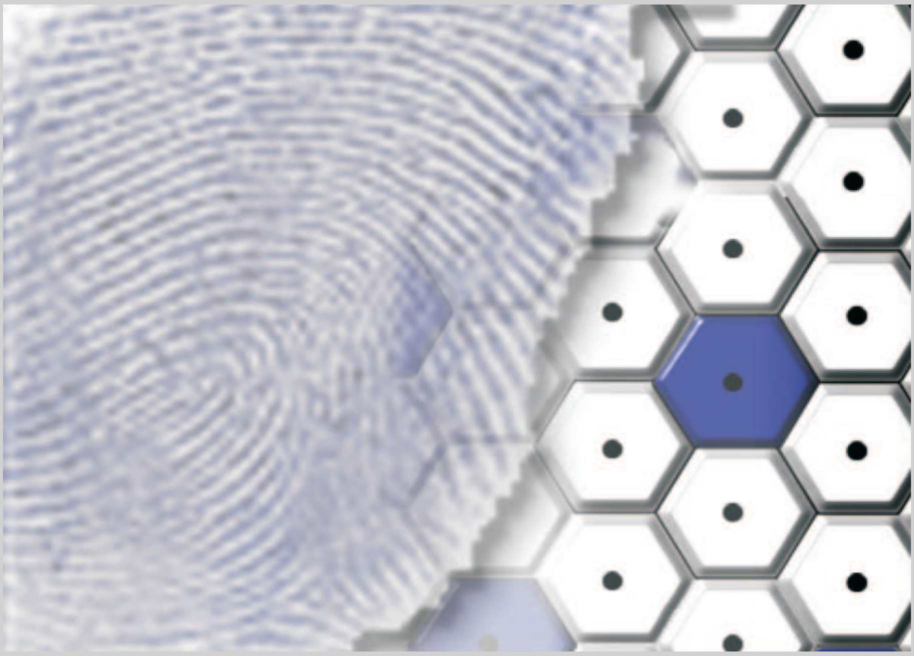
FernUniversität in Hagen



Network Security 1

Course Unit 1:
Introduction

Author:
Prof. Dr.-Ing. Firoz Kaderali

under collaboration of:
B. Cubaleska, A. Essoh, J. Gellweiler, T. Kisner,
B. Löhlein, N.-E. Ourahou, W. Qiu, S. Schaup,
G. Steinkamp, S. Songsiri, O. Stutzke

000 000 000 (04/06) **21731/7/01/S 1**

Table of Contents

Course Unit 1

1 Introduction

1.1 IT-Security in a networked world

The Internet is a world-wide network of computers, which has grown historically. The resulting work space (Cyberspace) is full of dangers, since protection from attacks on computers and their communication is incomplete. This is essentially due to the fact that during the development of the language of the Internet, the Transport Control Protocol/Internet Protocol (TCP/IP), security aspects were not taken in to consideration. For example TCP/IP in the wide-spread version 4 does not know of encryption (not even the encryption of passwords). Furthermore the sender addresses of a message can easily be forged and even complete messages can be forged or redirected by the intermediate nodes of the network, the routers. When using the Internet for both private and commercial applications it is therefore necessary to take additional security measures.

Cyberspace

TCP/IP

If an unauthorized person gains access to a computer or a communication network, data is in danger of being spied on, forged or deleted. Even the computer or network itself can be tampered with or crash. Depending on the application affected, an attack can have diverse and sometimes even disastrous consequences. Attacks range from industrial espionage and spying on public offices to the forgery and prevention of business and financial transactions. Personal privacy can also be affected.

The problems faced by Internet Security which are presented here, are only one aspect of Network Security dealt with in this course. Similar security problems can, in principle, be identified in every network and protocol, both wired and wireless. The number and scale of these IT-Systems has been constantly growing for several years and as a result of that, IT-Security has become more and more significant.

This becomes clear when the number and variety of attacks on network security is regarded. The following list provides a small selection of incidences:

I Love You *Virus, Mai 2000*
Estimated damage: 15 Bil. $

Code Red *Worm, July 2001*
Self-replicating malicious code that exploits a known vulnerability in Microsoft IIS servers. Performs Distributed Denial of Service (DDoS) attack on www1.whitehouse.gov.

Beagle *mass-mailing Worm, January 2004*
Distributes by using its own SMTP engine and over P2P-Networks. Works as Spam-Relay. Deactivates Virus-Scanners and other security related software.

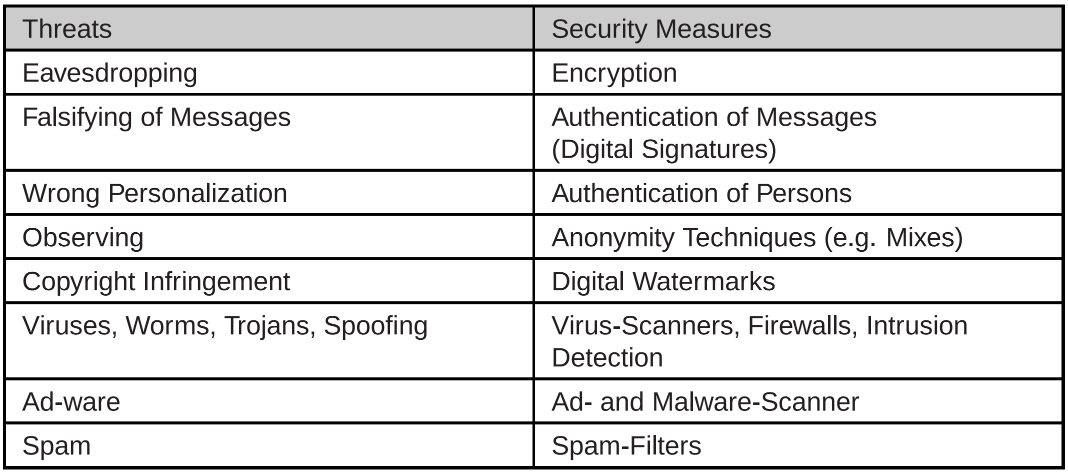
Phatbot *Worm/Botnet, April 2004*
Distributes by using backdoors of other Worms and Viruses as well as a

wide range of exploits and via mass-mailing. Builds remote controllable P2P networks for e.g. DDoS attacks and SPAM actions. ”Features” could be extended remotely on a modular basis.

EPOC.Cabir *Virus, June 2004*
First Bluetooth-Virus.

Spoofing attack *July 2004*
on German credit institute “Postbank”.

This list represents only a small excerpt of current incidents. Further occurrences can be found almost daily in the press. The large number of successful attacks on data and network security does not equate with the amount of technical security measures currently available. An analysis of threating scenarios leads to the following table:



Threats	Security Measures
Eavesdropping	Encryption
Falsifying of Messages	Authentication of Messages (Digital Signatures)
Wrong Personalization	Authentication of Persons
Observing	Anonymity Techniques (e.g. Mixes)
Copyright Infringement	Digital Watermarks
Viruses, Worms, Trojans, Spoofing	Virus-Scanners, Firewalls, Intrusion Detection
Ad-ware	Ad- and Malware-Scanner
Spam	Spam-Filters

A detailed analysis of these technical security measures (which are mostly based on hard cryptological methods) would go beyond the scope of this introduction. However from the author’s opinion, these methods are adequate to provide reasonable data and network security. In practice however the use of these methods is insufficient. This again is on the one hand because of the lack of user know-how and technical personnel (the lack of perception of dangers also belongs to this) and on the other hand because of the lack of suitability of these products and service for everyday life. With respect to the scope of network security, significance should be placed on education as well as on research and development.

In this course unit the application of above mentioned security mesures in current networks and protocols is elaborated in more detail.

1.2 Overview of this course

The Course *Network Security* consists of two parts: *Network Security I* and *Network Security II*. Each part consists of seven course units. The seven course units of Network Security I cover the six chapters: Introduction, Basics, Internet Security Protocols, World Wide Web Security, Anonymity Techniques, Packet Filters and Firewall Systems. Network Security II covers six chapters: Application Layer Security, Security in Wireless and Mobile Networks, Electronic Payment Systems, Security Aspects in Mobile Agent Systems, Copyright Protection and Intrusion Detection.

The following sections provide an overview of the contents of Chapters 2-12.

This chapter closes with a list of references and recommended readings.

1.3 Basics

In order to deal with network security, some basic knowledge is required. The kinds of attackers and attack scenarios on hosts and networks must be known as well as the security models and levels which can be extrapolated from them.

Furthermore a fundamental understanding of the basic techniques of communication networks is necessary. Knowledge and an understanding of the seven layers of the OSI reference model, the utilized switching techniques and the components involved in communication networks is of fundamental importance.

Additionally one should be familiar with the internet protocol family, should be familiar with the emergence and the history of the internet as well as the structure of the internet protocol stack. The fundamental protocols of the internet layer (IP) and the transport layer (TCP, UDP and ICMP) are of significant importance along with the security problems of the IP protocol family and common internet services.

An outline of this basic knowledge is given in Chapter 2.

1.4 Internet Security Protocols

The Internet protocol suite (TCP/IP) has been designed without consideration of security. It is very easy to spoof IP addresses, manipulate DNS and to eavesdrop the links.

Recently several cryptographic protocols have been proposed, specified, and partly implemented in the Internet and the WWW. The development of Internet standards for security (i.e. RFCs[1] published as a standard track document) has been slow. The first RFC to introduce a security-oriented protocol into the TCP/IP suite did not appear until 1987, with the publication of the first e-mail security protocol specifications. In the following years, a number of security-oriented Internet protocols were developed and are recently at various stages in the Internet standardisation process.

[1] Request for Comment

Internet Society, IAB, IETF, IRTF

Internet standards are formally developed under the auspices of the **Internet Society**, whose technical arm is the **Internet Architecture Board (IAB)**. IAB consists of two taskforces: **Internet Research Task Force (IRTF)** and **Internet Engineering Task Force (IETF)**. IETF consists of a large number of working groups (WG), where the bulk of standard development takes place. Despite the greatly increased activity in security standards in the IETF, the Internet is still not completely secure (the protocols developed must be used!).

IPSec

SSL, TSL

In chapter 3 we outline and briefly discuss some Internet security protocols. In the case of TCP/IP based networks, cryptographic security protocols can operate at any layer of the corresponding communications protocol suite. There are many proposals for providing security services at the network access, IP, transport and application layer. Here we focus on the **IPSec** set of security protocols in the IP layer and two transport layer security protocols, namely the **secure sockets layer (SSL)** and the **transport layer security (TLS) protocols**.

1.5 World Wide Web Security

The World Wide Web was originally developed as a publishing medium for public documents and therefore provided few controls for restricting access to information. As a wider range of documents and services appeared on the web, improved security facilities to satisfy the new requirements were needed.

There are basically three overlapping types of security risks regarding the World Wide Web ([Ste98]):

1. Bugs or misconfiguration problems in the Web server.
2. Browser-side risks.
3. Interception of network data sent from browser to server or vice versa by network eavesdropping.

Hypertext Transfer Protocol (HTTP)

Following a short introduction, chapter 4 deals with the principles of authentication in the sessionless **Hypertext Transfer Protocol (HTTP)** and then in Section 4.3 “Server-side security” and Section 4.4 “Client-side security” with the first two of the above-mentioned risks. Measures to protect from the third risk are dealt with in Chapter 3.

1.6 Anonymity Techniques

The objective of encryption is to achieve confidentiality of information. However, the fact that two people communicate is not disguised. The frequent opinion *Those who do not have to hide something need not be anonymous* may apply to everyday life but is not relevant in communication networks like the Internet, where vast possibilities for data recording and data mining are available.

For example, each user leaves traces when an e-mail is sent: all computers involved in the transport know both the sender and the receiver of the message. If this – as in most cases – is not encrypted, the content can be observed. This also applies to other services such as FTP (File Transfer Protocol), chat sessions or newsgroups.

There are examples of everyday life where not only the content of a message but also sender, receiver, and the fact that they communicated, are anonymous:

- Paying cash is an anonymous business. The payer cannot be identified via the coins used.
- Phone calls to charitable organizations (Samaritans, help for drug addicts etc) have to be anonymous. Such a guarantee is also desired by anonymous newsgroups in electronic networks.
- Box numbers in newspapers: the name of the person who advertised remains unknown.

If we transfer these examples into electronic communications environments, it is often difficult to satisfy both the demand for anonymity and reliability. Many solutions for the problems mentioned, do not achieve complete anonymity, they only achieve pseudo anonymity where a trustworthy third party carries out the anonymization.

Chapter 5 deals with some basic ideas of anonymity used in the **Mix-** and the **DC-concept** and introduces the following four basic types of anonymity: Sender Anonymity, Recipient Anonymity, Mutual Anonymity and Unobservability.

Mix-concept, DC-concept

1.7 Packet Filters and Firewall Systems

With host security you enforce the security of each host machine separately and make the effort to avoid or alleviate all the known security problems that might affect that particular host. Host security is hard to achieve and does not scale in the sense that as the number of hosts increases, the ability to ensure that security is at a high level for each host decreases. On the other hand, a network security model concentrates on controlling network access to your various hosts and the services they offer, rather than on securing them one by one. Network security approaches include building intermediate systems to protect your internal systems and networks, using strong authentification approaches, like public-key or one-time passwords, and using encryption and integrity checks to protect particularly sensitive data as it transits the network through routers.

Packet Filters
Firewall Systems

In Chapter 6, we discuss possible solutions to achieve network security with **packet filters** and/or **firewalls (firewall systems)**. There are many different definitions of the term ”firewall” in the literature. A firewall represents a blockade between a privately owned and protected intranet, that is assumed to be secure and its users are trusted, and another network, typically a publicly owned network or the Internet. The later is assumed not to be secure and not trustworthy. The purpose of the firewall is to prevent unwanted and unauthorized communication into or out of the protected network.

In [CB94] a firewall system is defined as a collection of components placed between two networks that collectively have the following properties:

1. All traffic from inside to outside, and vice versa, must pass through the firewall.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.

3. The firewall system itself is immune to penetration.

These properties are design goals. A failure in one aspect does not necessarily mean that the collection is not a firewall, but simply that it is not a good one. Consequently, there are different grades of security that a firewall can achieve. Note that there must be a local security policy when the rules of the firewall systems are established.

Application Gateways

Other definitions of firewall systems include connections and data streams from inside to outside and vice versa and must be strongly authenticated by users. In this case, the firewall system has to operate at higher layers in a communication protocol stack where information about users is available. These systems require the use of **application gateways**. Systems which only operate at lower layers without authentification information about the end users or connections are called packet filters. For the sake of clarity, in Chapter 6 we make a clear distinction between packet filters (operating at the network layer, Internet layer or transport layer in the Internet protocol stack) and firewalls operating at some higher layer.

The contents of Chapter 6 are categorized in five parts. Beginning with part 1 which deals with packet filtering followed by part 2 and 3 which introduce circuit-level and application-level gateways. Part 4 discusses how to set up network topologies for packet filters or firewall systems to make an intranet secure and finally, part 5 lists some further reading.

1.8 Application Layer Security

Users interact at the application layer of the OSI reference model for communication. The application layer must be protected as vigorously as the other layers of the OSI model.

Providing security at the application layer is also the most flexible, because the scope and strength of the protection can be tailored to meet the specific needs of the application [Opp00]. With this approach, application protocols must be modified to provide security services as well as programs written for these protocols. A disadvantage is that these new applications must be available to both communication parties. For example, S-HTTP (Secure Hypertext Transfer Protocol) is a security-enhanced HTTP protocol. An S-HTTP session requires the availability of an S-HTTP-capable client and an S-HTTP-capable server.

The focus of Chapter 7 is on security issues intrinsic to the application layer.

There are many application protocols and services layered on top of TCP and UDP (User Datagram Protocol). The most important of them will be outlined next. For each application protocol, we will focus on its security weaknesses and give alternatives, or security-enhancements proposed to provide the security required. So in Chapter 7, we will deal with:

1. Remote terminal access, implemented by the Telnet remote login protocol.
2. File transfer, implemented by the file transfer protocol (FTP).
3. The network file system (NFS) which uses RPC (Remote Procedure Call) to provide transparent file access over a network.

The topics S/MIME and executable content which are subject to network security will be introduced in Chapter 7.

1.9 Security in Wireless and Mobile Networks

Mobile networks have become a very attractive channel for the provision of electronic services: They are available almost anytime, anywhere, and the user acceptance of mobile devices is high. As a result, there is an ever increasing amount of services offered by mobile networks. They range from simple speech and information services to sensitive applications like banking or electronic commerce. But this is not the only reason that the security of data and signalling of information play a very important role. Communication traffic can be eavesdropped by everyone with very simple devices due to the very sensitive radio path of the data.

In Chapter 8 we will a have brief look at the development of mobile networks to date. The main discourse in Chapter 8 concentrates on the security in **GSM** networks. Further topics are the security mechanisms in **UMTS** networks, in the **WAP** protocol, in **WLAN** and in the **Bluetooth** standard.

GSM, UMTS, WAP, WLAN, Bluetooth

1.10 Electronic Payment Systems

With the rapid growth of the Internet, and particularly the World Wide Web (WWW), a major new industry has developed worldwide – electronic commerce. Online auctions, shopping portals and online book stores have become routine in our daily life. Also in areas of communication and transactions between government and public authorities with citizens (so-called **G2C**) and in **business to business (B2B)** the Internet and the WWW are used for more efficiency and for faster and more comfortable completion of real world processes. But whenever transactions are involved, in most applications payment is made in traditional ways. The most common payment method used in the WWW today is Credit-Cards.

G2C
B2B

Electronic payment systems enable secure payment (transfer of funds between different parties) in insecure network environments using newly developed cryptographic techniques. Most of us are familiar with electronic payment: we check our account balance and tenants transfer rent, gas, water and electricity bills via on-line internet services, etc. Electronic payment systems can be characterized in several ways: by the way in which money transfer is organized or by the type of information to be exchanged. Existing payment systems are Credit Card-based, electronic check, electronic cash and micropayment systems. Furthermore, electronic cash systems may be distinguished as **on-line** or **off-line systems** according to whether banks are involved during the payment process. Electronic cash resembles conventional cash. In Credit Card-based systems, bank accounts of customers are transferred via open networks and money is represented by numbers in the accounts. The Micropayment system is a special group in which the value of money per transaction is small and fixed with lower security requirements.

on-line, off-line systems

Various secure network payment schemes have been developed at universities and different research institutes as well as commercial organizations. Some of them have undergone small scale testing and some of them have been proven to fail for some reasons (for example, some unconditional privacy protecting systems could be eventually misused by criminals for blackmailing or money laundering).

New technologies, including new security tools, new cryptographic algorithms and new protocols are needed to protect privacy during transactions and to make the systems more secure, more efficient and more acceptable to organizations and individuals.

Chapter 9 introduces the main technologies involved in most payment systems currently available to network users. The characteristics of electronic payment systems are described in Section 9.2. We classify electronic payment systems in Section 9.3 and explain some systems from each category in Section 9.4. Chapter 9 ends with a bird’s eye view on the future of electronic payment systems.

1.11 Security Aspects in Mobile Agent Systems

Over the last decade, computer systems have evolved from centralized computing devices supporting static applications, into client-server environments that allow complex forms of distributed computing. Throughout this evolution limited forms of code mobility have existed: the earliest being remote job entry terminals used to submit programs to a central computer and the latest being Java applets downloaded from web servers into web browsers.

A new phase of evolution is now under way that goes one step further, allowing complete mobility of cooperating applications among supporting platforms to form a large-scale distributed system. This evolutionary path is the **mobile agent technology**. The mobile agent technology offers a new computing paradigm in which a program in the form of a software agent or a mobile agent, can start the execution of its code on a host computer, transfer itself to another agent-enabled host on the network, and resume the execution of the code on the new host.

mobile agent technology

The challenges of mobile agents lie in the lack of proven applications, security, infrastructure and standards. Applications using mobile agent technology are, for example e-Commerce, Software distribution, Information retrieval, System administration and Network management. Infrastructures can be viewed as system components. In a mobile agent system, these infrastructures (i.e. communication, naming ser- vice, controlling and locating) should be provided. Communication defines how a mobile agent communicates with other mobile agents. Some existing commu- nication protocols are message passing protocol and synchronous communication. Naming service is the process of efficiently naming a mobile agent in such a way that each mobile agent possesses a unique name. In other words, given a mobile agent's name, one can identify the owner of this mobile agent and distinguish this mobile agent from other mobile agents belonging to the same owner. Locating is the process of locating the current position of a mobile agent in the system. Controlling is composed of how mobile agents migrate (i.e. code serialization), how a visited host executes a visiting mobile agent.

Standards characterize general rules for applications using mobile agent implementations. Security is hard to achieve for mobile agents. It is generally composed of protecting mobile agents from malicious hosts and protecting hosts from malicious mobile agents. In Chapter 10, we emphasize security issues of mobile agent systems. The contents of Chapter 10 are categorized into four parts. Beginning with part 1 which provides an introduction to the agent technology. Part 2 demonstrates the history of the mobile agent concept. Part 3 introduces an overview of mobile agent systems. And finally, part 4 explains explicitly security issues of mobile agent systems.

1.12 Copyright Protection

Not everything on the Internet is public domain and may be taken without permission from the creator/owner. Copyright is the protection of published works. There are some technologies that can be used to protect and enforce copyrights on works published on the Internet. Two of these technologies are **watermarking** and **fingerprinting**.

watermarking, fingerprinting

Copyright protection becomes more difficult in the digital world than in the analogue world. A copy of digital data can be easy, inexpensive, and quickly created and distributed. Moreover, such a copy is not distinguishable from the original[2].

In Chapter 11 we will a have brief look at Copyright protection.

1.13 Intrusion Detection

With an increasing number of interconnected devices, modern technology can be used to it´s fullest potential, but, at the same time the potential risk of attacks which can be insider misuse, theft of proprietary information, viruses, software vulnerabilities, etc. also rises. With regard to vulnerabilities reported to the Computer Emergency Response Team (CERT), there was an increase of a factor of 32 in the past ten years (http://www.cert.org). Further, it can be observed that the attacks are also becoming more sophisticated – from password guessing at the beginning to more advanced attacks today such as malicious code attacks, website defacement, Distributed Denial of Service (DDoS), etc.

The Internet is an open and distributed system and a security challenge, especially as this open system becomes more complex. This, along with growing interconnectivity[3], the complexity of applications, operating systems and related protocols offered via the network as well as subconscious security behaviour of many users have led to a growth in security threats. One of the measures used to fight against these security threats is Intrusion Detection.

The idea behind the technique of detecting intruders is that when an intruder gets into a third party system, he leaves traces behind or behaves differently compared to the normal user. This means that if methods or mechanisms can be found to carefully analyse the dataproduced, there is a greater chance of detecting a violation of the system policy and hence the intruders. Depending on how the data is collected and analysed we speak of **Host-based Intrusion Detection Systems (HIDS)**, where the software is installed on a single host or of **Network based Intrusion Detection System (NIDS)**, whereby the IDS Software monitors a network segment or a complete network. To detect attacks on information systems, basically two approaches can be distinguished:

HIDS
NIDS

[2] In the analog world, as the number of copies increases, the quality of these copies decreases.

[3] The number of Internet hosts increased from 4.852.000 in January 1995 to 394.991.609 in January 2006 (http://www.isc.org)

Anomaly Detection

- **Anomaly Detection** (Statistical Approaches, Bayesian Networks, Neural Networks, etc.) and

Misuse Detection

- **Misuse Detection** (Pattern Matching, State Transition Analysis, etc.).

In Anomaly Detection a profile of the variable to be analysed is made e.g. the use of resources (CPU usage) or typical user behaviour (login behaviour, execution order and frequency of programs, etc.), this is also called the long term profile and is compared with the actual realisation of the variable (short term profile). If the difference between long term and short term behaviour exceeds an a priori defined threshold, the event can then be seen as an anomaly [Den87].

A different approach is followed in Misuse Detection whereby attack specific signatures are stored in the signature database. The data stream is then systematically analysed by searching for these attack signatures in the data stream. If a match occurs, there is an intrusion.

In the first part of Chapter 12, the basic principles which are primordial for the understanding of intrusions are introduced. We then present a brief scenario on how intrusions are prepared and subsequently different types of intrusions (protocol related intrusions, remote access intrusions, Malicious code, etc.) are dealt with. In the second part we show why traditional security mechanisms such as Access Control Lists (ACLs) and Firewalls fail to solve the intrusion related problems we are facing today. In closing, we deal with Intrusion Detection, introduce concepts and investigate methods and where required, related techniques in greater detail.

1.14 Recommended literature for this course

There are many good reference books for communication techniques and cryptography. Here we mention some books which can be useful for further study.

For the general topic of communication techniques: [Kad91], [Kad95], [KDS+00], [Tan00] and [Spu00].

For the special topic on Internet protocols and services: [Los99], [Fei99], [Com00] and [KDS+00].

For a general understanding of cryptographic definitions, algorithms and protocols we recommend the following books and courses: [MOV96], [Sti95], [Sch96], [Buc99] and [KCL+00].

For the special topic on network and Internet security: [Smi97], [Fuh98], [FRU00], [Opp00], [DH99] and [Eck06].

References

[Buc99] Johannes Buchmann. *Einführung in die Kryptographie.* Springer Verlag, 1999.

[CB94] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison-Wesley, 1994.

[Com00] Douglas E. Comer. *The Internet Book.* Prentice Hall International, 2000.

[Den87] Dorothy E. Denning. IEEE Transactions on software engineering, Vol. Se-13, No. 2, FEBRUARY 1987, 222-232.

[DH76] W. Diffie and Martin E. Hellman. *New directions in cryptography.* IEEE Transactions on Information Theory, 22(6):644– 654, November 1976.

[DH99] Naganand Doraswamy and Dan Harkins. *IPSec.* Prentice Hall International, 1999.

[Eck06] Claudia Eckert. *IT-Sicherheit: Konzepte, Verfahren, Protokolle 4. überarbeitete und erweiterte Auflage.* R. Oldenbourg Verlag, 2006

[Fei99] Sidnie Feit. *TCP/IP - Architecture, Protocols and Implementation with IPv6 and IP security.* Mc Graw Hill, 1999.

[FRU00] Stephan Fischer, Christoph Rensing, and Rödig Utz. *Open Internet Security.* Springer Verlag, 2000.

[Fuh98] Kai Fuhrberg. *Internet-Sicherheit: Browser, Firewalls und Verschlsselung.* Hanser Verlag, 1998.

[Kad91] Firoz Kaderali. *Digitale Kommunikationstechnik (Band 1).* Vieweg Verlag, 1991.

[Kad95] Firoz Kaderali. *Digitale Kommunikationstechnik (Band 2).* Vieweg Verlag, 1995.

[Kad00] Firoz Kaderali. *Anonymität im Internet* Berichte aus der Kommunikationstechnik Band5, Shaker Verlag, Aachen, 2000.

[Kah67] David Kahn. *The Codeberakers.* Macmillan Publishing Company, New York, 1967.

[KCL+00] Firoz Kaderali, Biljana Cubaleska, Bernhard Löhlein, Sonja Schaup, and Oliver Stutzke. *Course - Foundations of Cryptology.* Department of Communication Systems, University of Hagen, 2000.

[KDS+00] Firoz Kaderali, Thomas Demuth, Dagmar Sommer, Gerd Steinkamp, and Michael Stepping. *Course 20018 - Internet Techniques.* Department of Communication Systems, University of Hagen, 2000.

[Los99] Pete Loshin. *TCP/IP clearly explained.* Morgan Kaufmann, 1999. 3rd Edition.

[MOV96] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[Opp00] Ralf Oppliger. *Security Technologies for the Internet.* Artech House Publishers, 2000.

[Sch96] Bruce Schneier. *Applied Cryptography: protocols, algorithms, and source code in C.* John Wiley and Sons, 1996.

[Sch97] C. L. Schuba. *On the Modeling, Design, and Implementation of Firewall Technology.* PhD thesis, Pudue University, December 1997.

[Sha49] Claude Shannon. *Communication theory of secrecy systems.* Bell System Technical Journal, 28:656–715, 1949.

[Smi97] Richard E. Smith. *Internet cryptography.* Addison Wesley Longman Inc., 1997.

[Spu00] Charles E. Spurgeon. *Ethernet: The Definitive Guide.* O'Reilly and Associates, 2000.

[Ste98] Lincoln D. Stein. *Web Security: A Step-by-Step Reference Guide.* Addison Wesley, 1998.

[Sti95] Douglas R. Stinson. *Cryptography: Theory and Practice.* CRC Press, 1995.

[Tan00] Andrew S. Tanenbaum. *Computernetzwerke.* Pearson Studium, 2000.