Modulbeschreibung

Modulbezeichnung:	Netzsicherheit 1
Studiengang:	OpenC^{3}S - Zertifikat
Verwendbarkeit:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 1
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Dozent(in):	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min. Schriftliche Prüfung
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	
Sprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	
Einordnung ins Fachsemester:	
Generelle Zielsetzung des Moduls:	
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h

Lerninhalt und Niveau:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei wer-den sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asym-metrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Einführung in lokale Netze, • WLAN (IEEE 802.11), • VPN (IPSec, PPTP, IP Multicast), • Mobilfunk (GSM, UMTS), Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzu-stellen.
Angestrebte Lernergebnisse:	*Fachkompetenz:* Die Studierenden erkennen die wichtigen Strukturen von Sicherheitsmechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Die Studenten können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Jedes Semester
Anerkannte Module:	
Anerkannte anderweitige Lernergebnisse / Lernleistungen:	
Medienformen:	

Literatur:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Computer Networks, Andrw S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modul 1

Netzsicherheit 1

Studienbrief 1: Grundlagen Lokaler Netze

Studienbrief 2: Drahtlose Netzwerke (WLAN & Mobilfunk)

Studienbrief 3: Point-To-Point Sicherheit

Studienbrief 4: IP Sicherheit (IPSec)

Studienbrief 5: IP Multicast

Autor:

Prof. Dr. Jörg Schwenk

---

1. Auflage

Ruhr-Universität Bochum

© 2014 Ruhr-Universität Bochum
Bochum
Universitätsstr. 150
44801 Bochum

1. Auflage (25. Februar 2014)

Didaktische und redaktionelle Bearbeitung:

Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Verfasser unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Axiom	A
Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Merksatz	M
Quelle	Q
Satz	S
Übung	Ü

II. Zu den Autoren

Prof. Jörg Schwenk leitet den Lehrstuhl Netz- und Datensicherheit an der Ruhr-Uni Bochum seit dem Jahr 2003. Von 1993 bis 2001 arbeitete er im Bereich Sicherheit der Deutschen Telekom in verschiedenen Industrieprojekten. Anschließend lehrte er zwei Jahre lang an der Georg-Simon-Ohm FH Nürnberg. Er hat mehr als 60 Patente und mehr als 40 wissenschaftliche Publikationen verfasst. Seine Forschungsinteressen umfassen kryptographische Protokolle (SSL/TLS, IPSec), XML- und Webservice-Security, sowie Web- und Internetsicherheit.

III. Modullehrziele

Die Kryptographie war lange Zeit eine Wissenschaft für Spezialisten. Bis in die zweite Hälfte des letzten Jahrhunderts beschäftigten sich mit ihr nur Militärs und Diplomaten. Mit dem Aufkommen der elektronischen Datenverarbeitung und der digitalen Kommunikation kamen weitere Spezialisten hinzu: Bankangestellte, Datenschützer, Mobilfunker, Pay-TV-Anbieter und auch die ersten Hacker.
Mit dem Erfolg des Internet änderte sich die Situation grundlegend. Jetzt hatte jeder die Gelegenheit, persönliche Nachrichten per E-Mail zu versenden, oder Waren mit einem Mausklick im World Wide Web zu kaufen.
Gleichzeitig wuchs das Bewusstsein, wie unsicher das neue Medium ist: Durch Abhörpläne der nationalen Regierungen (die ähnlich wie beim Brief- und Fernmeldegeheimnis auch hier Einschränkungen im Rahmen der Verbrechensbekämpfung durchsetzen wollten) und durch kriminelle Aktivitäten (wie z.B. den Diebstahl von Kreditkartennummern von Webservern).

Zum Glück wurde im Jahr 1976 die Public Key-Kryptographie erfunden, die sich bestens für das offene Internet eignet. Die erste Implementierung des bekanntesten Public Key-Verfahrens RSA wurde unter dem Namen „Pretty Good Privacy (PGP)“ bekannt und begann, sich unter den Internet-Nutzern zu verbreiten. Damit begann der Siegeszug der Kryptographie im Internet: „Privacy Enhanced Mail“ und „Secure MIME“ für E-Mail, sowie SSL für das World Wide Web folgten. Schließlich wurde das Internet-Protokoll IP selbst mit den verschiedenen IPSec-Standards abgesichert.

Ziel dieses Moduls ist es, dem Leser eine fundierte Einführung in verschiedene Gebiete der Netzsicherheit zu geben. Damit soll er in die Lage versetzt werden, sich anschließend mit geringer Mühe in den Referenzdokumenten zurechtzufinden und mit ihrer Hilfe das passende Sicherheitssystem zu konzipieren oder zu implementieren.
Diesem Ziel dienen auch die zahlreichen Abbildungen, mit denen jeweils versucht wird, das im Text Gesagte (oder zu Ergänzende) graphisch möglichst anschaulich und einprägsam darzustellen.

Das Modul ist streng praxisorientiert, d.h. es wird nur die heute tatsächlich eingesetzte Kryptographie behandelt.
Zum didaktischen Konzept des Moduls gehören auch die angeführten erfolgreichen Angriffe auf Sicherheitsstandards (WEP, PPP, GSM, IPSec): Aus den Fehlern anderer Standards kann man lernen. Diese Darstellungen sollen also nicht dazu verleiten, eigene Angriffe auf bestehende Infrastrukturen zu starten, sondern der Leser soll sie beim Entwurf eigener Konzepte stets im Hinterkopf behalten.

Studienbrief 1 Grundlagen Lokaler Netze

1.1 Lernziele

Sie haben das OSI- und TCP/IP-Schichtenmodell verstanden. Sie kennen die Aufgaben, die Protokolle je nach Ansiedlung in den Schichten haben. Sie können Protokolle den Schichten der Referenzmodelle zuordnen.

Speziell lernen sie das Internet Protokoll (IP), das den Datenverkehr im World Wide Web reguliert, als Beispiel kennen.

1.2 Advanced Organizer

In diesem Studienbrief werden wir Sicherungsprotokolle auf der ersten und zweiten Schicht des OSI-Schichtenmodells, bzw. der ersten Schicht des TCP/IP-Modells betrachten. Auch wenn wir hier nicht näher auf die höheren Schichten eingehen, stellen wir alle Schichten ausführlich dar und ordnen das TCP/IP Modell in das OSI-Schichtenmodell ein.

1.3 Referenzmodelle

1.3.1 Das OSI-Referenzmodell

Das OSI-Schichtenmodell wurde von der Inernational Standard Organization (ISO) durch Day und Zimmermann 1983 entwickelt [DZ83]. Dies war der erste Schritt zur internationalen Standardisierung verschiedener Protokolle für eine Weltweite Kommunikation. Das Modell wurde 1995 nochmals in [Day95] durch John Day überarbeitet. Die Abkürzung OSI steht hier für *Open Systems Interconnection*, da es für die Verbindung offener Systeme gedacht ist. Dies sind Systeme, die kompatibel für die Kommunikation mit anderen Systemen sind.

Die Sieben Schichten des OSI-Modells basieren auf den folgenden Überlegungen:

1. Sobald ein neuer Abstraktionsgrad notwendig ist, soll eine neue Schicht eingeführt werden.

2. Die Funktion jeder Schicht sollte exakt definiert sein.

3. Die Funktionen jeder Schicht sollten unter Berücksichtigung von international genormten Protokollen gewählt werden.

4. Die Abgrenzung der Schichten sollte so definiert werden, dass der Informationsfluss über die Schnittstellen minimal ist.

5. Die Anzahl der Schichten sollte so groß sein, dass möglichst keine unterschiedlichen Funktionen in einer Schicht zusammen arbeiten müssen, aber klein genug, damit das Modell nicht unhandlich und unübersichtlich wird.

Nun betrachten wir in den folgenden sieben Abschnitten die einzelnen Schichten des OSI-Modells. Dabei arbeiten wir uns von unten nach oben vor. Zu beachten ist, dass das OSI-Modells keine Netzarchitektur darstellt, da die Details der Dienste und Protokolle in den einzelnen Schichten nicht angegeben sind. Die ISO hat hierfür in einem zusätzlichen internationalen Standard Normen ausgearbeitet, die kein direkter Bestandteil des OSI-Modells sind. Das Modell wird, selbst wenn die zugehörigen Protokolle längst nicht mehr verwendet werden, noch verwendet.

Die Bitübertragungsschicht

Die *Bitübertragungsschicht* (physical layer) organisiert die Übertragung von reinen Bits über einen Kommunikationskanal. Beim Design von Protokollen dieser Schicht muss Folgendes beachtet werden: Wenn eine Seite ein `1` Bit auf den Weg schickt, muss auch auf der anderen Seite ein `1` Bit ankommen und kein `0` Bit. Die entscheidenden Fragen sind hier: Welches elektrische Signal soll eine logische `1` oder `0` repräsentieren? Wie lang soll die Repräsentation sein? Soll gleichzeitig in beide Richtungen kommuniziert werden? Wie wird die Erstverbindung etabliert? Wie wird eine Verbindung getrennt, wenn beide Seiten fertig sind? Wie viele Pins hat ein Netzwerkstecker und wofür werden diese verwendet? Die Probleme liegen hier hauptsächlich beim Design elektrischer, mechanischer und zeitorientierter Schnittstellen sowie des physikalischen Mediums, welches sich unterhalb der Bitübertragungsschicht befindet.

Die Sicherungsschicht

Die *Sicherungsschicht* (data link layer) hat zur Hauptaufgabe eine reine Übertragungseinrichtung in eine Leitung zu verwandeln, in der keine unerkannten Fehler mehr auftauchen. Das wird durch Maskieren der realen Fehler erreicht, so dass diese in der Vermittlungsschicht gar nicht mehr auftreten. Erreicht wird dies, indem der Sender die zu vermittelnden Daten in *Datenframes* (data frame) einteilt (typisch sind einige Hundert oder ein paar Tausend Byte) und diese Frames sequentiell überträgt. Ein zuverlässiger Dienst bestätigt den fehlerfreien Empfang eines Frames, indem ein *Bestätigungsframe* (acknowledgement frame) als Antwort verschickt wird.

Ein weiteres Problem, welches auf der Sicherungsschicht (sowie den meisten höheren Schichten auch) auftritt, besteht darin einen sehr schnellen Sender daran zu hindern langsamere Empfänger mit einer zu großen Datenlast zu überfordern. Für dieses Problem gibt es eine Art Verkehrsregelung, die dem Sender mitteilen kann, wenn er mehr Daten senden kann, ohne den Empfänger zu überlasten.

Ein Broadcast Netzwerk wirft in der Sicherungsschicht zusätzlich die Frage auf, wie der Zugriff auf den gemeinsam verwendeten Kanal gesteuert werden kann. Die Lösung dieses Problems ist die *MAC*-Teilschicht (Medium Acccess Control). Dies ist eine spezielle Zwischenschicht der Sicherungsschicht, die den Medienzugriff steuert.

Die Vermittlungsschicht

Die *Vermittlungsschicht* (network layer) organisiert den Betrieb des Subnetzes. Eine der wichtigsten Designaufgaben ist die Auswahl der Paketrouten vom Ursprungs-

zum Bestimmungsort. Es gibt zwei unterschiedliche Herangehensweisen zum Lösen dieser Aufgabe: die Routen können durch statische Tabellen, welche fest im Netzwerk „verdrahtet“ sind organisiert sein, oder sie können (was der Normalfall ist) automatisch aktualisiert werden, was den Ausfall von einzelnen Komponenten kompensieren kann. Die Routen können aber auch zu Beginn jeder neuen Verbindung wie z.B. dem Anmelden an einem entfernten Server, festgelegt werden. Die Tabellen können natürlich auch sehr flexibel sein und für jedes Datenpaket neu ausgewählt werden um eine optimale Verteilung der Netzwerklast zu gewährleisten.

Wenn sich zu viele Pakete gleichzeitig in einem Subnetz befinden stehen sie sich gegenseitig um Weg und erzeugen Engpässe. Für solche Überlastungssituationen ist die Vermittlungsschicht zusammen mit höheren Schichten, welche die auf das Subnetz geleitete Last anpassen, verantwortlich. Die Qualität des bereitgestellten Dienstes (Verzögerung, Übertragungszeit, Jitter etc.) gehört jedoch zu den Aufgaben der Vermittlungsschicht.

Weitere Probleme können entstehen, wenn ein Paket auf seinem zum Ziel verschiedene Netzwerke durchqueren muss. Mögliche aufkommende Probleme könnten hier sein, dass die Netze unterschiedliche Adressierungen verwenden, oder dass das zweite Netz könnte die Datenpakete ablehnen, da sie zu groß für das Netz sind. Diese Probleme, sowie weitere mögliche Probleme dieser Art, müssen auf der Vermittlungsschicht gelöst werden um heterogene Netze miteinander zu verbinden.

Die Transportschicht

Die Aufgabe der *Transportschicht* liegt darin, Daten von der darüber gelegenen Schicht zu übernehmen und passend an die Vermittlungsschicht zu übergeben. Dabei muss sichergestellt werden, dass alle Teile der Daten am anderen Ende richtig ankommen. Wichtig ist hierbei, dass die Änderungen effizient durchgeführt werden und die oberen Schichten von Änderungen der Hardwarekomponenten unabhängig sind. Dies ist wichtig, da Hardwareänderungen unvermeidlich sind und im Laufe der Zeit anfallen werden.

Die Transportschicht bestimmt darüber hinaus auch die Art des Dienstes, welcher der Sitzungsschicht – und letztendlich dem Netzbenutzer – zur Verfügung gestellt wird. Die gebräuchlichste Art einer Transportverbindung ist ein fehlerfreier Punkt-zu-Punkt Kanal, über den die Nachrichten in Sendereihenfolge übermittelt werden.

Die Transportschicht stellt eine echte Ende-zu-Ende Schicht dar; sie transportiert die anfallenden Daten den gesamten Weg vom Ursprung bis zum Ziel. In anderen Worten kann man sagen, dass ein Programm am Ursprung mit einem analogen Programm am Ziel kommuniziert und dabei die selben Nachrichten Header und Steuerdaten verwendet. Auf den unteren Schichten arbeitet jedes Protokoll zwischen einem Rechner und seinem direkten Nachbarn und nicht zwischen dem eigentlichen Ursprung und dem eigentlichen Ziel. Diese sind möglicherweise durch eine Vielzahl an Routern und Netzen voneinander getrennt.

Die Sitzungsschicht

Die *Sitzungsschicht* (session layer) stellt den Benutzern die Möglichkeit zur Verfügung, von verschiedenen Rechnern Sitzungen untereinander aufzubauen. Diese Sitzungen stellen diverse Dienste zur Verfügung, wie zum Beispiel eine *Dialogsteuerung* (dialog control), welcher organisiert wer gerade Daten übertragen darf, oder eine *Token Verwaltung* (token management), die verhindert, dass zwei Parteien eine wichtige Operation parallel durchführen und eine *Synchronisation* (synchronization), die bei langen Übertragungen Fixpunkte setzt, von denen nach einem Verbindungsabbruch unter einer neuen Verbindung die Datenübertragung fortgesetzt werden kann.

Die Darstellungsschicht

In den unteren Schichten werden Protokolle angesiedelt, die die Übertragung einzelner Bits organisieren. Die *Darstellungsschicht* (presentation layer) hat die Syntax und Semantik der auf über die unteren Schichten übertragenen Daten zum Inhalt. Unterschiedliche Computer mit unterschiedlichen Betriebssystemen haben intern unterschiedliche Datendarstellungen, sollen aber trotzdem in einem Netzwerk untereinander kommunizieren können. Um dies zu ermöglichen, müssen die ausgetauschten Datenstrukturen abstrakt definiert werden, sowie eine Standardcodierung, welche „in der Leitung“ verwendet wird. Dies wird in der Darstellungsschicht verwaltet, so dass Datenstrukturen auf höheren Ebenen definiert und ausgetauscht werden können.

Die Anwendungsschicht

In der *Anwendungsschicht* (application layer) gibt es eine Vielzahl von Protokollen, welche von den Benutzern des Netzwerkes häufig verwendet werden. Das am häufigsten eingesetzte Protokoll ist wohl *HTTP* (HeyperText Transfer Protocol), welches die Grundlage des weltweiten Internets bildet. Ruft ein Benutzer zum Beispiel eine Webseite auf, so sendet der Browser den Namen der Seite über HTTP an den Host-Server der Webseite. Der Inhalt der Seite wird dann vom Server via HTTP zurück an den Browser gesendet, welcher die Seite dem Benutzer dann präsentiert. Weitere Beispiele für Protokolle der Anwendungsschicht sind die Mail Protokolle IMAP und POP, sowie andere Datenübertragungsprotokolle wie FTP.

1.3.2 Das TCP/IP Referenzmodell

ARPNET

In diesem Abschnitt wenden wir uns dem Referenzmodell zu, welches im ARPNET – dem Vorgänger aller Rechnernetze – und seinem Nachfolger – dem weltweiten Internet – verwendet wird. Ursprünglich war das ARPNET ein vom US Militär gefördertes Forschungsnetzwerk, welches einige hundert Universitäten in Nordamerika miteinander verbunden hat. In der ersten Version kommunizierten die einzelnen Standorte über gemietete Telefonstandleitungen. Später, als Satelliten- und Funknetzwerke hinzukamen, musste allerdings eine neue Referenzarchitektur gefunden werden, da die Verbindungsprotokolle einige Probleme aufwiesen. Somit wurde von Anfang an klar, dass der Fokus beim Entwurf des Modells auf einer nahtlosen Verbindung von unterschiedlichen Netzen lag. Das entstandene

Konstrukt wurde später nach den beiden Hauptprotokollen TCP und IP benannt und gilt heute als das *TCP/IP Referenzmodell*. Das Modell wurde 1974 erstmals von Cerf und Clark beschrieben [CK74] und 1989 von Barden als Standard in der Internetgemeinde definiert [Bra89].

Geschichtlich wurde das Internet also während des Kalten Krieges geboren. Eine große Sorge des US Verteidigungsministeriums war, dass Teile, oder sogar das gesamte Netzwerk durch nur einen gezielten Raketenangriff seitens der Sowjetunion auf einen Router lahm gelegt werden könnte. Somit galt als erklärtes Ziel, dass selbst bei einem Hardwareausfall einzelner Subnetze das Gesamte Netzwerk überlebensfähig bleibt und dass sogar bestehende Verbindungen (Gespräche) nicht unterbrochen werden. Kurz gesagt wollte das Verteidigungsministerium, dass solange die miteinander kommunizierenden Geräte intakt sind, die Verbindung nicht unterbrochen wird; selbst wenn einige der dazwischen liegenden Geräte ausfallen.

Die Netzzugangsschicht

Die hoch dynamischen Ansprüche an das Netzwerk führten dazu, dass das Netzwerk paketvermittelt auf der Grundlage einer verbindungslosen Schicht operiert. Die *Netzzugangsschicht* (link layer) – die unterste Schicht in dem Modell – bietet eine Beschreibung davon, was die Verbindungen wie etwa Serielle Leitungen oder Ethernet erfüllen müssen, um den Anforderungen der verbindungslosen Internetschicht zu genügen. Im eigentlichen Sinne ist die Netzzugangsschicht also keine Schicht, sondern eine Schnittstelle zwischen Hosts und Übertragungsleitungen.

Die Internetschicht

Die *Internetschicht* (internet layer) ist der Klebstoff, der das gesamte Netzwerkkonstrukt zusammen hält. Die Aufgabe der Internetschicht besteht darin, Pakete vom Host aus in jedes beliebige Netz einzuspeisen und an das Ziel zu befördern. Das Ziel und der Weg dorthin können potentiell unterschiedliche Netze sein und durchlaufen. Die Reihenfolge der Datenpakete muss dabei nicht eingehalten werden. Das bedeutet, die Daten können in anderer Reihenfolge erhalten werden, als sie gesendet wurden. Die Aufgabe der übergeordneten Schicht besteht in diesem Fall mitunter darin, die Daten wieder in die richtige Reihenfolge zu ordnen, wenn diese notwendig für die weitere Verarbeitung ist.

Die Internetschicht definiert ein offizielles Paketformart und ein Protokoll zur Datenvermittlung, welches den Namen *IP* (Internet Protocol) trägt. Das Protokoll *ICMP* (Internet Conrol Message Protocol) ist ein weiteres unterstützendes Protokoll der Internetschicht. Die IP-Pakete richtig zuzustellen ist die Aufgabe der Internetschicht. Dabei ist offensichtlich das Paket-Routing eines der Hauptprobleme.

Die Transportschicht

Über der Internetschicht im TCI/IP Modell liegt die *Transportschicht* (transport layer). Die Transportschicht im TCP/IP Modell soll, wie die Transportschicht im

OSI Modell, die Kommunikation zwischen Peer-Prozessen auf Quell- und Zielhost ermöglichen. Für diesen Zweck wurden die beiden Protokolle *TCP* (Transport Control Protocol) und *UDP* (User Datagram Protocol) definiert.

TCP ist ein zuverlässiges, erbindungsorientiertes Protokoll, welches einen Datenstrom von einem Rechner über das Internet zu einem anderen Rechner fehlerfrei übermittelt. Die eingehenden Daten werden in einzelne Nachrichten aufgeteilt und an die Internetschicht übermittelt. Am Zielrechner werden die einzelnen Datenpakete (welche in konfuser Reihenfolge ankommen können) vom TCP Prozess wieder zum ursprünglichen Datenstrom in richtiger Reihenfolge zusammengesetzt. Zusätzlich verwaltet TCP auch noch eine Flusskontrolle, welche sicherstellt, dass langsame Empfänger nicht von einem zu großen Datenstrom überlastet werden.

Das andere Protokoll UDP ist ein unzuverlässiges, verbindungsloses Protokoll. UDP wird verwendet, wenn die Reihenfolge der eingehenden Daten eine geringere Priorität hat als die zeitige Zustellung. Dies ist zum Beispiel bei Sprach- oder Videoübertragungen der Fall.

Die Anwendungsschicht

Es hat sich gezeigt, dass die Sitzungs- und Darstellungsschichten aus dem OSI-Modell für die Praxis nicht notwendig sind. Aus diesem Grund existieren sie im TCP/IP-Modell gar nicht.

Die oberste Schicht im TCP/IP Modell bildet die *Anwendungsschicht* (application layer). Sie beherbergt alle Protokolle aus den höheren Schichten. Ein paar Beispiele aus den frühen Zeiten des Internets sind Protokolle wie FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) und TELNET (virtuelles Terminal).

Abb. 1.1: Die Einordnung von OSI- und TCP/IP-Schichtenmodell

	OSI Modell	TCP/IP Modell	Protokolle
7	Anwendungsschicht	Anwendungsschicht	Telnet, FTP, SMTP, HTTP, DNS, NFS
6	Darstellungsschicht		
5	Sitzungsschicht		
4	Transportschicht	Transportschicht	TCP, UDP
3	Vermittlungsschicht	IP - Schicht	IP
2	Sicherungsschicht	Netzzugangsschicht	Ethernet, ATM, PPP, Frame Relax, X.25, IEEE 802.3/802.11
1	Bitübertragungsschicht		

1.4 Das Internet Protokoll IP

Das Internet Protocol (IP) hat in den letzten Jahren alle anderen Netzwerkprotokolle weitgehend verdrängt. Die Gründe für diesen verdienten Erfolg sind vielfältig und reichen von der sauberen Aufgabenteilung zwischen IP und TCP (Transport Control Protocol) – welches im Modul Netzsicherheit 2 genauer betrachtet wird – über die Verbreitung von Open Source Software bis hin zum Erfolg des WWW in der Geschäftswelt.

Das Internet Protocol in der aktuellen Version 4 [RFC 791] und der zukünftigen Version 6 [RFC 1883, RFC 2460] ist ein Netzwerkprotokoll und somit in der Vermittlungs- oder Netzwerkschicht (network layer) des OSI-Modells angesiedelt.

Aufgabe von IP ist es, Datenpakete über verschiedene Netzwerke hinweg von einem Quellrechner A hin zu einem Zielrechner B zu transportieren. IP arbeitet dabei verbindungslos und paketorientiert, d.h. es wird keine virtuelle Verbindung zwischen A und B aufgebaut, über die alle Pakete gesendet werden (dies ist z.B. bei ATM der Fall), sondern jedes IP-Paket wird einzeln behandelt, und Pakete von A nach B können durchaus auf verschiedenen Wegen transportiert werden.

Rechner werden in IP-Netzen durch ihre IP-Adresse identifiziert. Dies ist für IPv4 ein (in der Regel weltweit eindeutiger) 4 Byte-Wert. Traditionsgemäß wird dabei jede solche Adresse in „dotted decimal notation“ angegeben, d.h. jedes Byte wird als vorzeichenlose Dezimalzahl interpretiert, und die vier Bytes werden durch Punkte getrennt. (Z.B. lautet die IP-Adresse des Webservers der Ruhr-Universität Bochum `134.147.64.11`.)

In IPv6 sind die Adressen viel länger, nämlich 128 Bit oder 16 Byte. Sie werden hexadezimal geschrieben, wobei je 16 Bit zu einem Block zusammengefasst werden. Die 16 Bit Blöcke werden durch Doppelpunkt getrennt: `FFFE:8000:0:0:123:4567:89AB:CDEF` beschreibt z.B. eine IPv6-Adresse mit lokaler Gültigkeit in einem Netzsegment (Link Local Unicast Address).

Abb. 1.2: Ein typisches IPv4-Paket.

IP wird meist in Verbindung mit dem Transportprotokoll TCP benutzt (zunehmend häufiger auch UDP), und beide Header benötigen jeweils standardmäßig 20 Byte. Die Länge des Datenblocks wird oft auf 1460 Byte begrenzt, damit das ganze Paket in einem Ethernet-Frame transportiert werden kann. Die theoretische Maximallänge eines IP-Pakets beträgt 65535 Byte.

In einem IP-Netz entscheiden Router anhand der IP-Zieladresse über die Weitergabe des Pakets. Sie gehen dabei nach dem „best effort“-Prinzip vor, indem sie „nach besten Kräften“ versuchen, die Pakete beim Empfänger abzuliefern, die Pakete aber im Fehlerfall gelöscht und nur eine Fehlermeldung zurück an den Absender geschickt wird. Aufgabe von TCP ist es dann, die Daten zuverlässig beim Empfänger abzuliefern, ggf. durch mehrfaches Senden des gleichen IP-Pakets.

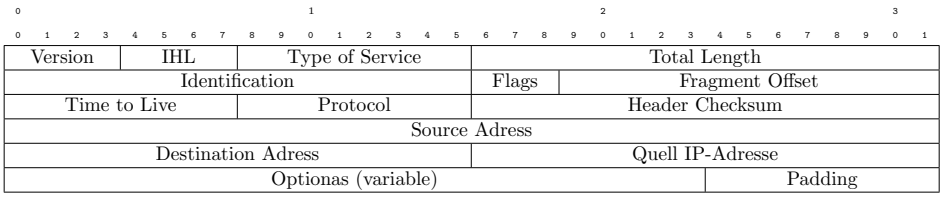

Abb. 1.3: Der IPv4-Header. Die wichtigsten Felder sind die IP-Zieladresse der Pakets (“Destination Address“) und die IP-Nummer des Absenders (“Source Address“).

IP-Pakete besitzen einen Header, der alle Informationen darüber enthält, wie mit dem Paket zu verfahren ist (Bild 1.4). Dieses Prinzip muss man auch bei der Verschlüsselung und Authentisierung von IP-Paketen beachten: Alle Informationen, wie ein Paket entschlüsselt und seine Authentizität überprüft werden können, müssen in einem zusätzlichen Header enthalten sein, der jeweils hinter dem IP-Header eingefügt wird. Da es sich bei der Kommunikation auf IP-Ebene oft um die Kommunikation zweier gleichberechtigter Partner handelt, basieren die meisten Vorschläge zum Schlüsselmanagement für IP-Sicherheit auf dem Schlüsselvereinbarungsprotokoll von Diffie und Hellman, das ja auch nur zwei gleichberechtigte Partner kennt. Wir werden uns im Studienbrief 4 ausführlich mit der Absicherung einer Verbindung auf IP-Ebene beschäftigen.

Ü

Übung 1.1

Laden Sie das Programm WIRE**SHARK** von der Homepage `http://www.wireshark.org/` herunter. Schneiden Sie mit diesem Tool den Datenverkehr in Ihrem Netzwerk mit. Beobachten Sie, welche IP Adresse Ihrem eigenen Computer zugeordnet ist und was für Daten Sie mit anderen Servern austauschen.

Unter Linux können Sie den Hostnamen mit dem Kommandozeilenbefehl `resolveip` den Hostnamen zu einer IP Adresse zuordnen. So finden Sie beispielsweise heraus, dass die IP Adresse `134.147.64.11` dem hostname `www1.rz.ruhr-uni-bochum.de` zugeordnet ist.

Studienbrief 2 Drahtlose Netzwerke (WLAN & Mobilfunk)

2.1 Lernziele

Sie kennen die kryptografische Primitiven, mit denen WEP und GSM abgesichert werden. Sie verstehen die Designfehler von RC4 und können diese gezielt ausnutzen um in der Praxis WEP zu brechen. Sie kennen den Aufbau und das Zusammenspiel der Komponenten von GSM und UMTS.

2.2 Advanced Organizer

Funknetzwerke erfordern ein hohes Maß an Sicherheitsmechanismen. Einem Angreifer stehen eine Vielzahl von Möglichkeiten zur Verfügung die Integrität und Authentizität von Daten in Funknetzwerken wie einem WLAN oder dem Mobilfunk zu kompromittieren.

In diesem Studienbrief gehen wir zunächst auf die Unsicherheiten von WEP ein. Wir werden den Angriff auf WEP sowohl theoretisch, wie auch praktisch verstehen und durchführen. Im zweiten Teil des Studienbriefes besprechen wir die Sicherheitsmechanismen von GSM und UMTS. Hierzu werden wir die Angreifermodelle genauer beleuchten.

2.3 Wireless LAN

Der Inhalt dieses Abschnittes ist das Kapitel 7.2 aus dem Buch [Sch10]. Lesen Sie die Seiten 186 bis 189.

2.4 Mobilfunk

Der Inhalt dieses Abschnittes ist das Kapitel 7.3 aus dem Buch [Sch10]. Lesen Sie die Seiten 189 bis 194.

Studienbrief 3 Point-To-Point Sicherheit

3.1 Lernziele

Sie kennen den Aufbau des Point to Point Protokolls. Sie verstehen warum ein praktischer Angriff möglich ist. Sie können neue Protokolle hinsichtlich ihrer Sicherheit gegen eine spezielle Klasse von Angriffen untersuchen.

3.2 Advanced Organizer

Die Sicherungsschicht (OSI-Schicht 2) dient eigentlich zur verlässlichen Übertragung von Datenrahmen ("Frames") zwischen zwei Computern (oder aktiven Netzwerkkomponenten) über ein einheitliches physikalisches Medium (z.B. eine direkte Kupferdraht-Verbindung) [Tan03]. Zu den Protokollen, die auf dieser Ebene eingesetzt werden, zählen so unterschiedliche Verfahren wie Ethernet (eine Rundfunksendung auf einem Draht) und diverse Modemstandards (Übertragung von Daten als Folge von Tönen über eine analoge Telefonverbindung). Mittlerweile ist das Einsatzgebiet von Schicht-2-Protokollen vielfältiger geworden. Es reicht von neuen physikalischen Medien wie Wireless LAN oder Mobilfunk bis hin zu Verbindungen, die größere Distanzen im Internet überbrücken.

7	Anwendungsschicht	Anwendungsschicht	Telnet, FTP, SMTP, HTTP, DNS, NFS
6	Darstellungsschicht		
5	Sitzungsschicht		
4	Transportschicht	Transportschicht	TCP, UDP
3	Vermittlungsschicht	IP - Schicht	IP
2	Sicherungsschicht	Netzzugangsschicht	Ethernet, ATM, PPP, Frame Relax, X.25, IEEE 802.3/802.11
1	Bitübertragungsschicht		

Abb. 3.1: Das TCP/IP-Schichtenmodell

Lese Aufgabe

Der Inhalt dieses Studienbriefes ist das Kapitel 7.1 aus dem Buch [Sch10]. Lesen Sie die Seiten 176 bis 186.

Studienbrief 4 IP Sicherheit (IPSec)

4.1 Lernziele

Sie haben ein detailliertes Wissen über die Mechanismen das Internet Protokoll abzusichern. Sie verstehen die technischen Herausforderungen ein so komplexes Protokoll wie IP sicher zu machen.

4.2 Advanced Organizer

In diesem Studienbrief konzentrieren wir uns auf die Vermittlungsschicht des OSI Modells und ihre Sicherheitsmechanismen.

Durch diese „evolutionäre Verdrängung“ hat sich die technisch günstige Situation ergeben, dass es auf der Netzwerkschicht fast aller Netzwerke ein einheitliches Datenformat gibt (vgl. Bild 4.1). Diese Tatsache kann man sich zunutze machen, wenn man mit einem einzigen Sicherheitsmechanismus eine Vielzahl von Anwendungen absichern möchte: Man kann auf der Ebene der IP-Pakete Verschlüsselung und Authentikation einsetzen.

7	Anwendungsschicht	Anwendungsschicht	Telnet, FTP, SMTP, HTTP, DNS, NFS
6	Darstellungsschicht		
5	Sitzungsschicht		
4	Transportschicht	Transportschicht	TCP, UDP
3	Vermittlungsschicht	IP - Schicht	IP
2	Sicherungsschicht	Netzzugangsschicht	Ethernet, ATM, PPP, Frame Relax, X.25, IEEE 802.3/802.11
1	Bitübertragungsschicht		

Abb. 4.1: Das TCP/IP-Schichtenmodell und seine Einordnung in das 7-Schichtenmodell der OSI. Für die Vermittlungsschicht gibt es im Internet nur ein einziges Protokoll: IP.

Lese Aufgabe

Der Inhalt dieses Studienbriefes ist das Kapitel 5 aus dem Buch [Sch10]. Lesen Sie die Seiten 124 bis 157.

Studienbrief 5 IP Multicast

5.1 Lernziele

Sie kennen die Schwierigkeiten Broadcastsysteme gegen Angriffe abzusichern. Sie kennen unterschiedliche Techniken Systeme sicher zu machen. Sie können die Sicherheit von Lösungen eigenständig analysieren.

5.2 Advanced Organizer

Multimedia-Daten werden oft von einer Gruppe von Nutzern gleichzeitig empfangen. Beispiele dafür sind Radio und Fernsehen: Die Daten werden im Rundfunk-Modus ("Broadcast") gesendet, und jeder Nutzer, der innerhalb des Sendebereichs ein passendes Gerät besitzt, kann durch Auswahl der jeweiligen Frequenz (bzw. des Kanals, Transponders) diese Daten empfangen.

Weniger bekannt sind die Techniken, die von Pay-TV-Anbietern verwendet werden, um ihre Inhalte nur zahlenden Abonnenten zukommen zu lassen. Man könnte diese Techniken als „selektiven Broadcast" oder auch als „Multicast über ein Broadcast-Medium" bezeichnen. Wir werden in den Studienbriefen kurz auf diese Techniken eingehen, da sie mittlerweile Eingang in die Internet-Standardisierung gefunden haben.

Der Trend zur Digitalisierung von Radio und Fernsehen lässt diese Medien enger mit dem Internet zusammenwachsen: Man kann jetzt IP-Pakete über Fernsehkanäle übertragen (z.B. über Satellit), und Radioprogramme über das Internet. Daher muss nach Möglichkeiten gesucht werden, wie man typische Radio- und Fernsehdienste, und insbesondere Pay-TV, im Internet möglichst effizient realisieren kann. Die Technik dafür, IP Multicast [RFC 1112], gibt es schon seit einigen Jahren.

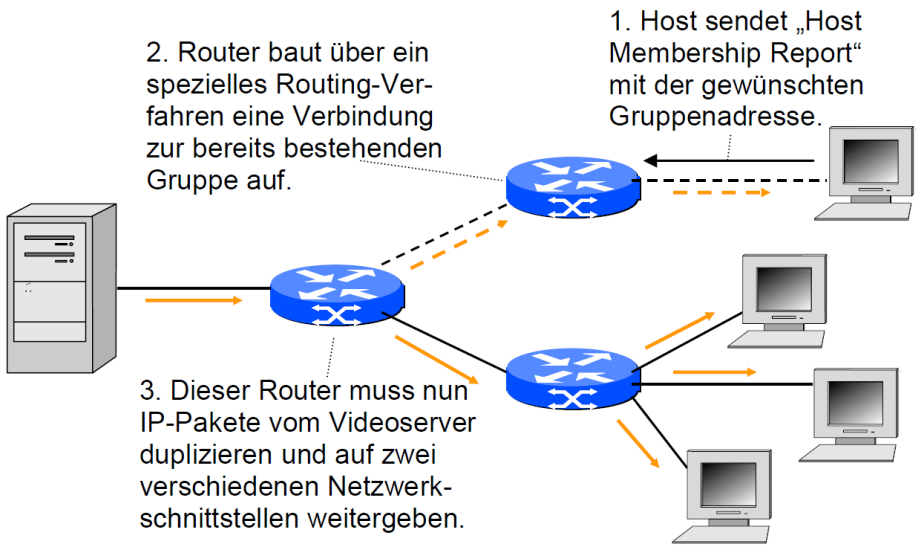

Abb. 5.1: Ein Host „abonniert" eine IP Multicast-Gruppe.

Lese Aufgabe

Der Inhalt dieses Studienbriefes ist das Kapitel 6 aus dem Buch [Sch10]. Lesen Sie die Seiten 158 bis 175.

Verzeichnisse

I. Abbildungen

II. Tabellen

III. Literatur

[Bra89] R. Braden, *Requirements for internet hosts - communication layers*, Tech. report, RFC1812] [RFC2277] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, 1989.

[CK74] Vinton G. Cerf and Robert E. Khan, *A protocol for packet network intercommunication*, IEEE TRANSACTIONS ON COMMUNICATIONS **22** (1974), 637–648.

[Day95] John Day, *The (un)revised osi reference model*, SIGCOMM Comput. Commun. Rev. **25** (1995), no. 5, 39–55.

[DZ83] J. D. Day and H. Zimmermann, *The OSI reference model*, Proceedings of the IEEE **71** (1983), no. 12, 1334–1340.

[RFC 1112] S.E. Deering, *Host extensions for IP multicasting*, RFC 1112, Internet Engineering Task Force, August 1989.

[RFC 1883] S. Deering and R. Hinden, *RFC 1883: Internet Protocol, version 6 (IPv6) specification*, December 1995, Obsoleted by RFC2460 [RFC 2460]. Status: PROPOSED STANDARD.

[RFC 2460] ———, *RFC 2460: Internet Protocol, Version 6 (IPv6) specification*, December 1998, Obsoletes RFC1883 [RFC 1883]. Status: DRAFT STANDARD.

[] J. Postel, *DoD standard Internet Protocol*, RFC 0760, Internet Engineering Task Force, January 1980.

[RFC 791] ———, *RFC 791: Internet Protocol*, September 1981, Obsoletes RFC0760 [**?**]. Status: STANDARD.

[Sch10] Jörg Schwenk, *Sicherheit und kryptographie im internet - von sicherer e-mail bis zu ip-verschlüsselung (3. aufl.)*, Vieweg, 2010.

[Tan03] Andrew S. Tanenbaum, *Computernetzwerke (4. aufl.)*, Pearson Studium, 2003.