1 Introduction

It is now a well-known fact that, despite all the benefits, the digital revolution with its omnipresent networking of information systems also involves some risks. This book looks at a specific category of risks, the category of risks that evolve as a result of eavesdropping and the manipulation of data transmitted in communication networks and the vulnerability of the communication infrastructure itself. In particular, measures are discussed that can be taken to minimise them.

Protecting transmitted data

Mankind very early on recognised the need to protect information that was being transferred or stored, and so the desire to protect information from unauthorised access is probably as old as writing itself. For example, reliable early records on protective measures describe a technique used by the Spartans around 400 BC. The technique entailed writing messages on a leather strip that was wrapped around a stick of a specific diameter. Before the message was delivered, the leather strip was removed from the stick, and a potential attacker who did not have a stick with the same diameter, because he did not know the diameter or anything about the technique, could not read the message. In a sense this was an implementation of the first 'analogue' encryption.

First substitution ciphers

In the fourth century BC, the Greek Polybius developed a table of bilateral substitution that defined how to encode characters into pairs of symbols and their corresponding reinstatement, thereby specifying the first 'digital' encryption method. Of the Romans we know that they often protected their tactical communication by using simple monoalphabetic substitution methods. The most widely known one was probably the 'Caesar cipher', named after its creator Julius Caesar, in which each character of the alphabet

Security in Fixed and Wireless Networks, Second Edition.
Guenter Schaefer and Michael Rossberg.

Title of the German original: Netzsicherheit ISBN 978-3-86490-115-7

is shifted upwards by three characters. Thus, 'A' becomes 'D', 'B' becomes 'E', etc.

Origins of cryptanalysis

The Arabs were the first people to develop a basic understanding of the two fundamental principles of *substitution*, that is, pure character replacement, and *transposition*, that is, changing the sequence of the characters of a text. When they evaluated a method they also considered how a potential attacker might analyse it. They were therefore aware of the significance of relative letter frequency in a language for the analysis of substitution ciphers because it gave some insight into substitution rules. By the beginning of the fifteenth century, the Arabic encyclopaedia 'Subh al-a'sha' already contained an impressive treatment and analysis of cryptographic methods.

In Europe, cryptology originated during the Middle Ages in the papal and Italian city-states. The first encryption algorithms merely involved vowel substitution, and therefore offered at least some rudimentary protection from ignorant attackers who may not have come up with the idea of trying out all the different possible vowel substitutions.

Protection of infrastructure

Not wanting to turn the entire development of cryptology into a scientific discipline at this juncture, we can deduce from the developments mentioned that special importance has always been given to protecting information. However, a second category of risks is increasingly becoming a major priority in the age of omnipresent communication networks. These risks actually affect communication infrastructures rather than the data being transmitted. With the development and expansion of increasingly complex networks, and the growing importance of these networks not only to the economic but also to the social development of the modern information society, there is also a greater demand for ways to secure communication infrastructures from deliberate manipulation. For economic operation it is important to ensure that the services provided by communication networks are available and functioning properly as well as that the use of these services can be billed correctly and in a way that everyone can understand.

1.1 Content and Structure of this Book

In this book equal treatment is given to the two task areas in network security mentioned: *security of transmitted data* and *security of the communication infrastructure*. We start by introducing central terms and concepts and providing an overview of the measures available for information security.

Part 1 of the book deals with fundamental principles

Building on this introductory information, the rest of the chapters in Part 1 deal with the *fundamental principles of data security technology*. Chapter 2 uses basic concepts to introduce cryptology. Chapter 3 covers the use and functioning of *symmetric ciphering schemes*, whereas Chapter 4 is devoted to *asymmetric cryptographic algorithms*. Chapter 5 introduces *cryptographic check values* for the detection of message manipulation. Generating secure, non-predictable random numbers is the subject of Chapter 6. In a sense, the algorithms in these four chapters constitute the *basic primitives* of data security technology upon which the cryptographic protection mechanisms of network security are based. Chapter 7 discusses *cryptographic protocols* and introduces the authentication and key exchange protocols that are central to network security. Chapter 8 enlarges the topic in the context of scenarios with *group communication*. This deeper discussion may be skipped in an introductory course without impairing the understanding of further book chapters. Part 1 concludes with Chapter 9, which provides an introduction to the principles of access control.

Part 2 introduces architectures and protocols for network security

Part 2 of this book focuses on the architectures and protocols of *network security*. It starts with Chapter 10, which examines general issues relating to the integration of security services in communication architectures. Chapter 11 discusses security protocols of the data link layer, Chapter 12 examines the security architecture for the Internet protocol *IPsec* and Chapter 13 closes Part 2 by describing security protocols for the transport layer.

Part 3 is devoted to wireless and mobile communication

Part 3 of the book presents the field of *secure wireless and mobile communication*. Chapter 14 differentiates the additional security aspects that arise in mobile communications compared with conventional fixed networks, and presents approaches of a more conceptual nature for maintaining the confidentiality of the current location area of mobile devices. The other chapters in this part examine concrete examples of systems. Chapter 15 deals with the security functions of the IEEE 802.11 standard for wireless local networks and includes an in-depth discussion of the weaknesses of former versions of the standard. Chapter 16 introduces the security functions for the current standards for mobile wide-area networks, that is, *GSM*, *UMTS* and *LTE*.

Part 4 deals with protection of communication infrastructures.

While Parts 1 to 3 of the book mainly concentrate on the security of communication processes between end systems, the fourth and last part of the book deals with *protection of large networks and the communication infrastructure*. Chapter 17 first describes the basic problem of protecting systems in open networks and provides a short overview of systematic threat analysis. It also discusses

the problem of protecting end systems as a requirement for secure network operation. Chapter 18 deals with *denial-of-service attacks*, which affect end systems as well as the communication infrastructure. Chapters 19 and 20 cover the security of fundamental communication infrastructure services: *routing* and *name resolution*. *Internet firewalls* as the main means for realising subnet-related access control are introduced in Chapter 21. Since attacks cannot always be prevented through the proactive security measures described in these chapters, it often makes sense to introduce additional control through *intrusion detection systems* and/or *intrusion prevention systems*. The principles of such systems and existing techniques are introduced in Chapter 22. Finally, Chapter 23 deals with difficulties in the management of large security infrastructures.

The field of network security is currently marked by a major dynamic

Before our attentive and inquisitive readers get too involved in the further content of this book, they should be made aware that the field of network security has developed into a very active field during the last few years. Consequently, extensive improvements are constantly being made to existing security protocols and new protocols are being developed and introduced. Doing justice to the speed of this development in a textbook thus becomes a very difficult if not impossible undertaking. We therefore ask for the reader's understanding if a detail or two has already been resolved in a way that deviates from our interpretation in a particular chapter or totally new protocols have established themselves in the meantime and are not dealt with in this book. It is precisely because of the rapid developments in this field that the priority of this book is to provide the reader with a fundamental understanding of the central principles presented and to describe them on the basis of concrete and relevant sample protocols.

1.2 Threats and Security Goals

The terms *threat* and *security goal* play an important role in assessing the risks in communication networks, therefore they will first be defined in general terms.

Definition 1.1 *A* **threat** *in a communication network is a potential event or series of events that could result in the violation of one or more security goals. The actual implementation of a threat is called an* **attack**.

Examples of concrete threats

Definition 1.1 is kept quite abstract and refers to the term *security goal* defined below. The following examples clarify the types of threats that exist:

- a hacker intruding into the computer of a company;
- someone reading someone else's transmitted e-mails;
- a person altering sensitive data in a financial accounting system;
- a hacker temporarily shutting down a web site;
- somebody using or ordering services and goods in someone else's name.

Examples of security goals

The term *security goal* is another concept that is easier to explain with examples because at first glance security goals can vary considerably depending on the respective application scenario:

- Banks:
  - protection from deliberate or unintentional modification of transactions;
  - reliable and non-manipulable identification of customers;
  - protection of personal identification numbers from disclosure;
  - protection of personal customer information.
- Administration:
  - protection from disclosure of sensitive information;
  - use of electronic signatures for administrative documents.
- Public network operators:
  - restriction of access to network management functions to authorised personnel only;
  - protection of the availability of the services offered;
  - guarantee of accurate and manipulation-safe billing of use of services;
  - protection of personal customer data.
- Corporate and private networks:
  - protection of the confidentiality of exchanged data;
  - assurance of the authenticity of messages (details follow).
- All networks: Protection from intrusion from outside.

General definition of security goals

Some of the security goals listed above are of course relevant to several different application scenarios — even if they are not

repeated in the categories above. However, security goals can also be defined from a purely technical standpoint without being based on a concrete application scenario.

Definition 1.2 *In the field of network security, a distinction can be made between the following* **technical security goals***:*

- **Confidentiality:** *Transmitted or stored data and/or details about the communication itself, e.g. the identity of sender or receiver, should only be disclosed to authorised entities.*
- **Data integrity:** *It should be possible to detect unintentional or deliberate changes to data. This requires that the identification of the originator of the data is unique and cannot be manipulated.*
- **Accountability:** *It must be possible to identify the entity responsible for a particular event, e.g. use of a service.*
- **Availability:** *The services implemented in a system should be available and function properly.*
- **Controlled access:** *Only authorised entities should be able to access certain services and data.*

Not all security experts and standards see the last goal to be full-fledged, but rather already covered by the first two goals. However, for communication networks it is often reasonable to restrict access to the network, even though there is no direct threat by any unauthorised access for that network itself.

General technical threats

Like security goals, threats can be viewed from a primarily technical standpoint and therefore *technical threats* are distinguished as follows:

- *Masquerade:* An entity pretends to have the identity of another entity.
- *Eavesdropping:* An entity reads information that is meant for someone else.
- *Authorisation violation:* An entity uses services or resources although it does not have appropriate permission.
- *Loss or modification of information:* Certain information is destroyed or changed.
- *Forgery:* An entity creates new information using the identity of another entity.
- *Repudiation:* An entity falsely denies having participated in a particular action.
- *Sabotage:* Any action that is aimed at reducing the availability or correct functioning of services or systems. In the context of computer networks these attacks are usually referred to by the term *denial-of-service (DoS)*.

	Technical threats						
Technical security goals	Masquerade	Eavesdropping	Authorisation violation	Loss or modification of information	Forgery of information	Repudiation of events	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data integrity	x		x	x	x		
Accountability	x		x	x		x	
Availability	x		x	x			x
Controlled access	x		x		x		

Table 1.1
Technical security goals and threats

These terms can be used as the basis for creating a general classification that clarifies which security goals are in danger of being exposed to which threats. Table 1.1 provides an overview of this classification. The table can be read in two different ways. On one hand, it shows that information confidentiality is threatened by the technical threats of masquerade, eavesdropping and authorisation violation; on the other hand, it can also be directly inferred from the table that forgery primarily threatens the security goals of data integrity, accountability and controlled access.

Real attacks often combine several threats

In reality, a concrete attack often involves a combination of the threats mentioned above. An intrusion into a system often involves sniffing the access identification and related passwords. The identity of the sniffed identification is then provided for the access check with the latter representing a masquerade. Thus, Table 1.1 serves more the purpose of illustration than a definition of the abilities or possibilities of the different attacker types.

1.3 Network Security Analysis

When appropriate action is taken to counteract the above-mentioned threats to an actual application scenario, the countermeasures being considered first have to be evaluated carefully for the given network configuration. This requires a detailed *security analysis* of the network technology with an assessment of the risk potential of technical threats to the entities communicating in the network, along with an evaluation of the cost in terms of resources and time, that is, computing capacity, storage, message transfer, of executing known attack techniques.

Note: Unknown attack techniques are generally not possible to evaluate!

Sometimes the detailed security analysis of a given network configuration or a specific protocol architecture will be needed to convince an organisation's financial controlling of the need for

further security measures. Additionally, since the attack techniques as well as the network configuration are normally subjects of constant change, a security analysis and the respective derivation of risks needs to be constantly re-evaluated. In larger organisations it is advantageous to install a security management according to ISO 27001 [ISO13]. This includes, for example, the introduction of dedicated staff for IT security.

In any case, a key issue for security analyses is the question: 'How can the complexity of the overall system be effectively reduced?' Some fundamental techniques will be covered in Chapter 17 in more depth, but as a rule a detailed security analysis of a specific protocol architecture may be structured according to the following finely granulated *attacks at the message level*:

- Passive attacks: Eavesdropping on protocol data units (PDUs);
- Active attacks: Delay, replay, deletion and insertion of PDUs.

Combination of attacks

For any security analysis, one basic assumption needs to be that an actual hacker would have to be able to combine the attacks listed above in order to use them to construct more complex attacks from these basic building blocks interpreted as attack primitives. A 'successful attack' at the message level therefore requires that:

- the attack produces no directly detectable side effects for other communication processes, e.g. for other connections or connectionless data transmission;
- the attack produces few side effects for other PDUs in the same connection or in connectionless data transmission between the entities participating in the communication.

Otherwise, there is the inherent risk of attack detection and therefore the attacker may not be able to combine the building blocks to a more complex attack.

When a security analysis is produced for protocol architectures, each individual layer in the architecture should be checked for the attacks mentioned above.

Figure 1.1 shows the layered architecture typically used in communication systems today. In this architecture the end systems communicate with one another over a network of intermediate systems. The protocol functions are organised into five layers:

- The lowest layer is the *physical layer*, which is responsible for transmitting bit streams over a physical medium, e.g. line or radio transmission link.

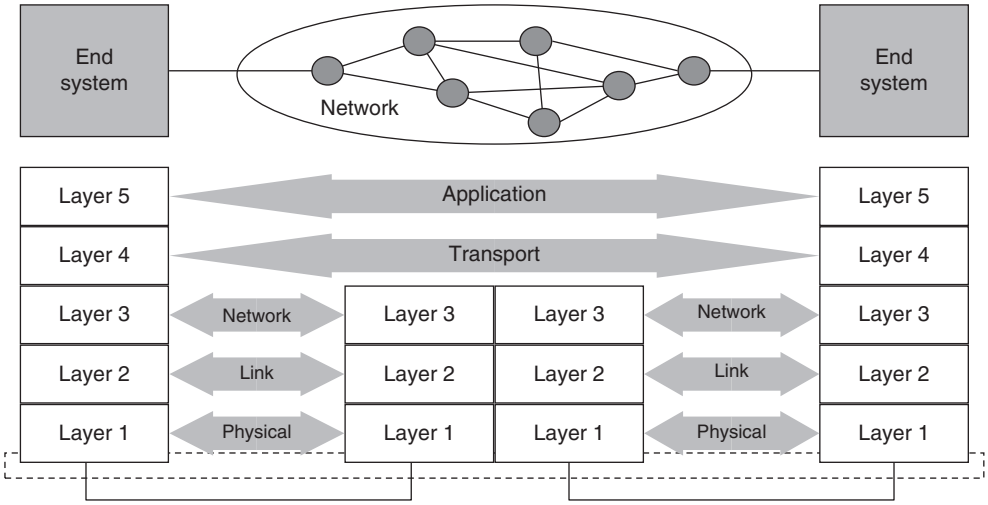

Figure 1.1
Architecture of layered communication systems

- The *data link layer* above it combines multiple bits from the transmitted bit stream into transmission frames and carries out transmission that is protected against errors between two systems connected over a physical medium. It performs two basic tasks. When a shared medium is available to several systems, it coordinates access to the shared medium *(medium access control, MAC)*. It also takes appropriate measures to detect transmission errors so that defective frames received at the receiver are detected and can be discarded.
- The *network layer* is responsible for the communication between end systems that are normally linked to one another over several intermediate systems. The main task of this layer therefore is routing and forwarding through the transmission network between the two end systems.
- The *transport layer* enables an exchange of data between the processes of the end systems. The key tasks of this layer are addressing applications processes, detecting errors at the end-to-end level and, with a reliable service, implementing measures for error recovery, e.g. through retransmission.
- Above the transport layer the *application layer* – as its name suggests – implements applications-specific protocols that are as diverse as the applications run in the end systems.

Only the three lower layers up to the network layer are normally implemented in the (intermediate) systems of the transmission network.

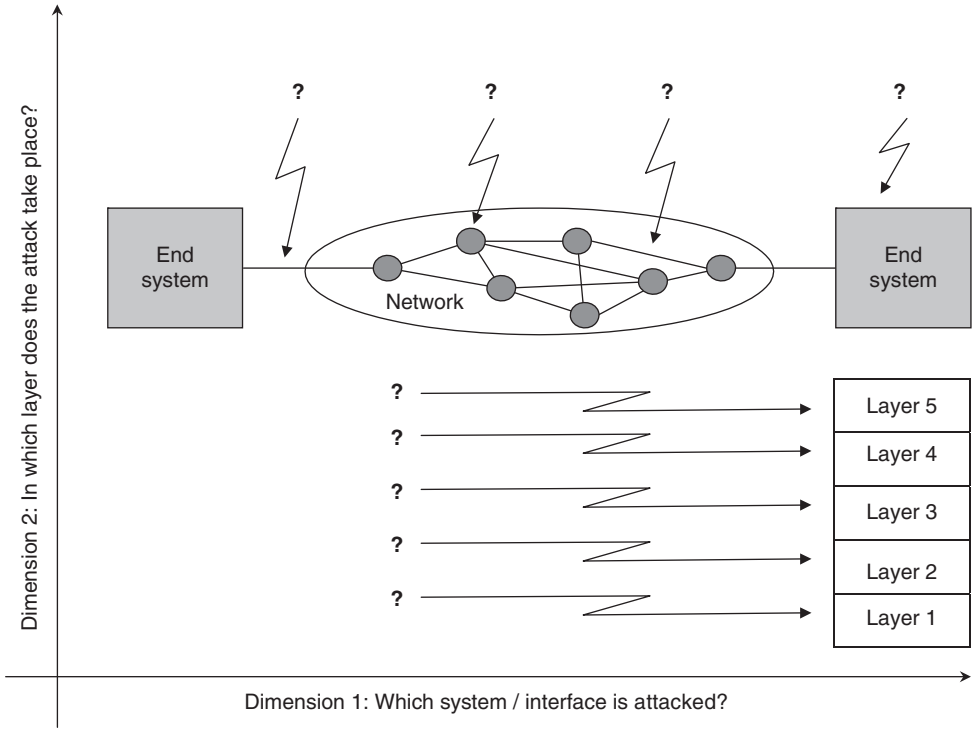

Figure 1.2 *Dimensions of the security analysis of layered protocol architectures*

According to the description given above, a security analysis of layered protocol architectures can be structured along two dimensions (also compare Figure 1.2):

- First the *systems and interfaces at risk* in the network configuration being analysed must be identified. For example, publicly accessible end systems, gateways to public networks as well as non-secure transmission routes (particularly in the case of wireless transmission) pose special security risks.
- The security analysis is also structured according to the *layer* in which an attack can take place. Attacks do not necessarily have to occur in the application layer. On the contrary, depending on the intentions of the hacker, the main attack point can be the layers below the transport layer.

A detailed security analysis is very useful for identifying the security risks that dominate in a particular network configuration. It can be used as the basis for selecting appropriate security measures to reduce these risks. The following section provides a general overview on this subject.

1.4 Information Security Measures

Many different security measures are available, each dealing with specific aspects of an information processing system and its embedding into the work processes supported by the system:

- *Physical security measures* include lock systems and physical access controls, tamper proofing of security-sensitive equipment and environmental controls such as motion detectors, etc.
- *Personnel security measures* begin with a classification of the security-specific sensitivity of a position and also include procedures for employee screening and security training and awareness.
- *Administrative security measures* include procedures for the controlled import of new software and hardware, detection of security-relevant occurrences through maintenance and regular checks of event logs as well as an analysis of known security breaches and incidents.
- *Media security measures* are aimed at safeguarding the storage of information. Procedures and control mechanisms are implemented to identify, reproduce or destroy sensitive information and data carriers.
- *Radiation security measures* are designed to prevent or limit electromagnetic emission from computer systems and peripheral devices (especially monitors) that a hacker could note and use to eavesdrop on information.
- *Life-cycle controls* monitor the design, implementation and introduction of information processing systems. The specification and control of standards to be upheld for programming and documentation are geared towards achieving a 'reliable' development process.
- *System security measures* for computers, operating systems and the applications run on computers are designed to secure information that is stored and processed in computing systems.
- Expanding on the latter category, *communication security measures* are designed to protect information while it is being transmitted in a communication network. In conjunction with the measures that protect the network infrastructure itself, they form the category of *network security measures*.

A secure information processing process requires a comprehensive catalogue of measures

The last category mentioned, network security, is the main subject of this book. However, it should be emphasised that a careful application of the entire catalogue of measures listed above is necessary to guarantee the security of information processing processes. This is due to the fact that a security system is only as secure as its weakest component. For example, a sophisticated password system that prevents the use of easily guessed passwords is minimally effective if users write their passwords on media that are not adequately protected or if a hacker can use a telephone call to induce someone to divulge a password ('social engineering').

1.5 Important Terms Relating to Communication Security

This section introduces the terms *security service, cryptographic algorithm* and *cryptographic protocol*, which are central to network security, and explains their relationship to one another.

Definition 1.3 *A* **security service** *is an abstract service that seeks to achieve a specific security objective.*

Implementation of security services

A security service can be implemented through either cryptographic or conventional means. For example, one way to prevent a file stored on a USB stick from being read by an unauthorised entity is to ensure that the file is encrypted before it is stored. On the other hand, the same goal can be achieved if the stick is locked up in a secure safe. Normally, the most effective approach is a combination of cryptographic and conventional methods.

Fundamental security services

In its generalisation, Definition 1.3 gives the impression that a multitude of different security services exist. Actually the number is surprisingly small; precisely five fundamental security services are distinguished:

- As subsequent discussions in this book will show, *authentication* is the most important of all security services because it allows manipulation-safe identification of entities.
- To a certain extent the security service *data integrity*, which ensures that data generated by a specific entity cannot undetectably be modified, is the 'little brother' of the authentication service.
- *Confidentiality*, which is aimed at preventing information from being made known to unauthorised entities, is probably the most widely known security service.

- The security service *access control* checks that only entities that have proper authorisation can access certain information and services in a specified way.
- The aim of the *non-repudiation* service is to enable the unique identification of the initiators of certain actions, such as the sending of a message, so that these completed actions cannot be disputed after the fact. In contrast to the authentication service this evidence can be provided to third parties.

Definition 1.4 *A* **cryptographic algorithm** *is a mathematical transformation of input data (e.g. data, keys) to output data.*

Cryptographic algorithms play an important role in the realisation of security services. However, a cryptographic algorithm used on its own is not sufficient because it also has to be embedded in a semantic context. This usually occurs as part of the definition of a *cryptographic protocol*.

Definition 1.5 *A* **cryptographic protocol** *is a procedural instruction for a series of processing steps and message exchanges between multiple entities. The aim is to achieve a specific security objective.*

The last two terms defined for cryptographic algorithms and protocols are of such fundamental significance for network security that they are dealt with in several chapters. However, the next chapter will first introduce the general basics of cryptology.