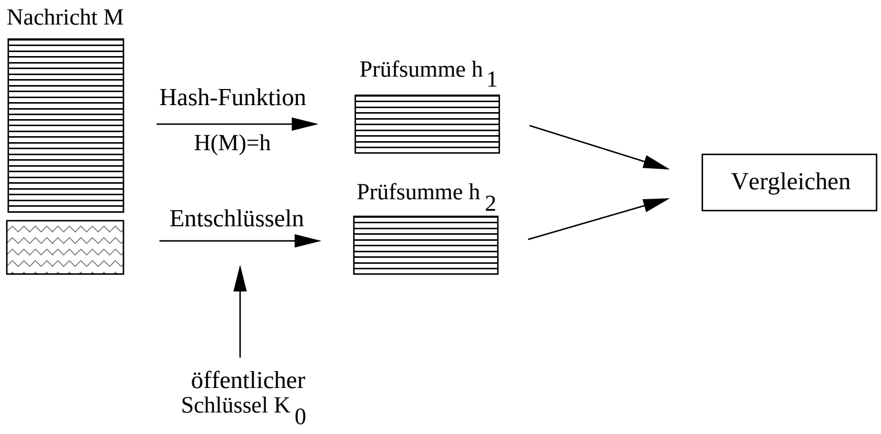

Abbildung 3.12: Prüfen einer digitalen Unterschrift

Will nun der Empfänger die Unversehrtheit der Nachricht überprüfen, so bildet er mit dem gleichen Verfahren eine Prüfsumme und entschlüsselt mit Hilfe des öffentlichen Schlüssels die mitgesandte Prüfsumme. Sind beide Prüfsummen gleich, so kennt er den Urheber der Nachricht und hat zusätzlich – im Gegensatz zur handschriftlichen Unterschrift – die Gewißheit, daß keine Daten verändert wurden (Abbildung 3.12).

Will man die elektronische Unterschrift mit Vertraulichkeit kombinieren, so ist eine zusätzliche Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers notwendig. Auf diese Weise lassen sich elektronische unterschriebene Nachrichten vertraulich über ein unsicheres Netz übertragen. Würde man die Nachricht nur verschlüsseln, so kann der Empfänger nicht nachprüfen, ob der Absender auch wirklich der Urheber der Nachricht ist, da jeder den öffentlichen Schlüssel des Empfängers verwenden könnte.

3.7.5 Anwendung kryptographischer Verfahren

Abbildung 3.13 zeigt eine beispielhafte Übertragung einer Nachricht über das Internet. Das Verfahren greift sowohl auf eine asymmetrische Verschlüsselung als auch auf den Mechanismus einer digitale Unterschrift zurück.

Die Nachricht wird zunächst mit dem privaten Schlüssel des Absenders unterschrieben und anschließend mit dem öffentlichen Schlüssel des Empfängers kodiert. Die Nachricht wird dann über das Internet zum Empfäger übertragen. Der Empfänger dekodiert mit seinem privaten Schlüssel die Nachricht und überprüft mit dem öffentlichen Schlüssel des Absenders die digitale Unterschrift.

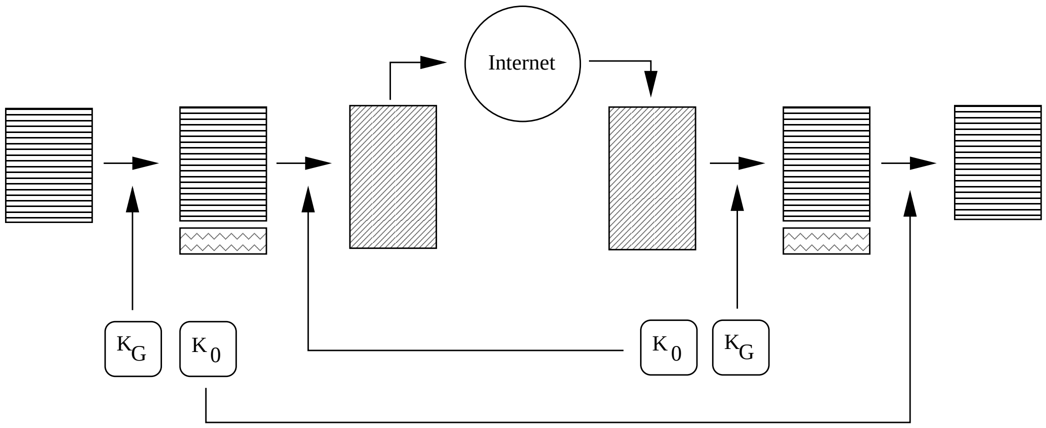

Abbildung 3.13: Anwendung kryptographischer Verfahren

Auf diese Weise können folgende Vorteile gegenüber der unverschlüsselten Übertragung erzielt werden:

- Die *Authentizität* des Absenders wird durch die digitale Unterschrift, die des Empfängers durch Verschlüsselung mit dessen öffentlichen Schlüssel garantiert.

- Die *unveränderte Übertragung* der Nachricht wird mit Hilfe der digitalen Unterschrift sichergestellt.
- Die *Uneinsehbarkeit des Inhaltes* ist auf Grund der (asymmetrischen) Verschlüsselung des Inhaltes gewährleistet.
- Die *Nichtabstreitbarkeit des Absendevorganges* der Nachricht wird ebenfalls mit Hilfe der elektronischen Unterschrift erreicht.

Eine beschriebene Anforderung kann mit den hier vorgestellten Verfahren nicht erfüllt werden: Die *Nichtabstreitbarkeit des Empfangsvorgangs* kann nur durch eine digital unterschriebene Bestätigung des Empfangsvorgangs seitens des Empfängers realisiert werden.

3.7.6 Zertifikate und Zertifizierungsinstanzen

Bei der Einführung von Sicherheitsmaßnahmen für die Datenübertragung im Internet nehmen Zertifzierungsstellen eine zentrale Bedeutung ein. Sie sind verantwortlich für die Zuordnung einer Identität zu einem öffentlichen Schlüssel und ermöglichen so eine effiziente Nutzung von asymmetrischen Verschlüsselnugsverfahren.

Eine vertrauliche Kommunikation ist nur dann gewährleistet, wenn die dabei verwendeten öffentlichen Schlüssel authentisch sind. Es muß also nachweisbar sein, daß es sich wirklich um den öffentlichen Schlüssel des Kommunikationspartners handelt.

Im Abschnitt 3.7.4 wurde beschrieben, wie mit digitalen Unterschriften die Identität des Kommunikationspartners festgestellt werden kann. Dieser Nachweis funktioniert jedoch nur dann, wenn der zur Verifikation verwendete öffentliche Schlüssel auch wirklich von der Person stammt, von der man annimmt, der Urheber der Nachricht zu sein.

Man erkennt, der öffentliche Schlüssel braucht zwar nicht geheimgehalten zu werden, aber er muß eindeutig einer Person zugeordnet werden können. Diese Zuordnung wird mit Zertifikaten erreicht, die von Zertifizierungsinstanzen ausgestellt werden.

3.7.6.1 Zertifizierungsinstanzen

Zertifizierungsinstanzen (Certification Authorities, CAs) sind vertrauenswürdige, unabhängige Organisationen, die mittels Zertifikaten bestätigen, daß ein bestimmter öffentlicher Schlüssel einer bestimmten Person oder Organisation gehört. Zu diesem Zweck werden die Daten des Inhabers sowie sein öffentlicher Schlüssel mit dem geheimen Schlüssel der Zertifizierungsinstanz elektronisch unterschrieben. Mit dem öffentlichen Schlüssel der Zertifizierungsinstanz können somit alle Zertifikate, die von dieser Instanz ausgestellt wurden, überprüft werden.

Das Problem der Zuordnung Zertifikat↔Inhaber liegt nun bei den Zertifizierungsstellen. Welche Daten die Zertifizierungsstelle wie streng prüft, wird in der öffentlich verfügbaren Zertifizierungs-Policy (Zertifizierungs-Verfahrensweise) festgehalten. Daraus folgt, daß je nach Zertifizierungsinstanz ein Zertifikat mehr oder weniger vertrauenswürdig ist. Dieses System kann man dadurch mit herkömmlichen Ausweisen vergleichen. Ein Personalausweis oder Reisepaß ist zur Feststellung der Identität vertrauenswürdiger als zum Beispiel ein Schülerausweis.

Neben der Zertifizierungs-Policy gibt es einen weiteren Grund für die Entstehung verschiedener Zertifizierungsstellen: Die große Anzahl von Internetbenutzern kann nur schwer von einer einzigen Instanz verwaltet werden.

Um nun zu verhindern, daß ein Benutzer wieder alle öffentlichen Schlüssel der jeweiligen Zertifizierungsinstanz benötigt, wurden Zertifizierungshierarchien eingeführt. Dabei zertifiziert eine Stelle nicht nur Benutzer, sondern auch andere Zertifizierungsstellen. Wie in Abbildung 3.14 zu erkennen ist, entsteht eine baumartige Struktur mit einer Wurzel, der sogenannten Top-Level CA.

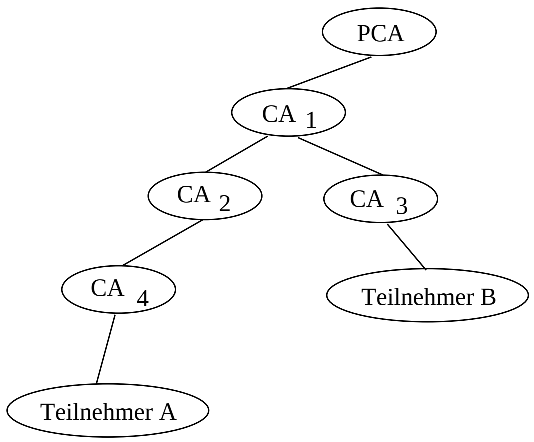

Abbildung 3.14: Einfache Zertifizierungshierarchie

Die oberste Zertifizierungsstelle wird auch als PCA (Policy Certification Authority) bezeichnet, da sie die Mindestanforderung der Zertifizierungs-Verfahren (Policy) für den gesamten Baum vorgibt. Im Gegensatz zu gewöhnlichen CAs werden von ihr keine Teilnehmer, sondern nur andere Zertifizierungsstellen zertifiziert.

Erhält nun Teilnehmer A auf irgendeinem Weg das Zertifikat von Teilnehmer B, so existieren grundsätzlich zwei Möglichkeiten das erhaltene Zertifikat zu überprüfen:

Im ersten Fall erhält ein Teilnehmer bei seiner Zertifizierung nur das Zertifikat der Top-Level CA über einen sicheren Kanal.

Will Teilnehmer A das Zertifikat von Teilnehmer B überprüfen, so braucht er nur die Zertifikate aller über Teilnehmer B liegenden Zertifizierungsinstanzen zu holen. Nun kann er von oben beginnend mit seinem sicheren Zertifikat der PCA eine Zertifizierungsstelle nach der anderen als authentisch erkennen. Schließlich erreicht er auch das Zertifikat von CA_4, mit dessen öffentlichen Schlüssel er auch das Zertifikat von Teilnehmer B überprüfen kann.

Im zweiten Fall erhält ein Teilnehmer bei seiner Zertifizierung nur das Zertifikat der ihn zertifizierenden Stelle. In diesem Fall wird jedoch vorausgesetzt, daß jede Zertifizierungsstelle sowohl ihre darunterliegenden als auch ihre darüberliegende CA zertifiziert.

Will Teilnehmer A das Zertifikat von Teilnehmer B überprüfen, so muß er in diesem Fall von unten ausgehend solange nach oben weitergehen, bis er eine Zertifizierungsstelle erreicht, die beiden gemeinsam ist. In einem extremen Fall ist das die Top-Level CA. Mit dem öffentlichen Schlüssel von CA_3 kann er das Zertifikat von CA_2 und auf dieselbe Art das Zertifikat von CA_1 verifizieren.

Nun kann er den Zertifizierungsast wie im ersten Beispiel beschrieben nach unten weiterverfolgen und überprüfen.

Um sich diese Prozedur bei weiteren Verifikationen von Teilnehmern zu ersparen, können die überprüften und als sicher erkannten Zertifikate auch in einer lokalen Datenbank gespeichert werden. Diese Arten von Zertifizierungshierarchien werden im Standard X.509 näher spezifiziert [stru95].

Eine Zertifizierungsstelle kann von ihr ausgestellte Zertifikate auch widerrufen. Jede CA besitzt daher eine Liste, die alle widerrufenen Zertifikate enthält. Diese Liste wird CRL (Certificate Revokation List) genannt. Beim Empfang eines neuen Zertifikates sollte gepüft werden, ob das Zertifikat noch gültig ist.

3.7.6.2 Zertifikate

Wie bereits erwähnt, sind Zertifikate von Zertifizierungsinstanzen elektronisch unterschriebene Daten des Zertifikatinhabers. Die Empfehlung X.509 Version 1 wurde 1988 veröffentlicht und beschreibt das Authentifizierungs-System für X.500 Directories sowie die X.509 Zertifikat-Syntax.

Ein Zertifikat nach X.509 dient in erster Linie der Bindung eines öffentlichen Schlüssels an eine bestimmte Person. Abbildung 3.15 zeigt den Aufbau eines X.509-Zertifikates in der Version 1. In Bezug auf die Bindung sind die beiden Felder *öffentlicher Schlüssel* sowie der *Name des Benutzers* von Bedeutung. Darüber hinaus sind die Versionsnummer des Formates, die innerhalb einer Zertifizierungs-

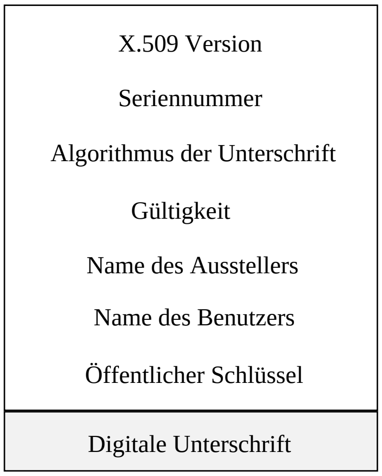

Abbildung 3.15: Aufbau eines X.509 Zertifikates

Kennung	Erklärung	Beispiel
c	Country, Land	de
o	Organisation	Uni-Dortmund
ou	Organisational Unit, Abteilung	Informatik
cn	Person	Christian Fiebig

Tabelle 3.3: X.509-Hierarchie

stelle eindeutigen Seriennummer, der zur Erstellung der digitalen Unterschrift eingesetzte Algorithmus und die Gültigkeitsdauer des Zertifikates enthalten. Der Name der ausstellenden Zertifizierungsstelle gibt einen Hinweis auf die Anforderungen, die für die Ausstellung des Zertifikates zu erfüllen waren, sowie auf den öffentlichen Schlüssel, der zur Überpüfung der digitalen Unterschrift des Zertifikates eingesetzt werden muß.

Mit dem Ziel, ein globales Verzeichnis zu schaffen, definieren die OSI-Standards auch einen globalen Namensraum, der die Bezeichnug aller Personen mit Hilfe eines eindeutigen Namens (engl.: Distinguished Name, DN) erlauben soll. Eindeutige Namen bestehen aus mehreren hierarchisch angeordneten Komponenten, die die betreffende Person identifizieren. Tabelle 3.3 zeigt einen Ausschnitt der angesprochenen Komponenten.

In einer Baumstruktur entspricht ein Pfad in dieser Hierarchie einem eindeutigen Namen.

3.7.6.3 X.509-Sperrlisten

Ein Zertifikat kann vorzeitig seine Gültigkeit verlieren, wenn beispielsweise der Verlust des zugehörigen privaten Schlüssels vorliegt, oder weil die im Zertifikat unterschriebene Zugehörigkeit einer Person zu einer Organisation nicht mehr besteht. In diesem Fall wird die Serienummer des Zertifikates einer sogenannten Sperrliste (engl.: Certificate Revocation List, CRL) hinzugefügt, die in regelmäßigen Abständen von der Zertifizierungsstelle digital unterschrieben und veröffentlicht wird. Bei Anwendungen, die ein hohes Sicherheitsneveau erfordern, kann die relevante Sperrliste überprüft werden, bevor ein Zertifikat mit gültiger Unterschrift akzeptiert wird. Die ITU-T-Empfehlung X.509 standardisiert auch das Format der zugehörigen Sperrliste. Mit der Veröffentlichung der Version 3 des Standards wurde auch in der Sperrliste die Integration von Erweiterungen vorgesehen. Abbildung 3.16 zeigt die Struktur einer Sperrliste.

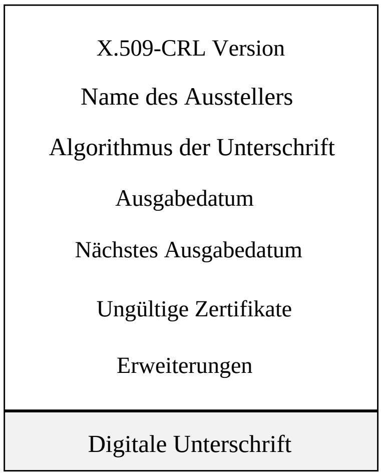

Abbildung 3.16: Aufbau einer X.509-Sperrliste

Bedeutende Felder der in Abbildung 3.16 gezeigten Sperrliste sind in erster Linie das Ausgabedatum sowie das Erscheinungsdatum einer aktuellen Version der Sperrliste. Auch die Länge des Intervalls zwischen der Ausgabe der Sperrlisten stellt ein wichtiges Kriterium einer Zertifizierungsstelle dar. Da der Widerruf eines Zertifikates erst mit der Herausgabe der nächsten Version der Sperrliste wirksam wird, kann ein kürzeres Intervall dazu beitragen, den Schaden durch einen in falsche Hände gefallenen privaten Schlüssel zu minimieren. Andererseits erhöht ein kurzes Intervall die Belastung der betroffenen Anwendungen, die jede neue Version der Sperrliste von der Zertifizierungsstelle *abholen* müssen.

3.8 Sicherheitsarchitektur im WWW

In den vorangegangenen Kapiteln wurden die technischen Rahmenbedingungen des kommerziellen Internet-Einsatzes beschrieben: Zum einen wurde gezeigt, mit welchen Schwachstellen die Internet-Technik in ihrer derzeitigen Form behaftet ist, zum anderen wurden kryptographische Verfahren als mögliche Abhilfe für diese Probleme beschrieben. Die in den vorangegangenen Kapiteln präsentierte Materie stellt folglich die Ausgangsbasis dar, mit der Unternehmen konfrontiert sind, die das Internet kommerziell nutzen wollen: Sei es als unternehmensinterne Kommunikationsinfrastruktur, sei es zur Durchführung kommerzieller Transaktionen mit Kunden über das globale Internet.

In diesem Kapitel werden die Bestandteile der Sicherheitsarchitektur eines WWW-basierten Informationssystems vorgestellt und voneinander abgegrenzt. Teilweise können die in diesem Rahmenkonzept vorgesehenen Komponenten bereits mit bestehenden Produkten realisiert werden, zum Teil sind sie noch Gegenstand kommerzieller und akademischer Forschungsbemühungen.

3.8.1 Transaktionssicherheit

Betrachtet wird vorerst die Situation eines Unternehmens, das mit Hilfe von Internet-Technik seine Leistungen an Kunden vertreiben will. Um die daraus resultierenden Anforderungen an die Übertragungssicherheit abzuleiten, kann direkt an die in den einleitenden Kapiteln aufgezählten Problembereiche angeknüpft werden. Die in weiterer Folge beschriebenen Rahmenbedingungen werden auch als *Transaktionssicherheit* bezeichnet.

- Die Kommunikationsparteien müssen sich einander gegenseitig *authentifizieren* können. Darunter ist zum einen der Nachweis der Identität bei der Herstellung einer Kommunikationsverbindung zu verstehen. Es muß darüber hinaus jedoch auch für die gesamte Dauer des Bestehens einer Verbindung verhindert werden, daß ein Betrüger den Platz einer der beiden Kommunikationsparteien einnehmen kann.

- Die *Integrität* der übertragenen Daten muß gewährleistet sein und dadurch eine Veränderung der Nachricht während der Übertragung von vornherein ausgeschaltet werden.

- Die *Uneinsehbarkeit des Inhaltes* während der Übertragung soll verhindern, daß unbefugte Personen, beispielsweise mit Hilfe von Paketfiltern Einsicht in die Daten nehmen können.

- Eine Anforderung, die im Fall von kommerziellen Transaktionen eine besondere Rolle spielt, ist die *Nicht-Abstreitbarkeit* des Absende- oder Empfangsvorganges einer Nachricht.

Die bestehenden Anwendungsprotokolle der Familie TCP/IP können durch entsprechende kryptographische Absicherung der Kommunikationskanäle um Authentizität, Integrität und Uneinsehbarkeit des Inhaltes ergänzt werden. Durch Integration in die Schichten der Internet-Protokolle kann diese Absicherung auch nahezu transparent für die betroffene Anwendungssoftware und damit auch für den Benutzer erfolgen.

Die Gewährleistung der Nicht-Abstreitbarkeit des Absende- oder Empfangsvorgangs wird jedoch sinnvollerweise als Bestandteil des *Anwendungsprotokolls* realisiert: Mit einer Authentifizierung auf der Basis kryptographischer Verfahren und der Möglichkeit der Erstellung digitaler Signaturen steht das Instrumentarium für die Bewältigung der Problematik der Nicht-Abstreitbarkeit zur Verfügung. Es fällt jedoch in den Aufgabenbereich der Anwendungsschicht, durch Protokollelemente festzulegen, wann eine derartige Absicherung notwendig ist.

Zahlreiche Protokollentwürfe auf Anwendungsebene haben auch genau dieses Thema zum Gegenstand, besonders im Bereich digitaler Zahlungsmittel. Es besteht im Fall einer Überweisung die Anforderung, daß weder der Absende- noch der Empfangsvorgang in Frage gestellt werden kann.

Beispielsweise bietet S-HTTP (Secure HTTP), eine Erweiterung von HTTP, die Möglichkeit, durch digitale Unterschriften die Nicht-Abstreitbarkeit durch den Sender oder Empfänger zu gewährleisten. Auf diese Weise können – so die rechtlichen Rahmenbedingungen dafür geschaffen werden[2] – verbindliche Angebote über S-HTTP vom Web-Server des Verkäufers zum Kunden übertragen werden.

Ein anderes Beispiel sind die im SET-Standard zur Abwicklung sicherer Kreditkartentransaktionen genormten Nachrichten zwischen Käufer, Verkäufer und Clearing-Stelle: Auch hier muß natürlich die Nicht-Abstreitbarkeit der Transaktion gewährleistet sein, die Realisierung erfolgt jedoch auf der Anwendungsebene.

3.8.2 Sicherheitsaspekte im Intranet

Die grundlegenden Anforderungen der Authentizität, Integrität und Uneinsehbarkeit des Inhaltes gelten auch für den unternehmensinternen Einsatz der Internet-Protokolle. Im Fall eines Zugriffs auf ein Dokument ist jedoch weniger die Authentifizierung des Benutzers, sondern vielmehr dessen Zugriffsberechtigung ausschlaggebend. Werden die Internet-Protokolle im unternehmensinternen Bereich

[2] Das Problem der rechtlichen Aspekte in Bezug auf das Internet ist nicht Bestandteil dieser Diplomarbeit und wird im weiteren Verlauf auch nicht weiter diskutiert.

eingesetzt, so wird die Durchführung der *Zugriffskontrolle* zum zentralen Aspekt.

Der Begriff der Zugriffskontrolle ist in der Informatik aus den Forschungsgebieten der Betriebssystem- oder Datenbank-Sicherheit gebräuchlich. Im einzelnen versteht man darunter die Bewältigung der folgenden Aufgaben [oppl97].

- Anlegen, Administration, Überwachung und Widerruf der einzelnen Zugriffsrechte (Privilegien),
- Identifikation und Authentifizierung der Benutzer,
- Überwachung der Zugriffe,
- Einschränkung bestimmter Arten von Zugriffen,
- Verhindern von unerlaubten Zugriffen.

Diese Anforderungen gelten auch für ein WWW-Informationssystem: Nicht jeder Benutzer verfügt a priori über Zugriff auf alle Web-Server, alle Mail-Server und das Recht, in jeder vorhandenen News-Gruppe Beiträge schreiben zu dürfen. Vielmehr sollen auch in einem Intranet die Zugriffsrechte auf einzelne Ressourcen in Übereinstimmung mit einem unternehmensweiten Sicherheitskonzept vergeben werden.

Im sogenannten *Orange Book*, dem Kriterienkatalog des amerikanischen Verteidigungsministerium für die C2-Zertifizierung von Softwareprodukten, wird der Begriff *Security Policy (Requirement 1)* folgendermaßen definiert [dod85]:

> *„There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object.“*

In dieser Definition sind einige wichtige Elemente enthalten: Zum einen wird hier der Begriff *Subjekt* für die zugreifende Person und die Beziehung *Objekt* für die gewünschte Ressource geprägt. Diese Terminologie zieht sich durch die gesamte Literatur zu betrieblichen Sicherheitskonzepten und wird vor allem in Zusammenhang mit Zugriffskontrollmechanismen häufig eingesetzt.

Zum anderen ist von *Zugriffsregeln* die Rede, welche die Zugriffsrechte eines Subjektes auf ein Objekt festlegen. Die Verwaltung dieser Zugriffsregeln ist eine zentrale Aufgabe des betrieblichen Sicherheitsmanagements, da auf diese Weise die Zugriffsrechte einzelner Mitarbeiter festgelegt werden. Die Struktur solcher Zugriffsregeln ergibt sich aus dem gewählten *Sicherheitsmodell* (engl.: Security Model), das die grundlegenden Eigenschaften eines Zugriffskontrollmechanismus festlegt.

Eine wesentliche Vorraussetzung für die Durchführung der Zugriffskontrolle in einem WWW-Informationssystem ist offensichtlich die Möglichkeit der *eindeutigen Identifikation der Subjekte und Objekte*. Die Objekte können mit dem in Abschnitt 2.3 beschriebene URL eindeutig identifiziert werden: Dieser beinhaltet sowohl das Objekt eines Zugriffes als auch den gewünschten Server.

Die Identifikation der Subjekte ist beispielsweise mit Hilfe des *„Distinguished Name"* möglich (siehe Kapitel 3.7.6.2).

Eine zusätzliche Anforderung an einen Zugriffskontrollmechanismus für WWW-Informationssysteme ergibt sich auch daraus, daß die Möglichkeit der Erweiterung des Systems über das Internet in Betracht gezogen werden muß. Der Zugriffskontrollmechanismus eines Intranets muß folglich neben der Verwaltung der unternehmensinternen Benutzer auch die Möglichkeit offen lassen, verschiedenen Kundengruppen unterschiedliche Zugriffsmöglichkeiten auf die Informationssourcen des Unternehmens zu schaffen.

Kapitel 4

Konzeption eines modularen Servers

4.1 Grundüberlegungen zur Architektur

Die hier präsentierte Sicherheitsarchitektur orientiert sich am abstrakten Begriff eines „Dienstes“, um die für den Betrieb eines abgesicherten WWW-Informationssystems notwendigen Komponenten und deren Aufgabe darzustellen. Solche Dienste können als Netzwerkdienst realisiert sein oder auch in anderer Form implementiert werden. An dieser Stelle ist lediglich von Bedeutung, welche Funktionalität von den einzelnen Komponenten bereitgestellt wird. Das hier präsentierte Rahmenkonzept soll sowohl den notwendigen Überblick über die einzelnen Problembereiche schaffen als auch einen Eindruck von den mit heute verfügbaren Mitteln realisierbaren Möglichkeiten vermitteln.

Abbildung 4.1 zeigt die Komponenten der Sicherheitsarchitektur für WWW-basierte Informationssysteme.

An der Spitze dieser Abbildung steht der *Autorisierungsdienst*, dessen Aufgabe darin besteht, zu entscheiden, ob ein Subjekt berechtigt ist, auf ein Objekt mit einer bestimmten Operation zuzugreifen. Diese Entscheidung wird auf Grund von Zugriffsrechten der betroffenen Subjekte getroffen. Der Autorisierungsdienst erfüllt somit die im letzten Abschnitt beschriebenen Aufgaben der Zugriffskontrolle.

Um Zugriffsregeln auf einfache Art und Weise spezifizieren zu können, werden die zugreifenden Subjekte oft zu Benutzergruppen und die Objekte zu Management-Bereichen zusammengefaßt. Dies hat den Vorteil, daß Zugriffsrechte lediglich einmal für eine Gruppe oder für einen Bereich spezifiziert werden müssen und die Implementierung des Sicherheitskonzeptes übersichtlich und ausdrucksstark bleibt. In den letzten Jahren setzte sich darüber hinaus auch zunehmend

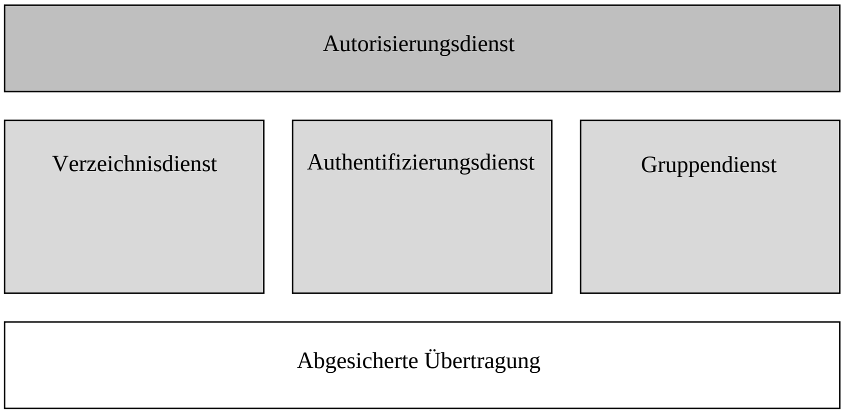

Abbildung 4.1: Sicherheitsarchitektur

das Konzept von *Rollen* zur Spezifikation von Zugriffsrechten durch. Das bedeutet, daß Zugriffsrechte nicht an einzelne Personen, sondern an ihre Funktion bzw. Aufgaben gebunden sind. Eine Rolle (z.B. die Bearbeitung eines bestimmten Sachgebietes) kann durch mehrere Personen erfolgen. Um Zugriffsentscheidungen treffen zu können, benötigt der Autorisierungsdienst folglich Information über die Gruppen, Bereichs- und Rollenzuordnungen der verwalteten Subjekte und Objekte. Diese Information wird von einer weiteren Komponente, dem *Gruppendienst*, verwaltet und zur Verfügung gestellt (vgl. [kers91]).

Eine weitere Voraussetzung für den Autorisierungsdienst ist die Authentifizierung der zugreifenden Subjekte. Diese Funktion wird vom *Autorisierungsdienst* erfüllt, der die Aufgabe hat, im internen Bereich die angesprochene Authentifizierung zu realisieren. Das hier beschriebene Modell geht davon aus, daß diese Authentifizierung mit Hilfe von sogenannten digitalen Zertifikaten geschieht. Darunter sind von einer berechtigten Stelle ausgestellte „digitale Personalausweise“ zu verstehen, die im einfachsten Fall neben dem Namen einer Person noch deren öffentlichen Schlüssel beinhalten.

Handelt es sich nicht um ein abgeschottetes Intranet, so obliegt es auch dem Authentifizierungsdienst, über die Gültigkeit der Authentifizierung von Benutzern aus dem globalen Internet zu entscheiden.

Grundlage des gesamten Sicherheitskonzeptes muß eine *abgesicherte Übertragung* sein, welche die in Kapitel 2.4.8 aufgezeigten Schwächen der Internet-Protokolle beseitigt. Die von dieser Komponente zu erfüllenden Aufgabe liegen in der verschlüsselten und verläßlichen Übertragung der Nachrichten zwischen den Kommunikationsparteien. Entsprechende Erweiterungen der Internet-Protokolle sind gegenwärtig in der Standardisierungsphase, einige davon finden auch schon als kommerzielles Produkt Verbreitung.

Allerdings sind die angesprochenen Konzepte meist nur einzelne und nicht in *einem* Server zusammengefaßt. Dadurch müssen weiterhin unterschiedliche Systeme miteinander kombiniert werden, um die volle Funktionalität zu erreichen. Ziel ist es auch, einen einheitlichen und transparenten Dienst für den Benutzer zu schaffen, der gleichzeitig Sicherheitsanforderungen seitens des Arbeitgebers und eines Informationsanbieters berücksichtigt.

4.2 Grobstruktur

Die Idee des Konzeptes ist es, die Internetkommunikation zwischen mehreren Teilnehmern über spezielle Server zu realisieren, die wiederum zu einem lokalen Netz mit Endbenutzern oder Datenbanken eine Schnittstelle bereitstellen. Diese Idee ist angelehnt an die von Proxy-Servern oder Bastion-Hosts, jedoch haben die Server hier eine andere Aufgabenstellung. Die Server sind zuständig für eine sichere Kommunikation, die Abrechnung von Dienstleistungen, Authentifizierung, sowie Zugriffsberechtigungen auf Datenbankbestände. Abbildung 4.2 gibt einen groben Überblick über das System.

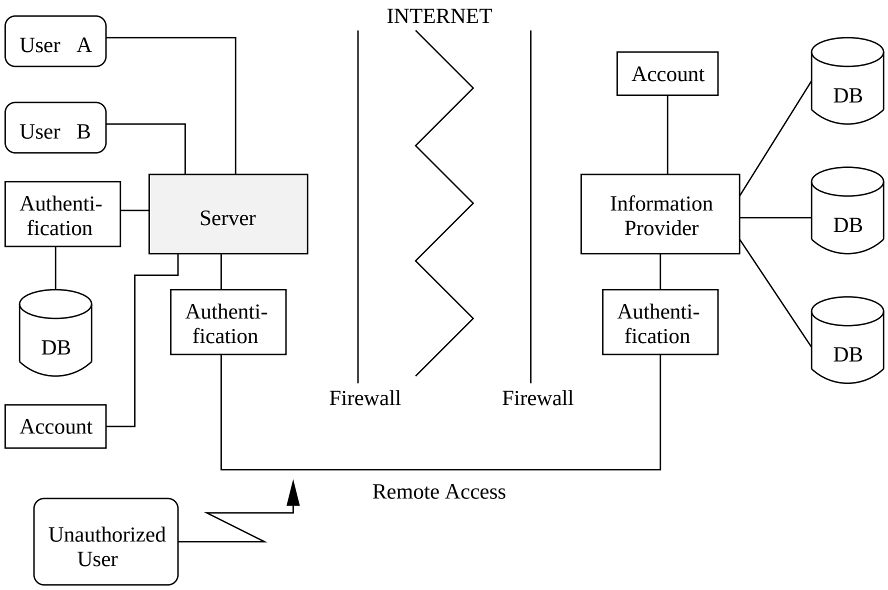

Abbildung 4.2: Grobstruktur des Systems

Bei der sicheren Kommunikation baut ein Server zu einem anderen Server eine Kommunikationsverbindung auf und es findet zunächst eine Authentifizierung statt. Zentraler Punkt ist hier die Verlegung von der Anwendung zum Server (siehe auch Kapitel 4.2.4). Authentifizierung bedeutet hier, daß sowohl der eigene Datenbestand als auch die angeforderten Information einer Kontrolle unterzogen werden müssen. Vorstellbar an dieser Stelle ist ein Abonnementen-Service, der den Provider veranlaßt, nach gewissen Zeitabständen dem Auftraggeber bestimmte

Information zur Verfügung zu stellen. Bei dieser Information kann es sich bspw. um sensible Forschungberichte handeln, die nicht für jeden Benutzer bestimmt sind. D.h., hier muß eine effektive Authentifizierung greifen. Dies bedeutet ferner, daß auch nicht jeder Benutzer beliebige Dokumente anfordern darf. Denkbar ist hier ein separates Konto für jeden Benutzer einzurichten, welches es ihm erlaubt, für sein Guthaben kostenpflichtige Dokumente „einzukaufen“.

4.2.1 Authentifizierung

Der Einsatz der im Kapitel 3.7 beschriebenen Verfahren greift in Zusammenhang mit der Absicherung von Internet-Protokollen. Voraussetzung ist die Existenz von vertrauenswürdigen öffentlichen Schlüsseln der Kommunikationspartner. Diese Rahmenbedingungen werden mit den schon angesprochenen Zertifikaten und Zertifizierungsstellen geschaffen. Werden die Anforderungen der Zertifizierungsstelle für einen erfolgreichen Identitätsnachweis erfüllt, so versieht diese den öffentlichen Schlüssel der identifizierten Person oder des identifizierten Dienstes mit ihrer eigenen digitalen Unterschrift. Der Vorteil für die Teilnehmer eines öffentlichen Netzes liegt darin, daß sie lediglich der Unterschrift der Zertifizierungsstelle vertrauen müssen und sich auf diese Weise der Authentizität der präsentierten öffentlichen Schlüssel sicher sein können.

Diese Konzepte sind nicht erst mit der Kommerzialisierung des Internet entstanden, sondern stammen aus der Umgebung der ISO-Standards für offene Systeme [eich93].

4.2.2 Lokale Sicherheit

4.2.2.1 Vertrauenssache: Quota & Logfiles

Abbildung 4.3 zeigt einen möglichen Kontrollmechanismus, der sowohl auf der Clientseite als auch auf der Serverseite greift. Hier werden auf beiden Seiten Logfiles angelegt, die jede Kommunikationsverbindung (insbesondere Datentransfer) protokollieren. D.h., es werden bspw. das Datum, die Zeit, der Benutzer, die Dokumentarten und die Kosten eines Dokumentes festgehalten. Vorstellbar wäre auch die Anzahl der Zugriffe bzw. die Anzahl der einzelnen Verbindungen auszuwerten. Ein spezieller Counter könnte diese Arbeit übernehmen. Um Kosten einzuschränken bzw. besser kontrollieren zu können besteht die Möglichkeit, jedem Benutzer ein bestimmtes Konto anzulegen, das ihm erlaubt, für einen gewissen Betrag Daten einzukaufen. Im Beispiel stehen „Client 1“ 150 DM und „Client 2“ 50 DM zur Verfügung. Die Kosten für die angebotenen Dokumente betragen 100 DM bzw. 2000 DM. Besteht nun die Absicht Dokumente zu kaufen, werden zuvor die Kosten einer Transaktion ermittelt. Dabei fragt zunächst der lokale Server beim Provider Art und Preis des gewünschten Dokumentes an (die Anfrage nach Preisen sollte kostenfrei bleiben). Nach dieser Aktion wird entschieden, ob die Transaktion zu Stande kommt oder nicht. Im Beispiel hat „Client 1“ nur die Möglichkeit „Doc A“ zu erwerben. Der „Master“ hingegen darf auf jedes Dokument zugreifen, da er kein Limit besitzt.

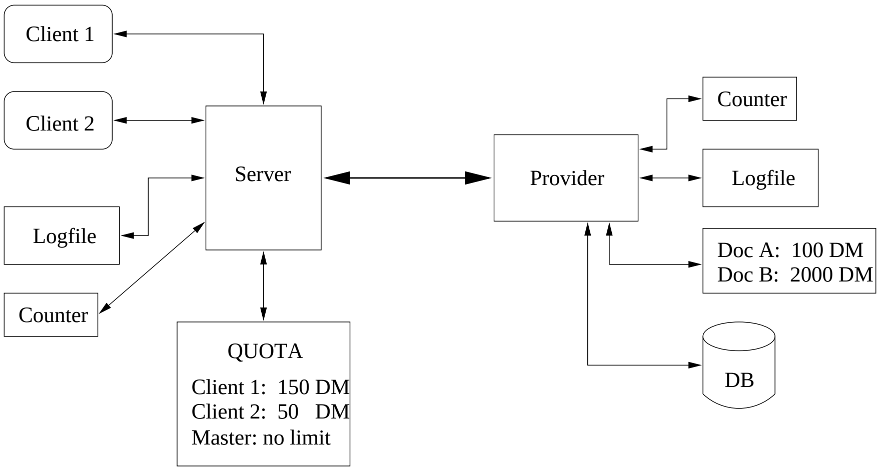

Abbildung 4.3: Quota- und Logfile-Methode

Die Logfiles geben beiden Kommunikationspartnern die Möglichkeit, insbesondere Abrechnungen nachzuhalten. Wird bei einem Abgleich der beiden Logfiles eine Differenz festgestellt, so haben die Clientseite bzw. auch der Provider das Recht die Verbindung abzubrechen oder zu verweigern. Mit dieser Methode können Manipulationen erkannt werden und entsprechende Maßnahmen ergriffen werden. Ferner schließen Counter und Logfiles mögliche unautorisierte Benutzer aus, die eventuell versuchen, Zugriff auf Dokumente zu erhalten. Eine sichere Kommunikation kann auch hier mit dem Schlüsselkonzept erfolgen. Weiterhin kann durch die Logfiles auf der Clientseite eine doppelte Beschaffung eines Dokumentes verhindert werden, wodurch wieder Kosten gespart werden können. Hier spielt das Konzept des Information-Cache eine Rolle.

4.2.2.2 Information-Cache

Um Kosten zu sparen oder um Dokumente besonders schnell für andere Benutzer zur Verfügung zu stellen, können einige Dokumente in einem speziellen Cache zwischengespeichert werden. Wie in Abbildung 4.4 gezeigt, werden die Daten, die von außen geholt werden nicht nur einfach an den Client weitergeleitet, sondern zusätzlich in einem Cache für künftige Zugriffe bereitgehalten. So können eventuell auch Benutzer auf Dokumente zugreifen, die von ihren Kosten her eigentlich zu teuer für ihr jeweiliges Benutzerkonto sind. Insgesamt kann eine Firma als Kunde eines Informationsanbieters so eventuell Kosten sparen.

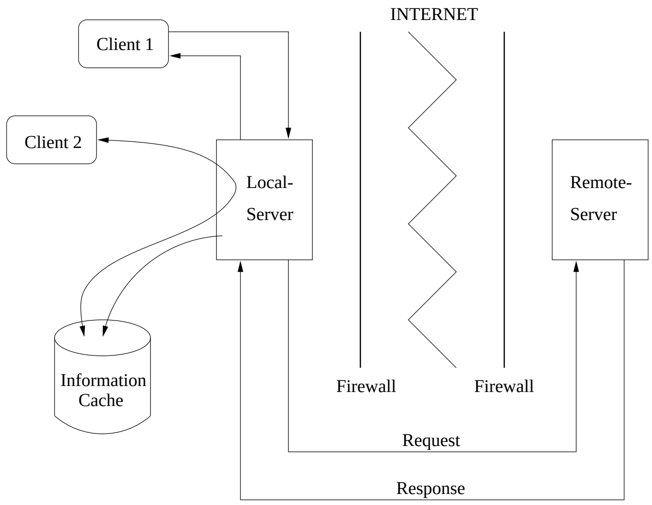

Abbildung 4.4: Information Cache

Verschiedene Strategien versuchen möglichst aktuelle Dokumente zu liefern. Ziel dieser Strategien ist es, die Dokumente im Cache so häufig wie nötig zu aktualisieren, aber gleichzeitig so wenig wie möglich externe Zugriffe durchzuführen. Zur Lösung werden dazu Eigenschaften von *Last-Modified*, d.h., wann das Dokument zuletzt verändert wurde und *Expires*, ein Verfallsdatum des Dokumentes, verwendet.

4.2.3 Modularisierung

Um eine flexible Kommunikation zu ermöglichen, wird für das System eine spezielle Modulbibliothek bzw. Protokolle spezifiziert. Anhand dieser Bibliothek können sich beide Kommunikationspartner auf ein geeignetes Übertragungsschema einigen. Dieses Schema bzw. Protokoll kann beliebig, und bei jedem Verbindungsaufbau neu gewählt werden. Dieser Mechanismus erlaubt eine leichte Erweiterbarkeit der Kommunikationsmöglichkeiten. Ein weiterer Vorteil ist, daß hier in Bezug auf die Kosten einer Transaktion und die Sensibilität der zu übertragenden Daten besser eingegangen werden kann. Der Aufwand, der für eine Anfrage (request) bzw. eine Antwort (response) betrieben werden sollte hängt in erster Linie von der „Wichtigkeit“ der Daten ab. Weniger sensible Information werden somit kostengünstiger verarbeitet und angeboten. Dabei wird eine Anfrage nach Daten, die für jeden Benutzer frei zugänglich sind allgemeiner behandelt als eine Anfrage nach nicht frei zugänglichen Daten. Eine allgemeine Anfrage wäre bspw. das Informationsangebot des Providers zu erfragen. Solche Art Anfragen müssen nicht unbedingt „sicher“ über das Internet übertragen werden. D.h., ein einfaches HTTP-Protokoll, welches den Kommunikationsablauf vollständig im Klartext abwickelt, würde hier ausreichen. Ein möglicher Angriff auf solche

Daten würde keinen oder nur geringen Schaden anrichten. Andererseits müssen sensiblere und kostenintensivere Daten besser vor möglichen Angriffen geschützt werden. Die Übertragung der Daten muß daher über einen sicheren Kanal laufen. Hier bieten sich spezielle Verschlüsselungsstrategien an, die einen Angriff zwar nicht verhindern können, aber die Daten für dritte unbrauchbar machen. Nachdem sich beide Kommunikationspartner auf eine Strategie geeinigt haben, erfolgt der Datenaustausch über einen sicheren Kanal. Ein sicherer Kanal bedeutet aber, daß die Kommunikationskosten aufgrund von künstlich erzeugten Redundanzen steigen (vgl. Kapitel 4.7).

4.2.4 Sichere Übertragung

Konzepte mit Zertifikaten und Public-Key-Infrastrukturen (PKI) erlauben eine verläßliche Authentifizierung eines Benutzers bzw. eines Dienstes. Zertifikate alleine genügen jedoch nicht, um die Anforderung an die Transaktionssicherheit zu erfüllen. In Kapitel 4.1 wurde diese Problematik bereits angesprochen. Konkret bedeutet dies:

- Definition der notwendigen Protokollstrukturen zur Übertragung von verschlüsselten oder unverschlüsselten Daten sowie einer digitalen Unterschrift zur Sicherstellung der Authentizität der übertragenen Daten.

- Definition eines Protokolls zur Schlüssel-Akquisition, das zum erstmaligen Austausch eines für diese Verbindung eingesetzten symmetrischen Schlüssels verwendet werden kann. Aufgabe dieses Schlüssel-Management-Protokolls (engl.: Key Management Protocol) ist darüber hinaus auch die Durchführung der erstmaligen Authentifizierung der beteiligten Kommunikationspateien. Dabei kommt der in Kapitel 4.2.1 vorgestellte Mechanismus des Authentifizierungsdienstes zum Einsatz.

- Zugänglichkeit dieser Funktionalität entweder durch transparente Integration in die Ebenen der TCP/IP Protokolle oder als Integration in eine Programmbibliothek mit definierten Schnittstellen.

Abbildung 4.5 zeigt die Möglichkeiten der Integration eines sicheren Transportdienstes in die ab Kapitel 2.4 beschriebenen Ebenen der Internet-Protokolle. Die Verfahren setzen auf dem Internet-Protokoll auf und bedienen sich der bestehenden Adressierungs- und Routingmechanismen, um die verschlüsselten Daten über das Internet weiterzuleiten (vgl. [oppl97, bhim96]).

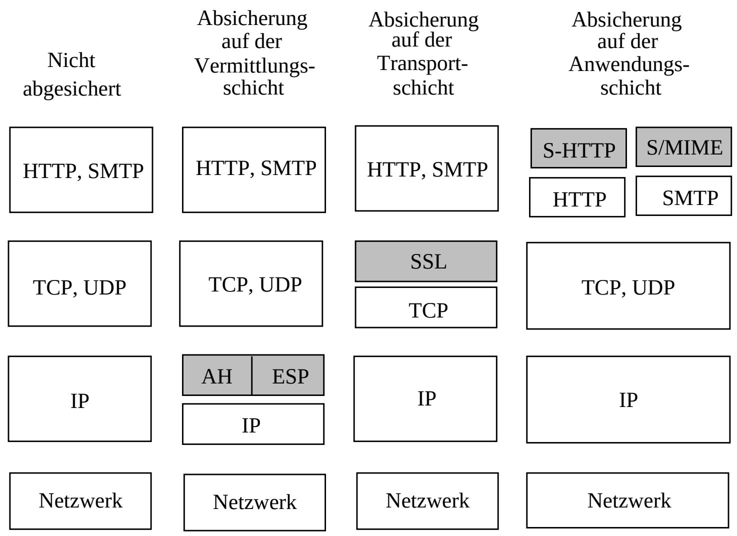

Abbildung 4.5: Absicherung der Internet-Protokolle

4.2.4.1 Absicherung auf der Vermittlungsschicht

Findet die Absicherung auf der Vermittlungsschicht statt, so werden die Protokollelemente der darüberliegenden Schicht – TCP-Segmente oder UDP-Datagramme – in verschlüsselter Form in IP-Datagramme eingebettet und übertragen. Beim Empfänger wird dieser Vorgang rückgängig gemacht und es werden die ursprünglichen Protokollelemente an die entsprechenede Software weitergeleitet. Der Vorteil dieser Lösung liegt darin, daß bestehende Anwendungen nicht modifiziert werden. Die Absicherung erfolgt für Anwendungsprotokolle transparent durch die Netzwerksoftware. Der Nachteil dieser Variante ist, daß die rechenintensiven kryptographischen Verfahren gleichermaßen auf alle Anwendungsprotokolle angewendet werden müssen.

Innerhalb der IETF ist die IP Security (IPSEC) WG mit der Spezifikation eines IP-Security Protocols (IPSP) und eines entsprechenden Internet Key Management Protocols (IKMP) beauftragt [oppl97].

Die Architektur von IPSP ist in RFC 1825 beschrieben [atki95a]. Grundsätzlich werden zwei Sicherheitsmechanismen unterschieden:

- Ein Authentification Header (AH), der in RFC 1826 spezifiziert ist, und
- ein Encapsulated Security Payload (ESP), der in RFC 1827 spezifiziert ist (vgl. [atki95b, atki95c]).

Der AH-Mechanismus schützt in erster Linie die Authentizität und Integrität von IP-Paketen, während der ESP-Mechanismus auf den Schutz der Vertraulichkeit abzielt. Standardalgorithmen für die AH- und ESP-Mechanismen sind in den

RFCs 1828 und 1829 spezifiziert [karn95, metz95]. Es handelt sich dabei um DES (Data Encryption Standard), sowie MD5 mit vor- und nachgestellten Schlüsseln für AH (vgl. [stro98]).

Ein Anwendungsgebiet der Absicherung auf der Vermittlungsschicht ist die Einrichtung von sogenannten *virtuellen privaten Netzen (VPN)* [smit97]. Dieses Verfahren dient dazu, zwei voneinander räumlich getrennte, sichere Bereiche miteinander über ein unsicheres, öffentliches Netz zu verbinden.

4.2.4.2 Absicherung auf der Transportebene

Als Alternative zur Vermittlungsschicht stellt die Absicherung auf der Transportebene dar. Hierbei entscheidet eine Applikation dynamisch, ob eine Verbindung in Bezug auf ihre Authentizität, Integrität und Vertraulichkeit zu schützen ist, und die Verbindung dementsprechend aufbaut.

Diese Möglichkeit ist unter anderem von der Firma Netscape aufgegriffen worden und in Form eines Secure Socket Layer (SSL) Protokolls umgesetzt worden. Die Firma Microsoft hat ein mit SSL vergleichbares Sicherheitsprotokoll für die Transportschicht spezifiziert und als PCT (Private Communications Technology) bezeichnet.

SSL und PCT sind in Bezug auf die verwendeten Record-Formate kompatibel, so daß ein Server auch beide Protokolle unterstützen kann. Ein weiteres Sicherheitsprotokoll für die Transportschicht ist das sogenannte SSH (Secure Shell). Netscape, Microsoft und die Entwickler von SSH versuchen im Rahmen einer Transport Layer Security (TLS) WG der IETF auf ein Transport Layer Security Protocol (TLSP) zu einigen (siehe auch [oppl97, bahn98]).

4.2.4.3 Absicherung auf der Anwendungsebene

Eine weitere Möglichkeit ist die Absicherung auf der Anwendungsebene. Darunter ist die Integration der gewünschten kryptographischen Operation in das Anwendungsprotokoll zu verstehen. Aus dem Blickwinkel der einzelnen Anwendungen ist dies eine sichere Lösung, da die Funktionalität exakt auf die Sicherheitsbedürfnisse der Applikationen abgestimmt werden können. Ein Beispiel für die Absicherung auf Anwendungsebene ist der PEM-Standard (Privacy Enhanced Mail) zur Abwicklung elektronischer Mail oder auch die Durchführung kommerzieller Transaktionen nach dem SET-Verfahren. Beide Konzepte verwenden X.509-Zertifikate. Weitere Beispiele diesbezüglich sind PGP (Pretty Good Privacy) für SMTP (Simple Mail Transfer Protocol) bzw. Secure-HTTP (S-HTTP) für HTTP (vgl. [mart98]).

4.2.5 Kommunikation mit dem SSL-Protokoll

Wie schon oben erwähnt, basiert die gesamte Kommunikation im WWW auf dem Transportprotokoll HTTP (Hyper Text Transport Protocol), welches ein potentielles Sicherheitsrisiko darstellt. Abhilfe schaffen hier Verfahren, die auf SSL (Secure Socket Layer, Netscape Inc.) und S-HTTP (Secure HTTP, Terisa Systems) aufsetzen.

Mit Hilfe eines Public-Key-Verfahrens wird dabei zunächst während einer Handshake-Sequenz zwischen Server und Client ein geheimer Schlüssel, der sogenannte „Secret Master“, ausgetauscht. Der Client generiert dazu mit Hilfe eines Zufallszahlengenerators eine Bitsequenz (Pre-Master-Secret) und sendet sie dem Server, verschlüsselt mit dessen öffentlichen Schlüssel.

Aus dieser Pre-Master-Secret-Bitsequenz generiert der Server und der Client jeweils nach einem festgelegtem Hash-Funktions-Algorithmus den sogenannten Master-Key. Jeder weitere Datenaustausch erfolgt nun nach der im Handshake-Prozeß verhandelten symmetrischen Verschlüsselungsmethoden (bspw. RC4 oder DES) unter Benutzung des Master-Keys. Dem Benutzer selbst bleibt der Mechanismus des gesicherten Verbindungsaufbaues transparent. Zusätzlich zur Verschlüsselung können übertragene Nachrichten auch mit einer digitalen Signatur versehen werden, wodurch die Authentifikation sowohl des Servers als auch des Clients möglich ist.

Abbildung 4.6 stellt den gesicherten Nachrichtenaustausch mit SSL dar.

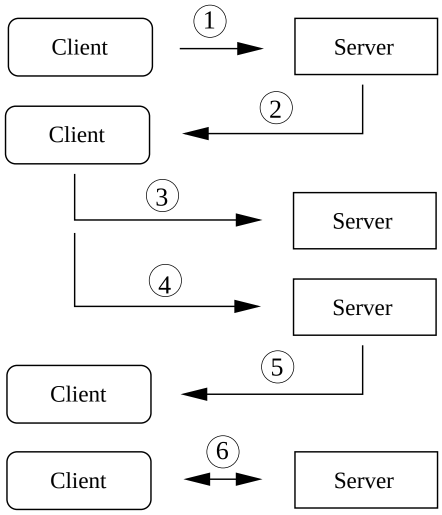

Abbildung 4.6: Sichere Kommunikation mit SSL

Die sechs Phasen [ahuj96] der Kommunikation:

1. CLIENT-HELLO / SERVER-HELLO: In der sogenannten „Hello-Phase“

baut der Client eine Verbindung zum Server auf und teilt diesem mit, welche kryptographischen Algorithmen er unterstützt. Der Server wählt daraus ein Public-Key-, ein Privat-Key- und ein Hash-Verfahren aus und teilt sie dem Client mit.

2. CLIENT-MASTER-KEY / CLIENT-DH-KEY: Der Server sendet ein Zertifikat, das unter anderem den öffentlichen Schlüssel des Servers enthält. (Mit Hilfe des Zertifikates kann der Client überprüfen, ob die Antwort tatsächlich vom gewünschten Server stammt.)

3. CLIENT-SESSION-KEY: Der Client generiert einen Sitzungsschlüssel (Session key) für einen Datenaustausch per Private-Key-Verfahren. Diesen Schlüssel chiffriert der Client mit dem öffentlichen Schlüssel des Servers und schickt diesen an den Server.

4. SERVER-VERIFY: Der Client authentifiziert den Server, indem er ihm eine Reihe von mit dem Sitzungsschlüssel chiffrierten zufälligen Testnachrichten schickt, die der Server nur dann korrekt dechiffrieren und bestätigen kann, wenn es sich um den „echten“ Server handelt.

5. REQUEST-CERTIFICATE / CLIENT-CERTIFICATE: In einem optionalen Schritt kann der Server auf vergleichbare Weise den Client authentifizieren. Die Client-Authentifikation funktioniert nur dann, wenn der Client über ein offiziell registriertes Zertifikat verfügt.

6. CLIENT-FINISHED / SERVER-FINISHED: Beide Seiten schließen den initialen Verbindungsaufbau ab und chiffrieren alle weiteren Datenpakete mit dem Sitzungsschlüssel.

4.2.6 Manipulationen erkennen

Die in Kapitel 3.5 beschriebenen Methoden lassen sich durch bestimmte Mechanismen nach Abbildung 4.7 erkennen und behandeln.

Das Erfassen aller sicherheitsrelevanten Ereignisse in einem IT-System dient dem Zweck der nachträglichen Entdeckung von Ereignissen, vor allem aber der Beweisführung bei Manipulationen. Dabei müssen die Systeme privilegierte Rollen zulassen, denen das Recht zur Bearbeitung von Protokollaufzeichnungen, zum Löschen nicht mehr aktueller Aufzeichnungen und Erstellen der Protokollparameter, zur Auswahl aufzeichnungswürdiger Aktionen, übertragen wird.

Sinnvoll ist eine Beweissicherung letztlich nur dann, wenn Auswerteprozeduren vorhanden sind, mit denen die gesamten Aufzeichnungen nach sicherheitskritischen Ereignissen durchsucht und gezielt nach bestimmten Verhaltensweisen von Benutzern mit manipulativen Absichten analysiert werden können.

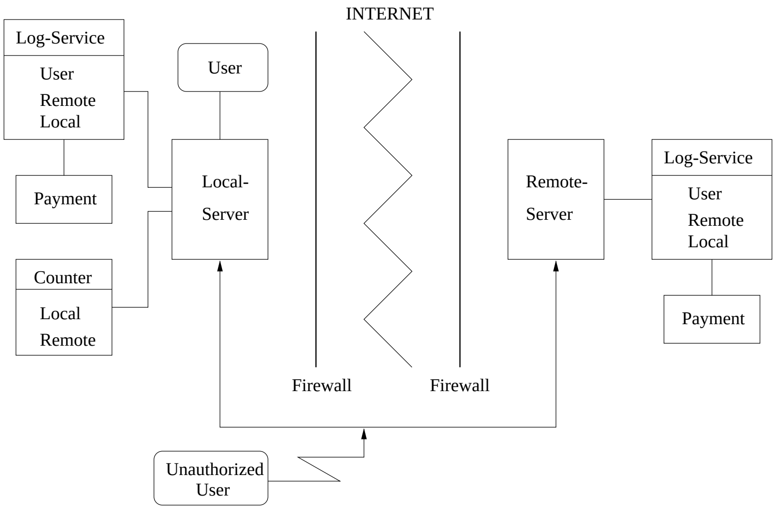

Abbildung 4.7: Erkennen von Manipulationen

Qualitätsaspekte bei der Beweisführung sind die Vollständigkeit der Protokollsätze, die Untäuschbarkeit des Protokollierungssystems, das Erfassen von Aktionen von Personen mit besonders privilegierten Rollen.

Das Konzept sieht hier spezielle Datenbanken bzw. Logfiles vor, die jede Kommunikationssituation oder Datenübertragung protokollieren. Dieses Protokoll wird auf beiden Seiten, d.h. auf der Sender- und der Empfängerseite, parallel mitgeführt. Auf diese Weise ist beiden Partnern eine Kontrollmöglichkeit gegeben, die bspw. dem „lokalen“ Administrator bestimmte Aktivitäten auf seinem System zeigt. Besonders markant ist hier das Abrechnungssystem, welches den „Zahlungsverkehr“ zwischen dem Dienstleistungsanbieter und dem Dienstleistungsnehmer regelt. Zu beliebigen Zeitpunkten oder bei jedem Verbindungsaufbau werden diese beiden Datenbestände auf ihre Gültigkeit hin überprüft. Sollte nun eine Unstimmigkeit in den Abrechnungen auftreten, so werden diese erkannt und entsprechende Maßnahmen können eingeleitet werden. Der Provider könnte bspw. seine Dienstleistungen sperren.

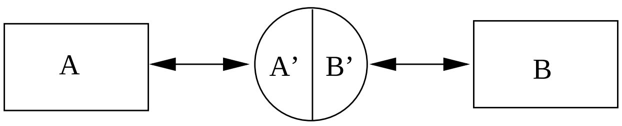

Abbildung 4.8: Angiff auf das Sicherheitssystems

Dieses Konzept kann als sicher gelten, wenn ein Angreifer nicht alle Kommunikationsphasen abhören kann bzw. protokolliert. Sollte es einem Angreifer jedoch gelingen, durch die in Kapitel 3.5 gezeigten Methoden jede aufgebaute Verbindung zu beeinflussen, so hat dieser die Möglichkeit, dieses Sicherheitssystem zu überwinden. Abbildung 4.8 verdeutlicht diese Methode des Angriffs.

Hierbei schaltet sich der Angreifer direkt in die Kommunikationsverbindung ein und täuscht den regulären Partnern A und B jeweils einen „falschen“ Partner A' bzw. B' vor.

4.3 Sicherheitsprotokoll des Servers

Im folgenden wird das spezielle Sicherheitsprotokoll des Servers beschrieben, welches für den Austausch der Logfile-Daten zuständig ist. Abbildung 4.9 stellt einen exemplarischen Kommunikationablauf von zwei beteiligten Server dar. In dem gezeigten Szenario fordert der im Bild als *Server 1* bezeichnet Server, einen Sicherheitscheck von *Server 2* an.

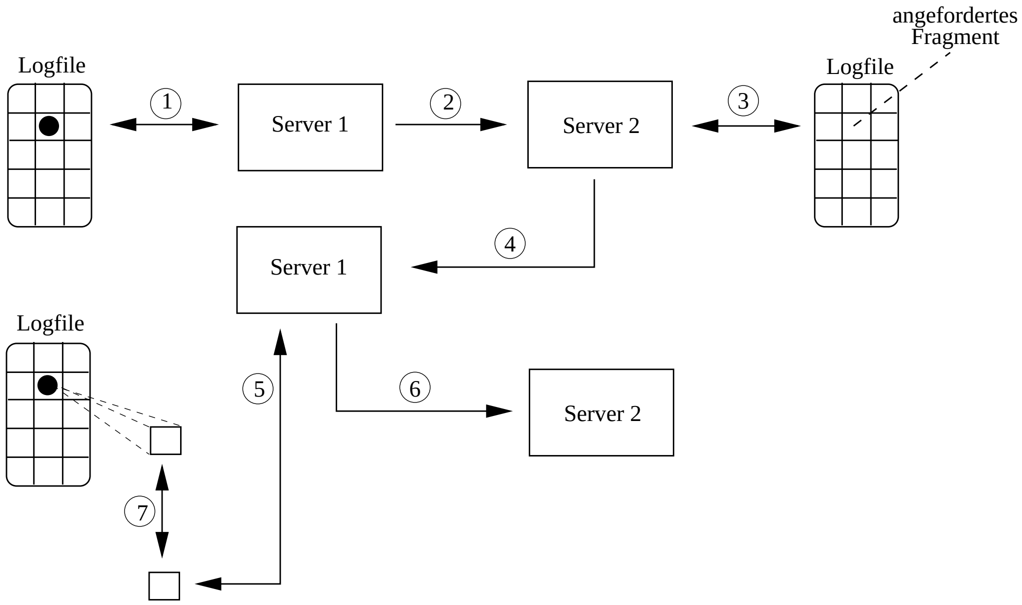

Abbildung 4.9: Sicherheitsprotokoll des Servers

Die Kommunikation der beteiligten Server wird in sieben Phasen abgewickelt:

1. FRAGMENT AUSWAHL: Im ersten Schritt wählt *Server 1* ein Fragment aus seinem Logfile aus, welches optional gewählt werden kann. Im vorliegenden Fall handelt es sich um das Fragment, das mit einem Punkt gekennzeichnet ist.

2. KOORDINATEN SENDEN: Hat *Server 1* seine Auswahl getroffen, sendet er anschließend die „Koordinaten“ diese Stelle an *Server 2*.

3. KOORDINATEN REGISTRIEREN: *Server 2* registriert diese Aufforderung und ließt die angeforderten Daten aus seinem lokalen Logfile aus.

4. FRAGMENT SENDEN: Der aufgefordete Server sendet den Inhalt dieses Fragment an *Server 1* zurück.

5. FRAGMENT AUFBEREITEN: *Server 1* greift die gesendeten Daten auf und platziert diese in seinem lokalen sicheren Bereich.

6. EMPFANG QUITTIEREN: In dieser Phase schickt *Server 1* dem entferntern Server eine Quittung, daß dieser ein Fragment erhalten hat.

7. FRAGMENTE VERGLEICHEN: In einer abschließenden Phase prüft *Server 1* die gesendeten Daten, indem dieser einem Abgleich der Daten mit denen des Fragmentes vergleicht, welches *Server 1* in Phase 1 ausgewählt hat.

Die oben angesprochenen Koordinaten des Fragmentsegmentes können als Blöcke in einer Filestruktur identifiziert werden. Diese Blöcke können eine feste Länge haben oder sie werden durch eine Anfangs- und eine Endeposition festgelegt. Abbildung 4.10 greift diese beiden Mechanismen auf.

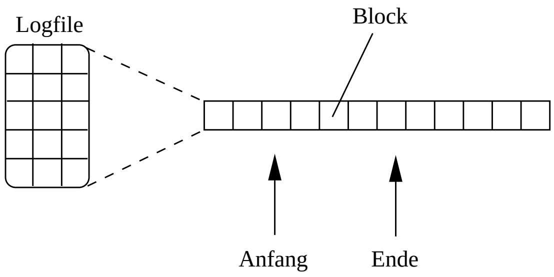

Abbildung 4.10: Auswahl der Logfile-Fragmente

Ferner besteht die Möglichkeit, ählich wie bei SSL, für die Übertragung der Daten ein kryptographisches Verfahren einzusetzen.

4.4 Sicht des Benutzers

Die Vorteile der Implementierung der kryptographischen Absicherung der übertragenen Daten auf der Transportschicht liegen in der Tatsache begründet, daß auf der Transportschicht im Gegensatz zur Vermittlungsschicht bereits zwischen den einzelnen Diensten unterschieden wird. Dadurch können, wie in Abbildung 4.11 gezeigt, wahlfrei einzelne Dienste abgesichert und andere unverschlüsselt eingesetzt werden.

Abbildung 4.11 zeigt ferner, daß es möglich und sinnvoll sein kann, denselben Dienst sowohl in einer abgesicherten als auch in einer nicht abgesicherten Variante anzubieten. Wie in Abschnitt 4.2.3 bereits erwähnt wurde, wird weniger

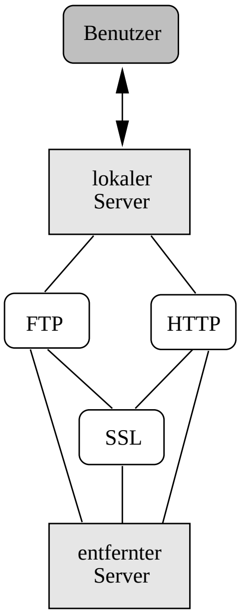

Abbildung 4.11: Sicht des Benutzers

sensitive Information für jedermann zugänglich gemacht, während bei sicherer Transaktionen auf den „sicheren“ Server verwiesen wird. In Abbildung 4.11 sind exemplarisch die Dienste FTP und HTTP dargestellt. Der Verbindungsaufbau und die Wahl der einzelnen Module wird für den Client bzw. Benutzer transparent gehalten.

4.5 Sicherheitsdienste

In folgenden Abschnitt werden einige von der OSI vorgeschlagenen Sicherheitsdienste beschrieben.

- *Authentifikationsdienste:* Authentifikationsdienste (authentification services) prüfen die Authentizität von Kommunikationspartnern und Datenquellen.
- *Zugriffskontrolldienste:* Ist eine Partnerinstanz authentifiziert, stellt ein Zugriffskontrolldienst (access control service) sicher, daß Zugriffe auf lokale oder entfernte Betriebsmittel in einem offenen System nur autorisiert erfolgen können.
- *Datenvertraulichkeitsdienste:* Datenvertraulichkeitsdienste (data confidentiality services) schützen die in offenen Systemem übertragenen Daten vor

Verschlüsselung
Digitale Unterschriften
Zugangskontrollmechanismen
Datenintegritätsmechanismen
Authentifikationsmechanismen
Verkehrsstopfung
Wegwahl

Tabelle 4.1: OSI-Sicherheitsmechanismen

passiven Angriffe. Obwohl Datenvertraulichkeitsdienste in der Regel die ersten Sicherheitsdienste sind, mit denen Datensicherheit assoziiert wird, sind in der Praxis oft weniger wichtig als zum Beispiel Authentifikations- und Datenintegritätsdienste.

- *Datenintegritätsdienste:* Datenintegritätsdienste (data integrity services) sind eigentlich erst im Zusammenspiel mit entsprechenden Authentifikationsdiensten sinnvoll und sollen vor aktiven Angriffen zu schützen.

- *Verbindlichkeitsdienste:* Wenn sich die elektronische Kommunikation längerfristig durchsetzen soll, dann ist unter anderem sicherzustellen, daß elektronisch abgegebene Willensbekundungen nachweisbar und verbindlich sind. Dazu sind rechtskräftige Verbindlichkeitsdienste (non-repudiation services) erforderlich.

4.6 Sicherheitsmechanismen

Sicherheitsdienste werden von Sicherheitsmechanismen umgesetzt. Dabei ist die Zuordnung von Sicherheitsmechanismen zu -diensten nicht eindeutig. Verschiedene Sicherheitsdienste können von einem oder mehreren Sicherheitsmechanismen umgesetzt werden [muft89].

In der OSI-Sicherheitsarchitektur sind die in Tabelle 4.1 zusammengestellten und im folgenden beschriebenen Sicherheitsmechanismen genannt.

- Die Verschlüsselung (encipherment) ist ein grundlegender Sicherheitsmechanismus, der bei der Umsetzung von fast allen Sicherheitsdiensten eine Rolle spielt.

- Zur Umsetzung von Datenintegritäts- und Verbindlichkeitsdiensten eignen sich digitale Unterschriften.

- Zugriffskontrollmechanismen (access control mechanisms) haben sicherzustellen, daß identifizierte und authentifizierte Subjekte nur auf Objekte zugreifen können, für deren Benutzung sie auch autorisiert sind.

- Zur Sicherung der Datenintegrität können z.B. Nachrichtenauthentifizierungscodes (MACs) eingesetzt werden.

- Die Authentifikationsmechanismen, die in offenen Systemen eingesetzt werden können, sind a priori dieselben, wie sie im Zusammenhang mit lokalen Zugangskontrollen.

- In Rahmen einer Verkehrsstopfung (traffic padding) wird auf einem Kanal ein konstanter Datenfluß dadurch erreicht, daß Kommunikationspartner mit Informationsleeren Daten überbrückt werden.

- Die Schwierigkeit, mit der passive (und aktive) Angriffe verübt werden können, hängt in der Regel auch von der Wegwahl (routing control) ab.

4.7 Kosten einer Transaktion

Elektronische Märkte werden künftig traditionelle Märkte teilweise ersetzen und zu tragenden Pfeilern des gesamtwirtschaftlichen Systems werden. Diese Entwicklung setzt jedoch voraus, daß elektronische Märkte gegenüber heutigen Märkten Vorteile wie beispielsweise reduzierte Transaktionskosten besitzen. Somit nehmen Digitale Zahlungsmittel eine Schlüsselstellung für die Entwicklung des *Electronic Commerce* ein, denn erst sie ermöglichen es, die Ware nach der Online-Auswahl auch online zu bezahlen. Sogenannte Micropayment-Systeme sind geeignet für Waren mit geringem Wert, zum Beispiel digitale Bilder, Online-Artikel oder wie schon in Abschnitt 4.2.3 angesprochen, das Informationsangebot eines Providers zu erfragen. Traditionelle Zahlungsmöglichkeiten wie Rechnung, Abbuchung oder Kreditkarte wären für derartige Artikel zu teuer, da die Transaktionskosten nicht über dem Wert der Produkte liegen dürfen. Auch ein Verschlüsselungskonzept wie SET wäre für Micropayment-Systeme zu teuer, da künstlich erzeugte Redundanz in den zu übertragenden Daten anfällt.

Elektronische Märkte unterscheiden sich von traditionellen Märkten durch den spezifischen Einsatz der Informations- und Telekommunikationstechnologie. In [schm95] werden die Kosten einer Transaktion weiter in eine *Informationsphase*, *Vereinbarungsphase* und eine *Abwicklungsphase* unterteilt.

Abrechnungs- und Transaktionssysteme werden von mehreren Firmen, wie zum Beispiel ECash von DigiCash (www.digicash.com/ecash), Cybercash (www.cybercash.com) oder Millicent (www.millicent.digital.com) entwickelt und von Banken getestet und eingesetzt. Die Systeme unterscheiden in diesem Zusammenhang zwischen *Mikrozahlung*, *Makrozahlung* und *Picozahlung*. Hiebei handelt sich um Beträge im Pfennig-Bereich oder im Zehntelpfennig-Bereich (bei Millicent).

Sichere Datenübertragung, Transaktionskosten, Anonymität von Zahlungsvorgängen, Akzeptanz, Übertragbarkeit und Fälschungssicherheit sind Kriterien, die beim Thema Geld zu beachten sind und im Zusammenhang mit der digitalen Variante diskutiert werden. Für Micropayment-Systeme gibt es einige Besonderheiten zu beachten, denn aufgrund des geringen Wertes einzelner Zahlungen stehen nicht Sicherheit und Anonymität, sondern niedrige Transaktionskosten und Rechenzeit sowie einfache Handhabung im Vordergrund. Fälschungsaktivitäten lohnen sich kaum.

Kapitel 5

Implementierung

5.1 Der WWW-Server Jigsaw

Der WWW-Server *Jigsaw* ist ein in Java implementierter Server des W3-Konsortiums [jig1][1]. Die folgende Beschreibung des Servers setzt auf der Version 1.0beta2 auf. Interessant sind einige spezielle Eigenschaften, die Jigsaw im Vergleich zu anderen Servern, wie beispielsweise den Apache, auszeichnen. Wie bereits erwähnt, ist Jigsaw in Java implementiert. Aus diesen Eigenschaften folgt, daß der Server als plattformunabhängig angesehen werden kann. Durch die einheitlichen Eigenschaften von Bytecode und virtueller Java-Maschine[2] kann der Server unter verschiedenen Betriebssystemen wie beispielsweise Unix oder Windows NT eingesetzt werden.

Jigsaw bietet die Möglichkeit der dynamischen Erweiterbarkeit, d.h., es werden Verfahren angeboten, die es erlauben, eigene Java-Klassen in den Server einzubringen. Dies ist auch während des laufenden Betriebs des Servers möglich – es ist nicht nötig, den Server zuvor zu beenden.

5.1.1 Ressourcen

Der Server betrachtet jedes Objekt, welches er ausliefert, als eine Ressource. Eine Ressource im Jigsaw-Kontext ist beispielweise eine Datei oder ein Verzeichnis. Dazu gehören je nach Typ Information wie Datentyp, Datum der letzten Änderung, Verfallsdatum, Zugriffsschutz etc.

[1]Folgende Ausführungen beziehen sich ebenfalls auf das Handbuch zum Server.

[2]Ein Java-Quelltext wird in Java-Bytecode übersetzt, der auf einer virtuellen Java-Maschine (engl.: virtual machine) abläuft. Bytecodes sind eine Maschinensprache für eine abstrakte Maschine, die von den virtuellen Maschinen jedes Java unterstützenden Systems zur Laufzeit interpretiert werden kann.

Ressourcen werden beim Jigsaw nach Möglichkeit im Hauptspeicher bzw. in einem Cache gehalten. Bei einem wiederholten Zugriff auf dieselbe Ressource wird der Client unmittelbar aus dem Cache bedient. So werden effiziente Zugriffe sichergestellt.

Ressourcen werden als Java-Objekte betrachtet und als solche sind sie Instanzen von Klassen. Jigsaw definiert eine Reihe von Klassen, insbesondere eine namens *w3c.jigsaw.resources.Resource*[3], die als Hauptklasse aller vom Server ausliefernde Objekt bezeichnet wird. Eine wichtige Unterklasse davon ist *w3c.jigsaw.resources.HTTPResource*, die für die Verteilung per HTTP zuständig ist.

Persistenz ist eine weitere wesentliche Eigenschaft von Ressourcen. D.h., sie bleiben über das Ende des Serverprozesses hinaus erhalten und stehen zu einem späteren Zeitpunkt unverändert zur Verfügung. Die Attribute von Ressourcen sind über sogenannre Formulare editierbar und konfigurierbar.

5.1.2 Filter

Die oben angesprochenen Ressourcen lassen sich mit sogenannten Filtern versehen. Dabei handelt es sich um spezielle Ressourcen, die eine Anfrage an den Server entweder vor Abruf der eigentlichen Ressource oder das Ergebnis manipulieren. Diese Filter werden als Eingabe- bzw. als Ausgabefilter bezeichnet.

Der folgende Code realisiert einen *Counter-Filter*, der Zugriffe auf bestimmte Bereiche protokolliert bzw. zählt:

```
package w3c.jigsaw.filters;

import w3c.jigsaw.http.*;
import w3c.jigsaw.resources.*;

public class CounterFilter extends ResourceFilter {

    // --  Attribute index - The counter attribute --

    protected static int ATTR_COUNTER = -1 ;

    static {
        Attribute a   = null ;
        Class     cls = null ;

        try {
            cls = Class.forName("w3c.jigsaw.filters.CounterFilter") ;
        } catch (Exception ex) {
```

[3]Die Darstellung der Klassen orientiert sich an den Schemata von Java.

```
            ex.printStackTrace() ;
            System.exit(1) ;
        }
        // -- Declare the counter attribute --
        a = new IntegerAttribute("counter"
                                 , new Integer(0)
                                 , Attribute.EDITABLE) ;
        ATTR_COUNTER = AttributeRegistry.registerAttribute(cls, a) ;
    }
}
```

5.1.2.1 Authentifizierung

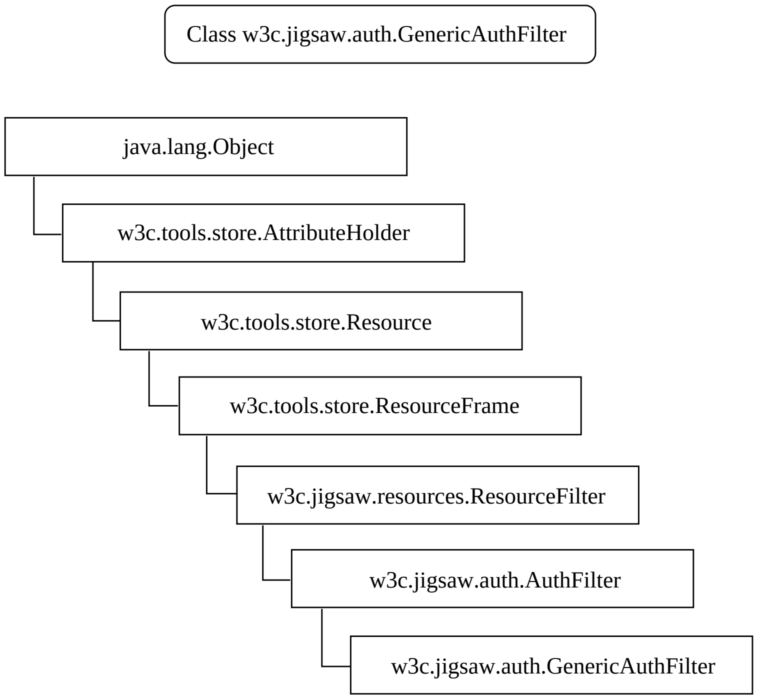

Abbildung 5.1: Die Jigsaw Klasse *GenericAuthFilter*

Wichtig für einen Server sind die implementierten Authentifizierungsmechanismen. Jigsaw bietet die Möglichkeit bestimmte Schutzbereiche einzurichten, sogenannte *Realms (Bereiche)*. Ressourcen lassen sich einem Realm so zuordnen, daß der Zugreifende gegenüber dem Server seine Identität nachweisen muß. Der Server entscheidet dann, ob dieser Benutzer den gewünschten Zugriff ausführen darf oder nicht.

Die Authentifizierung ist in Jigsaw als Eingabefilter realisiert. Wird dieser Filter für einen zu schützenden Bereich installiert, so muß jede Anfrage auf diese Ressource diesen Filter durchlaufen. In Jigsaw ist die in HTTP definierte *Basic*

Authentification implementiert. Der Server fragt hiebei nach der Benutzerkennung und dem Paßwort. Ferner püft Jigsaw auch die IP-Adresse des Benutzers. Diese Angaben werden aber unverschlüsselt übertragen, und bieten daher keinen sehr hohen Schutz gegenüber einem Angreifer. Abbildung 5.1 zeigt die in Jigsaw implementierte Hierarchie in Bezug auf die Authentifizierung.

Wie bereits erwähnt, können Filter nicht nur für die Authentifizierung genutzt werden, sondern stellen einen Mechanismus dar, der sich allgemein nutzen läßt, um *Requests* oder deren Ergebnisse zu bearbeiten. Jigsaw begrenzt zum Beispiel durch den Filter die Zahl der gleichzeitigen Zugriffe auf eine Ressource, ein weiterer leitet die Nutzdaten durch ein externes Programm.

5.1.3 Servlets

Zu den Nachteilen von Java-Applets gehört, daß sie bislang nur beim Client lauffähig waren. Jigsaw bietet die Möglichkeit, Objekte auf dem Server zu starten. Diese Objekte werden Servlets genannt. Im Vergleich dazu hat auch der von der Firma Sun entwickelte Server *Jeeves* die Fähigkeit serverseitige Anwendungen zu unterstützen [jeev98].

Servlets sind zu einem spezifischen Interface konforme Java-Objekte. Sie ähneln Applets insofern, als sie – dynamisch über das Netz zu ladende – Bytecode-Objekte sind. Andererseits haben Servlets kein eigenes grafisches Interface.

Man unterscheidet lokale und entfernte Servlets. Entfernte Servlets sind wie Applets durch eine URL-Adresse identifizierbar, lokale durch ihren Klassennamen. Servlets lassen sich direkt (durch Angabe eines Servlet-Namen) oder indirekt (durch Verknüpfung mit Dokumenten) aufrufen.

Anders als bei CGI-Anwendungen (Common Gateway Interface) wird für Servlets kein eigener Prozeß kreiert, was eine bessere Performance bewirkt. Fordert ein Client einen Servlet-URL an, so stößt ein Thread das Servlet an. Dieser Anstoß kann paralell erfolgen, so daß Multithreading möglich ist.

Servlets können zudem in einer Kette verbunden werden (Chaining), bei der die Ausgabe eines Servlets als Eingabe des nächsten fungiert. Auf diese Weise lassen sich Filter implementieren, deren erstes Servlet beispielsweise Benutzereingaben prüft, das zweite eine Datenbank abfragt und ein nächstes eine HTML-Tabelle erzeugt.

Das folgende kleine Servlet-Listing erzeugt das aktuelle Datum und die aktuelle Zeit, die anschließend ausgegeben werden:

```
import java.io.*;
import java.util.Date;
import java.util.Hashtable;
```

```
import javax.servlet.*;
import javax.servlet.http.*;

public class DateServlet extends HttpServlet {

    public void service(HttpServletRequest req, HttpServletResponse res)
        throws ServletException, IOException
    {
        Date today = new Date();
        res.setContentType("text/plain");

        ServletOutputStream out = res.getOutputStream();
         out.println(today.toString());
    }

    public String getServletInfo() {
        return "Returns a string representation of the current time";
    }
}
```

Server	Version	1.a	1.b	2.a	2.b	3	4.a	4.b
CERN-Server	3.0	11	10	11	11	NA	11	10
Apache	1.0.2	35	24	30	30	NA	33	30
Apache	1.1.1	42	30	35	33	85	34	31
phttpd	0.99.70.1	46	37	39	38	4	39	37
Jigsaw	1.0alpha1	22	18	19	9	26	19	8
Jigsaw	1.0alpha3	22	18	19	18	26	19	18

Tabelle 5.1: WWW-Server im Leistungsvergleich

5.1.4 Performance

Das W3-Konsortium führte einige Benchmarks durch und legte ein Ergebnis vor, welches die Anzahl der Anfragen pro Sekunde widerspiegelt. Der Leistungsvergleich wurde mit den in Tabelle 5.1 erwähnten Servern vorgenommen. Insgesamt wurden für jeden Server vier Benchmarks durchgeführt, die sich in der Art und Weise der Anfragen unterschieden. *1.a* und *1.b* waren Anfragen auf einzelne Dokumente der Größen 4KB bzw. 40KB. Bei *2.a* und 2.b wurden mehrere Dokumente gleichzeitig vom Server angefordert. Bei Benchmarks *3* handelte es sich um einen sogenannten *Keep-alive-Bench*. Abschließend wurde ein *Long-live-Bench* durchgeführt (*4.a* und *4.b*)

Bei den Zellen, die mit *NA* gekennzeichnet sind, konnte der Test nicht durchgeführt werden. Ausführliche Spezifikationen zu den Benchmarks sind in [jig2] zu finden.

In der Tabelle ist zu erkennen, daß die Geschwindigkeit von Jigsaw durchweg über der des CERN-Servers liegt, aber unterhalb der des Apache-Servers. Jigsaw kann also den vermeintlichen Nachteil durch den zusätzlichen Aufwand der Bytecode-Interpretation kompensieren [jig2].

5.2 Klassen und Konzepte

Im folgenden werden einige Bausteine näher beschrieben, die maßgeblich bei der Integration in das Server-System Bedeutung finden.

Abbildung 5.2 zeigt einen Ausschnitt des Servers, der einige Module bzw. Ressourcen widerspiegelt. Der Ausschnitt beschränkt sich auf die Anwendung von Filtern, Servlets und die Übertragungsmechanismen des Servers. Diese Komponenten kommunizieren über spezielle Schnittstellen miteinander.

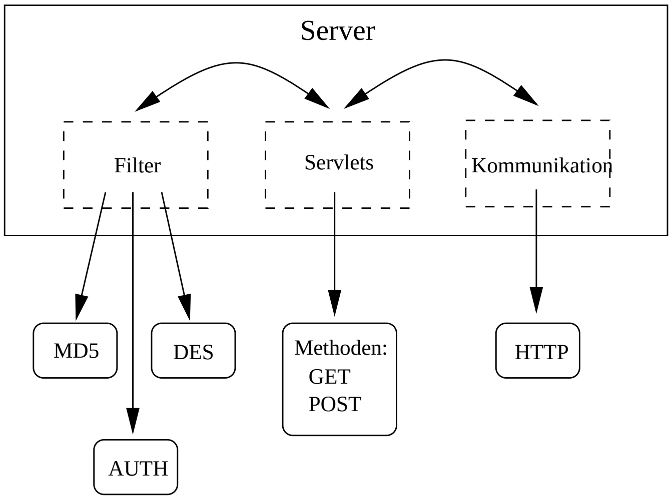

Abbildung 5.2: Ausschnitt des Servers

5.2.1 Kommunikation mit dem HTTP-Servlet

In Bezug auf Servlets und das Kommunikationsmanagement werden die Methoden *GET* und *POST* verwendet. Die HTTP-Kommunikation des Servers ist über die Ableitung des *HttpServlet* realisiert. Das *HttpServletRequest*-Objekt liefert den Zugriff auf die Übergabeparameter und die Umgebungsvariablen. Das *HttpServletResponse* gewärleistet neben dem Zugriff auf einen *OutputStream* auch die Möglichkeit auf Fehler-Codes zu reagieren. Das folgende Listing realisiert den Prototypen für die Kommunikation:

```
import javax.servlet.http.*;

public class ServersHTTPServlet extends HttpServlet {

   public void ServersPost (HttpServletRequest req, HttpServletResponse res)
       throws ServletException, IOException
       {
            // Reaktion auf POST-Parameter
       }

   public void ServersGet (HttpServletRequest req, HttpServletResponse res)
       throws ServletException, IOException
       {
            // Reaktion auf GET-Parameter
       }
}
```

5.2.2 Die Krypto-Ressource als Filter

Die Einbindung des Verschlüsselungmechanismus wird über einen speziellen Filter realisiert. Dieser Filter ist als Eingabe implementiert und integriert das Hash-Verfahren *MD5* (MD steht für *Message Digest*).

5.2.2.1 Funktionsweise von MD5

MD5 realisiert eine von Ron Rivest konstruierte Einweg-Hashfunktion. Der Algorithmus produziert einen 128-Bit Hashwert.

MD5 verarbeitet die Eingaben in Form von 512-Bit Blöcken, die in sechzehn 32-Bit Teilblöcke aufgeteilt werden. Als Ergebnis liefert der Algorithmus vier 32-Bit Blöcke, die aneinandergehängt den 128-Bit Hashwert liefern.

Zunächst wird die Nachricht so aufgefüllt, daß die Länge einem Vielfachen von 512 minus 64 Bit entspricht. Dabei wird an die Nachricht ein 1-Bit, entsprechend viele 0-Bits und eine 64-Bit Darstellung der Länge der Nachricht angehängt. Dieses Anhängen von Daten wird auch als *padding* bezeichnet [schn96].

Die Hauptschleife des Algorithmus wird für alle 512-Bit-Blöcke der Nachricht durchgefürt. Die Hauptschleife besteht aus vier Runden, die jeweils 16mal eine bestimmte Operation, d.h., eine nichtlineare Funktion auf die Eingabewerte ausführt. Die vier Operationen werden mit FF(), GG(), HH() und II() bezeichnet [schn96]. Die folgenden Prototypen realisieren die vier Operationen:

```
private final int FF(int a,int b,int c,int d,int x,int s,int ac) {
    a += (F(b, c, d) + x + ac) ;
    a = rotate_left(a, s) ;
    a += b ;
    return a ;
}

private final int GG(int a,int b,int c,int d,int x,int s,int ac) {
    a += (G(b, c, d) + x + ac) ;
    a = rotate_left(a, s) ;
    a += b ;
    return a ;
}

private final int HH(int a,int b,int c,int d,int x,int s,int ac) {
    a += (H(b, c, d) + x + ac) ;
    a = rotate_left(a, s) ;
    a += b ;
    return a ;
}

private final int II(int a,int b,int c,int d,int x,int s,int ac) {
```

```
    a += (I(b, c, d) + x + ac) ;
    a = rotate_left(a, s) ;
    a += b ;
    return a;
}
```

Kapitel 6

Zusammenfassung und Ausblick

Die vorliegende Diplomarbeit verschafft einen Überblick, die notwendigen Komponenten für eine Sicherheitsarchitektur zu bestimmen und die Verfahren zu deren Realisierung voneinander abzugrenzen. Gleichzeitig werden Forschungs- und Entwicklungstendenzen in den einzelnen Bereichen vermittelt.

Die Betonung im Titel dieser Diplomarbeit muß sicherlich auf dem Wort „Aspekte“ liegen, da im Verlauf dieser Arbeit immer wieder auf neue Anhaltspunkte und Quellen gestoßen wurde, die wiederum neue Sicherheitsprobleme aufdeckten. Das Ziel dieser Arbeit liegt somit nicht in der akribischen Aufzählung aller möglichen Sicherheitsprobleme, sondern darin, ein *Konzept für einen modularen und skalierbaren Server* zu entwickeln, der einerseits eine größtmögliche Sicherheit gegenüber den unterschiedlichen Angriffsarten ermöglicht und andererseits die Kosten dafür durch ein globales Konzept möglichst gering hält.

Mit dem zunehmenden Einsatz von Informationssystemen als Intranet im unternehmerischen Bereich und der steigenden Bedeutung von kommerziellen Transaktionen über das globale Internet rückt die Frage nach der Sicherheit der eingesetzten Verfahren in den Vordergrund. Eine Menge innovativer Techniken zielt auf die Absicherung der Datenübertragung über die Internet-Protokolle ab und das Angebot an kommerziellen Produkten zur Sicherung von IT-Systemen ist in der letzten Zeit stark angestiegen.

In dieser Arbeit werden über die technischen Hintergründe des Internet, Sicherheitsaspekte aufgezeigt und Lösungsansätze dargestellt. Diese Lösungsansätze werden so betrachtet, so daß diese in einem einheitlichem Konzept auftauchen. Einen großen Teil nehmen hier die Internet-Protokolle und die kryptographischen Verschlüsselungsverfahren und deren Anwendungen ein.

In die Konzeption des modularen Servers gehen primär die von der OSI vorgeschlagenen Sicherheitsdienste ein, die anschließend in der Implementierung berücksichtigt werden. Die Idee des Konzeptes ist, die Kommunikation über spezielle Server zu realisieren, die für eine sichere Datenübertragung, Authentifizierung von Benutzern, die Abrechnung von Dienstleistungen, sowie Zugriffsberechtigungen auf Datenbestände zuständig sind.

Diese Dienste, die gewisse Sicherheitsmaßnahmen realisieren, können allerdings keinen hundertprozentigen Schutz für IT-Systeme liefern. Derartige Ziele würden voraussetzen, daß alle auf einem System ausführbaren Aktionen vorhersehbar sind und somit Bedrohungen ausschließen.

Für diese unfangreichen Anforderungen müssen entsprechende Konzepte und Systeme entwickelt werden, die diese Aspekte aufgreifen. Diese Diplomarbeit geht einen Schritt in diese Richtung.

Glossar

Angreifer: Person, die einen →Angriff verübt.

Angriff: Bewußter und absichtlicher Versuch, eine →Verwundbarkeit in einem System auszunutzen.

AH (Authentication Header): Bestandteil von →IPSP. Felder im Protokollkopf zur Übertragung einer →digitalen Unterschrift der im Datagramm enthaltenen Daten. Siehe auch →ESP.

ARP (Adress Resolution Protocol): →Internet-Protokoll der Netzwerkzugangsschicht, das der Auflösung von →Internet-Adressen zu Adressen des Protokolls der Sicherungsschicht in Broadcast-Netzen (siehe auch →Ethernet) dient.

Asymmetrische Verschlüsselung (Public-Key-Kryptographie): Bezeichnung für kryptographische Verfahren, die auf dem Einsatz von Schlüsselpaaren beruhen. Eine mit dem einen Schlüssel eines Schlüsselpaaren verschlüsselte Nachricht kann nur mit dem zugehörigen zweiten Schlüssel entschlüsselt werden. Ein Schlüssel des Paares wird in der Regel öffentlich bekanntgegeben. Wird mit diesem öffentlichen Schlüssel eine Nachricht verschlüsselt, so wird deren Uneinsehbarkeit sichergestellt, da sie nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden kann. Wird im Gegensatz dazu mit dem privaten Schlüssel verschlüsselt, so können diese Verfahren zur Erstellung von →digitalen Unterschriften eingestzt werden. Siehe auch →RSA.

Authentifizierung: Verifizierung der Identität eines Kommuniukationspartners und Sicherstellung, daß diese Identität über die Dauer einer Kommunikationsbeziehung erhalten bleibt.

Basic Authentification: Einfacher Mechanismus zur →Authentifizierung des Benutzers, der seit der Version 1.0 Bestandteil von →HTTP ist und auf der Übertragung von Benutzername und Passwort beruht.

Brute-Force-Angriff: Versuch einen mit einem bekannten Verfahren verschlüsselten Klartext durch Ausprobieren aller möglichen Schlüssel zu entschlüsseln.

Die Dauer eines Brute-Force-Angriffs hängt wesentlich von der eingesetzten Schlüssellänge ab.

Bedrohung: Umstand, der direkt oder indirekt zu einem Schaden oder Sicherheitsverlust führen kann.

CPS (Certificate Policy Statement): Geschäftsbedingungen einer →Zertifizierungsstelle, die unter anderem Aufschluß über die Voraussetzungen für die Ausstellung eines Zertifikates geben.

DES (Data Encryption Standard): Symmetrisches Verschlüsselungsverfahren mit einer konstanten Schlüssellänge von 56 Bit und veröffentlichen Algorithmus. Wird in den USA bereits seit 1976 als Regierungsstandard für nichtklassifizierte Kommunikation eingesetzt.

Digitale Unterschrift: Mechanismus zur Gewährleistung der →Authentizität einer Nachricht durch Ergänzung um einen kryptographischen Code. Wird bei Verwendung von Verfahren der →asymmetrischen Verschlüsselung mit dem privaten Schlüssel erstellt.

Digital-ID: Siehe →Zertifikat.

DN (Distinguished Name, eindeutiger Name): Eindeutige Bezeichnung eines Eintrages im →X.500-Directory. Setzt sich aus den Werten der teilqualifizierten Attribute aller Einträge im Pfad bis zum Ursprung des Directory zusammen. Kommt auch in →X.509-Zertifikaten zum Einsatz.

Eindeutiger Name: Siehe →DN.

ESP (Encapsulated Security Payload): Bestandteil des →IPSP. Protokolldefinition zur verschlüsselten Übertragung eines →IP-Datagrammes (Tunnel Mode) oder des darüberliegenden Transportprotokolls (Transport Mode). Siehe auch →AH.

Ethernet: LAN-Protokoll der OSI-Ebene 2, das zur lokalen Vernetzung von Rechnern eingesetzt wird und Datenübertragungsgeschwindigkeiten von bis 100 Mbit/s erlaubt (Fast-Ethernet).

Filter: Spezielle →Ressource, die eine Anfrage an den Server vor oder nach dem Abruf manipuliert.

Firewall: Spezielle Computersysteme zum Schutz von privaten Datennetzen gegenüber eines öffentlichen Netzes.

Hash-Verfahren: Einweg-Funktion, die aus einer beliebigen Menge von Daten eine Prüfsumme fixer Länge, den sogenannten Message Digest, berechnet.

HTML (Hypertext Markup Language): Im →WWW eingesetzt Beschreibungssprache von Hypertext-Dokumenten. Beinhaltet neben der Struktur des Dokumentes auch die mit Hilfe von →URLs angegebene Hypertext-Verbindungen zu anderen Dokumenten oder auch anderen →Internet-Diensten.

HTTP (Hypertext Transfer Protocol): Auf dem Transportprotokoll →TCP aufbauendes →Internet-Protokoll, das zur Übertragung von →MIME-Entitäten dient. Wird in erster Linie im →WWW für den Transfer von →HTML-Dokumenten und darin enthaltenen Multimedia-Komponenten eingesetzt. Eine →Authentifizierung des Benutzers kann durch Angabe von Benutzername und Kennwort (→Basic Authentification) erforgen.

Hypertext: Textdokument, welches über besonders hervorgehobene Schlüsselwörter Verzweigungen in andere Textdokumente ermöglicht.

IDEA (International Data Encryption Algorithm): Symmetrisches kryptographisches Verfahren mit einer Schlüssellänge von 128 Bit und veröffentlichem Algorithmus.

IETF (Internet Engineering Task Force): Gremium, das die Weiterentwicklung der Internet-Technik durchführt. Die Aktivitäten der IETF finden in Arbeitgrippen statt, die sich bestimmten Themenbereichen widmen. Zur Koordination der Tätigkeit einer IETF-Arbeitsgruppe werden →Internet-Drafts oder im fortgeschrittenen Standardisierungsprozeß auch →RFCs eingesetzt.

Integrität (integrity): Die Integrität bezeichnet die Eigenschaft eines IT-Systems, nur erlaubte und beabsichtigte Veränderungen an gespeicherte, verarbeitete oder übertragene Information zuzulassen.

Internet: Aus dem →ARPANET hervorgegangener Zusammenschluß von →IT-Systemen und Netzen auf der Basis der →TCP/IP-Protokolle.

Internet-Adresse (IP-Adresse): Durch das →Internet-Protokoll definierte, welweit eindeutige Adresse einer Station im Internet. Die IP-Adresse besteht aus vier Bytes, die durch Punkte voneinander getrennt sind und läßt sich in eine für den →Routingvorgang benötigte Netzadresse und eine Host-ID unterteilen. Eine Erweiterung des zunehmend enger werdenden Adreßraumes ist durch →IPv6 vorgesehen. Da die IP-Adresse nicht unveränderlich mit einer bestimmten Station verbunden ist (siehe →ARP), kann sie nur eingeschränkt zur Identifikation von Rechnern eingestzt werden.

Internet-Dienst: Synonym für →Internet-Protokoll der Anwendungsebene im →OSI-Modell.

Internet-Draft: Formlose, befristet gültiges Arbeitsdokument im Standardisierungsprozeß der Internet-Technik. Wird häufig zur Dokumentation der Aktivitäten von →IETF-Arbeitsgruppen eingesetzt.

Internet-Protokoll (IP): 1. Das Internet-Protokoll ist der zentrale Bestandteil der Protokollfamilie TCP/IP auf der Vermittlungsebene und beschreibt unter anderem das Format der →Internet-Adresse und den →Routingvorgang.

2. Im Plural: Gesamtheit aller Protokolle für den Datenaustausch im Internet. Die in vier Schichten aufgebaute Protokollfamilie umfaßt auf der untersten Ebene Standards für den Netzwerkzugang (beispielsweise →ARP, →SLIB oder →PPP) auf der Vermittlungsschicht das zentrale Internet-Protokoll und auf der Transportschicht die Protokolle →TCP und →UDP. Auf der Anwendungsschicht werden schließlich Internet-Dienste wie →HTTP definiert.

IP-Adress-Spoofing: Rechner, der unter einer falschen →Internet-Adresse auftritt. Wird zumeist durch Modifikation der Absender-Adresse im →IP-Datagramm erreicht.

IPSP (IP Security Protocol): Von der →IPSEC-Arbeitsgruppe der →IETF entwickelte Standards zur Absicherung der →Internet-Protokolle auf Vermittlungsebene, die auch in die Enwicklung von →IPv6 Eingang findet. Umfassen Protokolldefinitionen (→AH und →ESP) sowie ein Protokoll zur Schlüsselverwaltung (→ISAKMP).

IPv6: Nächste Generation der →Internet-Protokolle. Die Entwürfe beinhalten unter anderem die Absicherung der Intermet-Protokolle in Übereinstimmung mit dem →IPSP sowie eine Erweiterung der Adreßinformation im →IP-Datagramm von vier auf sechs Bytes und dadurch eine Vergrößerung des Adreßraumes.

IT-System: Informationstechnisches System, das eingesetzt werden kann, um informationstragende Daten zu speichern, verarbeiten und übertragen.

Jigsaw : Ein in Java implementierter Server des W3-Konsortiums.

Kryptoanalyse: Teilgebiet der →Kryptologie, die sich mit der Analyse und Bewertung von krytographischen Verfahren befaßt.

Kryptographie: Teilgebiet der →Kryptologie, die sich mit dem Ver- und Entschlßseln von Nachrichten befaßt.

Kryptologie: Wissenschaft, deren Aufgabengebiet das „Verheimlichen von Nachrichten“ ist. Umfaßt die →Kryptographie und die →Kryptoanalyse.

Micropayment: Zahlungssystem im *Electronic Commerce*, das zur Abrechnung von Online-Artikeln mit geringem Wert eingesetzt wird.

MIME (Multipurpose Internet Mail Extension): Verfahren zur Spezifikation unterschiedlicher Dokumenttypen und Kodierungsverfahren, das für den Einsatz mit E-Mail (siehe auch →SMTP) entwickelt wurde.

Orange Book: Siehe →TCSEC.

OSI-Modell (Open Systems Interconnection): Modell aus sieben Schichten für den Datenaustausch in offenen Systemen. Standards der unteren vier Ebenen (Transportsystem) decken Bereiche wie Übertragungsmedien, Zugangsverfahren, Wegwahl oder Transportadressen ab. Die oberen drei Schichten (Anwendungssystem) behandelt zum einen Funktionalität wie Sitzungsmanagement und Datentransformation, zum anderen werden auch Anwendungsdienste standardisiert. Bedeutung erlangt das OSI-Modell in erster Linie als Referenzmodell zur Einordnung von Netzwerkprotokollen. Dokumentiert in der Form von Empfehlungen der →ITU-T, die zum Großteil auch als ISO-Standards übernommen wurden.

Paketfilter (Paket Sniffer): Software zum Abhören von Rahmen in einem Broadcast-Netz wie beispielsweise →Ethernet.

PGP (Pretty Good Privacy): Software zur →symmetrischen und →asymmetrischen Verschlüsselung von Daten. Wird im Internet häufig zur Übertragung von E-Mail über das →Internet-Protokoll →SMTP eingesetzt.

Port-Nummer (Dienstnummer): Bestandteil des Protokollkopfes von TCP-Segmenten oder UPD-Datagrammen.

Public-Key-Kryptographie: Siehe →Asymmetrische Verschlüsselung.

RC2, RC4, RC5: Von Ron Rivest für die →RSA Data Security entwickelte symmetrische Verschlüsselungsverfahren mit variabler Schlüssellänge.

Ressource: Objekt des Servers →Jigsaw. Beispielsweise eine Datei oder ein Verzeichnis.

RFC (Request For Comment): Vom Internet Architecture Board herausgegebene Norm. Zentrales Dokument im Standardisierungsprozeß der Internet-Technik. der Status eines RFCs gibt Aufschluß über den Stellenwert des Textes.

Routing: Weiterleiten von IP-Datagrammen über unterschiedliche Netze der OSI-Ebene zwei hinweg bis zum Zielnetz. Der Routingvorgang wird in der Regel von Internet-Routern durchgeführt, die untereinander Adreßinformationen mit Hilfe von Routing-Protokollen austauschen.

RSA: Von Ron Rivest, Adi Shamir und Leonard Adleman entwickeltes →asymmetrisches Verschlüsselungsverfahren.

Servlet: Objekt, welches serverseitig gestartet werden kann.

SET (Secure Electronic Transactions): Von den Kreditkartengesellschaften Visa und Mastercard entwickelter Standard zur sicheren Abwicklung von Kreditkartentransaktionen zwischen Verkäufer, Käufer und Clearing-Stelle über die →Internet-Protokolle.

S-HTTP (Secure-HTTP): Erweiterung von →HTML und →HTTP, welche die Übertragung von verschlüsselten und/oder digital unterschriebenen →MIME-Entitäten in beide Richtungen vorsieht. Diese Absicherung von HTTP auf der Anwendungsebene erlaubt den applikationsspezifischen Einsatz kryptographischer Verfahren.

SMTP (Simple Mail Transfer Protocol): Auf dem Transportprotokoll →TCP aufbauendes →Internet-Protokoll, das zur Übermittlung von E-Mail dient. Eine Authentifizierung des Benutzers wird nicht durchgeführt.

Sperrliste (Certificate Revocation List, CRL): Von einer →Zertifizierungsstelle periodisch veröffentliche Liste von ungültigen Zertifikaten. Die Publikation der Sperrliste erfolgt in elektronischer Form und mit →digitaler Unterschrift durch die ausstellene Zertifizierungsstelle. Die →X.509-Standards definieren unter anderem auch das Format von Sperrlisten.

SSL (Secure Socket Layer): Von der Firma Netscape entwickeltes Verfahren zur Absicherung der Internet-Protokolle auf der Transportschicht. Auf diese Weise können einzelne Anwendungsdienste (beispielsweise →HTTP) ohne Modifikation um →symmetrische Verschlüsselung und →Authentifizierung der Kommunikationspartner mit Hilfe von →X.509-Zertifikaten ergänzt werden.

Symmetrische Verschlüsselung: Bezeichnung für kryptographische Verfahren, die auf dem Einsatz des gleichen Schlüssels zur Ver- und Entschlüsselung von Daten beruhen.

TCP/IP: Bezeichnung für die Familie der →Internet-Protokolle, die auf die zentrale Bedeutung der Protokollstandards →TCP und IP (→Internet-Protokoll) eingeht.

TCSEC (Trusted Computer System Evaluation Criteria): Vom amerikanischen National Computer Security Center (NCSA) für das Department of Defense (DoD) veröffentlichter Standard, der Kriterien für die Bewertung der Sicherheit von Softwareprodukten behandelt. Wird auch als „Orange Book“ bezeichnet.

UDP (User Datagram Protocol): Verbindungsloses Kommunikationssteuerungsprotokoll auf Transportebene aus der Familie der Internet-Protokolle.

URL (Uniform Resource Locator): Format zur einheitlichen Spezifikation eines Internet-Dienstes sowie eines Datenobjektes.

Verfügbarkeit (availibility): Die Verfügbarkeit bezeichnet die Eigenschaft eines IT-Systems, bestimmte Dienstleistungen in zugesicherter Form und Qualität erbringen zu können. Die Verfügbarkeit von Information ist darin enthalten. Sie besagt, daß Information in entsprechender Frist und in erwarteter oder geforderter Form und Qualität zur Verfügung stehen muß.

Vertraulichkeit (confidentiality): Die Vertaulichkeit bezeichnet die Eigenschaft eines IT-Systems, gespeicherte, verarbeitete oder übertragene Information nur berechtigten Personen oder -gruppen zugänglich zu machen.

Verwundbarkeit: Schwäche in einem Sicherheitssystem, die entweder technisch bedingt ist oder aus dem Einsatz des Systems entsteht.

WWW (World Wide Web): Auf Hypertext basierendes Informationssystem im Internet.

X.509-Zertifikat: In der ITU-T-Empfehlung standardisiertes Format eines →Zertifikates zur Zertifizierung von Personen oder Server-Diensten. Dieses enthält unter anderem den öffentlichen Schlüssel und den →DN der zertifizierten Person sowie den →DN und die Unterschrift der ausstellenden →Zertifizierungsstelle.

Zertifikat (Digital-ID, digitaler Personalausweis): Durch die →digitale Unterschrift des Ausstellers hergestellte Bindung eines öffentlichen Schlüssels an eine bestimmte Ermächtigung. Im Fall der im Internet verbreiteten →X.509-Zertifikate handelt es sich dabei um die Identität einer Person oder eines Server-Dienstes. In diesem Fall übernimmt die ausstellende →Zertifizierungsstelle die Überprüfung der Identität in Übereinstimmung mit ihrem →CPS.

Zertifizierungsstelle (Certification Authority, CA, Trust Center): Aussteller von →Zertifikaten. Handelt es sich wie im Fall von →X.509-Zertifikaten um Identitätszertifikate, so übernimmt die Zertifizierungsstelle die Überprüfung der Identität der betroffenen Person oder des betroffenen Dienstes. Der für die Ausstellung eines Zertifikates notwendige Identitätsnachweis kann aus dem →CPS ersehen werden.

Zugriffskontrolle (Access Control): Vorgang der Überprüfung der Berechtigung eines Subjektes, eine Operation auf ein bestimmtes Objekt auszuführen.

Literaturverzeichnis

Printmedien

[ahuj96] V. Ahuja. *Network and Internet Security.* Academic Press, USA, 1996

[amor94] E.G. Amoroso. *Fundamentals of Computer Security Technology.* Prentice-Hall, New Jersey, 1994

[bada94] A. Badach, E. Hoffmann, O. Knauer. *High Speed Internetworking.* Addison-Wesley, Bonn, 1994

[bahn98] T. Bahnes. *Sicherheit auf der Transport- und Sitzungsschicht.* Seminarband, Universität Dortmund, Lehrstuhl Informatik 1, 1998

[barz91] H.W. Barz. *Kommunikation und Computernetze.* Hanser, München, 1991

[baur:93] F.L. Bauer. *Kryptologie.* Springer-Verlag, Berlin, 1989

[berg96] U. Bergmann. *WWW – Anbieten und Nutzen.* Hanser, München, 1996

[beye89] T. Beyer. *Sicherheitsprobleme von Computernetzen.* Springer-Verlag, Berlin, 1989

[bhim96] A. Bhimani. *Securing The Commercial Internet.* ACM Vol. 39, 1996

[birm96] K.P. Birman. *Building secure and reliable network applikations.* Manning Publications, Greenwich, 1996

[ches96] W.R. Cheswick, S.M. Bellovin. *Firewalls und Sicherheit im Internet.* Addison-Wesley, Deutschland, 1996

[come93] D. Comer, D. Stevens. *Internetworking with TCP/IP.* Prentice-Hall, USA, 1993

[cont97] M. Conti, E. Gregori, L. Lenzini. *Metropolitan Area Networks.* Springer-Verlag, London, 1997

[denn82] D.E. Denning. *Cryptography and Data Security.* Addison-Wesley, USA, 1982

[denn98] D.E. Denning, P.J. Denning. *Internet besieged: countering cyberspace scofflaws.* ACM Press, Oxford, 1998

[dod85] Department of Defense Standard. *Department Of Defense Trusted Computer System Evaluation Criteria.* DoD 5200.28-STD, Dezember 1985

[ehle94] S. Ehlers u.a. *Telekommunikation: Dienste, Übersichten, Entscheidungshilfen.* Verlag Technik, Berlin, 1994

[eich93] B. Eichler. *Informatios- und Vermittlungsdienste in offenen verteilten Systemen.* ADV, Wien, 1993

[fitz95] J. Fitzgerald. *Business Data Communications.* John Wiley & Sons, New York, 1995

[ford94] W. Ford. *Computer Communications Security-Prinziples, Standard Protocols and Techniques.* Prentice-Hall, Englewood Cliffs, 1994

[fuhr96] N. Fuhr. *Informationssysteme.* Skript zur Stammvorlesung, Universität Dortmund, Lehrstuhl Informatik 6, 1996

[full97] S. Fuller, K. Pagan. *Intranet Firewalls: Planning & Implementing Your Network Security System.* Ventana, USA, 1997

[fumy95] W. Fumy. *Standards und Patente zur IT-Sicherheit.* Oldenbourg Verlag, München, 1995

[gasm94] L. Gasman. *Broadband Networking.* VNR, New York, 1994

[gett96] J. Gettys. *Hypertext Transfer Protocol – HTTP/1.1.* Internet Draft, W3 Consortium/MIT, 1996

[hahn94] H. Hahn, R. Stout. *Internet Complete Reference.* Osborne McGray-Hill, USA, 1994

[hals88] F. Halsall. *Data communications, computer networks and OSI.* Addison-Wesley, Great Britain, 1988

[hans96] H.R. Hansen. *Wirtschaftsinformatik 1.* Lucius & Lucius, Stuttgart, 1996

[heid96] B. Heidecke. *Analyse und Bewertung von Sicherheitskonzepten in Client/Server-Systemen am Beispiel von Novell NetWare.* Diplomarbeit, Universität Dortmund, Lehrstuhl Informatik 1, 1996

[hoff95] L.J. Hoffman. *Building in Big Brother.* Springer-Verlag, New York, 1995

[hunt92] C. Hunt. *TCP/IP Network Administration.* O'Reilly, Sebastopol, 1992

[kern89] H. Kerner (Hrsg.). *Rechnernetze nach ISO-OSI, CCITT.* H. Kerner, Wolfsgraben, 1989

[kers91] H. Kersten. *Einführung in die Computersicherheit.* Oldenbourg Verlag, München, 1991

[klut96] R. Klute. *Das World Wide Web.* Addison-Wesley, Bonn, 1996

[kyas97] O. Kyas. *Internet Security – Risk Analysis, Strategies and Firewalls.* International Thomson Publishing, USA, 1997

[maie95] G. Maier, A. Wildberger. *In 8 Sekunden um die Welt: Kommunikation über das Internet.* Addison-Wesley, Bonn, 1995

[mart98] W. Martens. *Sicherheit auf der Anwendungsschicht: WWW.* Seminarband, Universität Dortmund, Lehrstuhl Informatik 1, 1998

[muft89] S. Muftic. *Security Mechanisms for Computer Networks.* Ellis Horwood, Chichester (UK), 1989

[niem95] K.D. Niemann. *Client/Server-Architektur.* Vieweg Verlag, Braunschweig/Wiesbaden, 1995

[oppl97] R. Oppliger. *IT-Sicherheit.* Vieweg Verlag, Braunschweig/Wiesbaden, 1997

[perl94] R. Perlman. *Interconnection: Bridges und Router.* Addison-Wesley, Deutschland, 1994

[pfle97] C.P. Pfleeger. *Security in Computing.* Prentice-Hall, USA, 1997

[rued95] R. Buck-Emden. *Die Client/Server-Technologie des SAP-Systems R/3.* Addison-Wesley, Deutschland, 1995

[sand96] W. Sander-Beuermann, S. Yanoff. *Internet: kurz und fündig.* Addison-Wesley, Bonn, 1996

[schm95] B. Schmid. *Elektronische Einzelhandels- und Retailmärkte.* Teubner Verlag, Stuttgart, 1995

[schn96] B. Schneier. *Applied Cryptography – Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, New York, 1996

[shaf94] S.L. Shaffer, A.R. Simon. *Network Security.* Academic Press, Cambridge, 1994

[siya95] K. Siyan, C. Hare. *Internet Firewalls and Network Security.* New Riders Publishing, Indianapolis, 1995

[smit97] R.E. Smith. *Internet cryptography.* Addison-Wesley, Massachusatts, 1997

[star97] T. Stark *Encryption for a Small Planet.* BYTE Magazine, März 1997

[stro98] O. Strozyk. *Sicherheit auf der Netzwerkschicht.* Seminarband, Universität Dortmund, Lehrstuhl Informatik 1, 1998

[stru95] A. Glade, H. Reimer, B. Struif (Hrsg.). *Digitale Signatur & Sicherheitssensitive Anwendungen.* Vieweg Verlag, Braunschweig/Wiesbaden, 1995

Online Dokumentationen

[atki95a] R. Atkinson. *Security Architecture for the Internet Protocol. RFC 1825*, August 1995

[atki95b] R. Atkinson. *IP Authentication Header. RFC 1826*, August 1995

[atki95c] R. Atkinson. *IP Encapsulating Security Payload (ESP). RFC 1827*, August 1995

[jig1] A. Baird-Smith. *Jigsaw Reference Manual.* W3-Konsortium, 1997 (Stand: 16.12.1997)
http://www.w3.org/pub/WWW/Jigsaw/User

[jig2] A. Baird-Smith. *Jigsaw Performance Evaluation.* W3-Konsortium, 1997 (Stand: 16.12.1997)
http://www.w3.org/pub/WWW/Jigsaw/User/Introduction/performance.html

[deer95] S. Deering, R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification. RFC 1883*, Dezember 1995

[hobb98] R. Hobbes. *Hobbes' Internet Timeline.* (Stand: 15.01.1998)
http://info.isoc.org/guest/zakon/Internet/History/HIT.html

[jeev98] Sun Microsystems, 1998 (Stand: 12.02.1998)
http://java.sun.com/products/jeeves

[karn95] P. Karn, P. Metzger, W. Simpson. *The ESP DES-CBC Transform. RFC 1829*, August 1995

[metz95] P. Metzger, W. Simpson. *IP Authentication using Keyed MD5. RFC 1828*, August 1995

[post81] J. Postel. *Internet Protocol: DARPA Internet Program Protocol Specification. RFC 791*, September 1981

[rsa98] RSA Laboratories. *Answers to Frequently Asked Questions About Today's Cryptography.* (Stand: 10.02.1998)
http://www.rsa.com