

Security in Networks

Arno Wacker
Distributed Systems
University Duisburg-Essen

Contact Info

- Arno Wacker
- Department Distributed Systems
- Head: Prof. Dr.-Ing. Torben Weis

- Mail: arno.wacker@uni-due.de
- Room 913, Building BB, 9th floor*
- Tel.: +49-203-379-4474*
- Office Hours
 - Directly after lecture, or make an appointment via email

- Exercises: Kerstin Luck (kerstin.luck@uni-due.de)
 - Schedule: directly after the lecture

*will change during May/June

Overview 1 / 2

- Encryption/Decryption Algorithms
 - Classical Cryptography
 - Symmetric cryptographic algorithms (AES, DES, 3DES)
 - Asymmetric cryptographic algorithms (RSA)
 - Key Exchange Protocols (Diffie–Hellman)
- Hash functions and Signatures
 - Cryptographical hash functions
 - Modification Detection Codes (MDC)
 - Message Authentication Codes (MAC)
 - Digital signatures
 - Random numbers

Overview 2 / 2

- Access Control
 - Usage of passwords
 - Access–Control mechanisms
- Specific protocols and technologies
 - Cryptographical protocols
 - Kerberos
 - IPsec
 - SSL
 - Firewalls

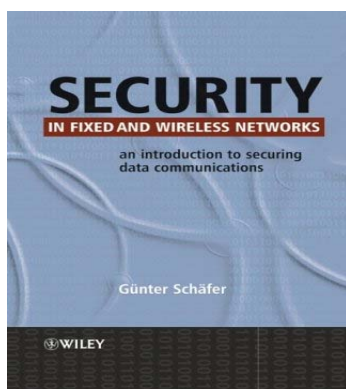
Recommended Books



Günter Schäfer
Netz-sicherheit
dpunkt.verlag

- The lecture closely follows this book
- The book is available in
 - English
 - German
- Price tag
 - German version: EUR 44
 - English version: > EUR 44
- More resources
<http://www.guenterschaefer.de/Netz-sicherheit>

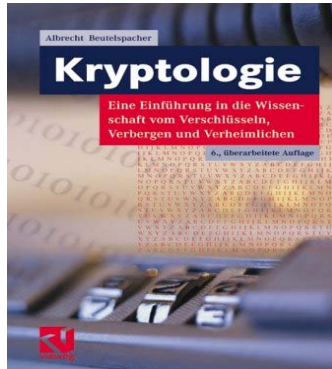
Recommended Books



Günter Schäfer
Security in Fixed and Wireless Networks
Wiley

- The lecture closely follows this book
- The book is available in
 - English
 - German
- Price tag
 - German version: EUR 44
 - English version: > EUR 44
- More resources
<http://www.guenterschaefer.de/Netz-sicherheit>

Recommended Books (2)



Albrecht Beutelspacher
Kryptologie
Vieweg Verlag



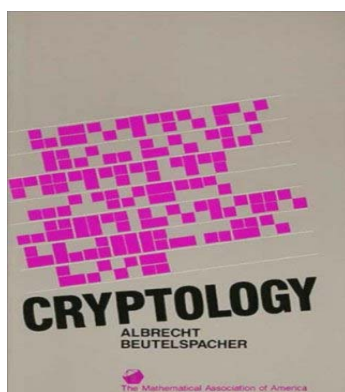
Distributed Systems
University Duisburg-Essen

Arno Wacker

7

- Good introduction to cryptography
- Easy to understand and very entertaining
- Not very detailed, no strict scientific book
- The book is available in
 - English
 - German
- Price tag
 - German version: EUR 20,90
 - English version: \$ 40

Recommended Books (2)



Albrecht Beutelspacher
Cryptology
ISBN: 0883855046



Distributed Systems
University Duisburg-Essen

Arno Wacker

8

- Good introduction to cryptography
- Easy to understand and very entertaining
- Not very detailed, no strict scientific book
- The book is available in
 - English
 - German
- Price tag
 - German version: EUR 20,90
 - English version: \$ 40

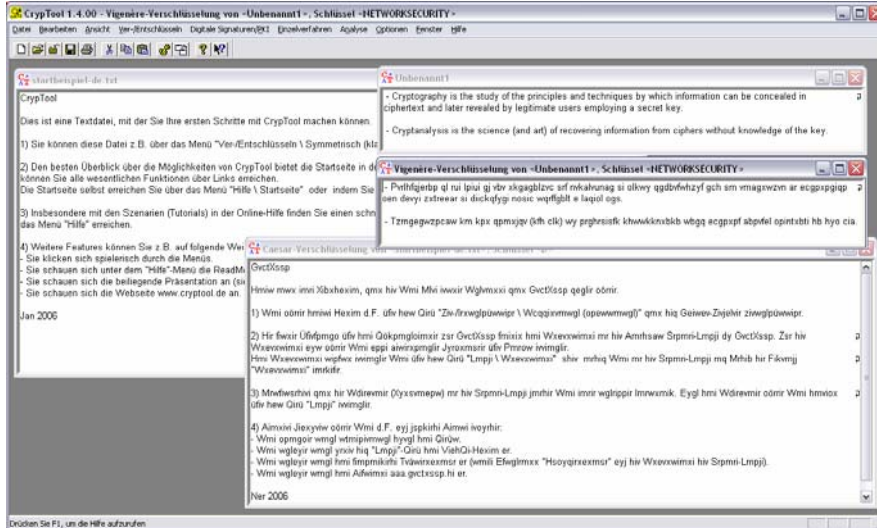
Exam

- Written Exam
 - Duration: 90 Minutes
 - Form: Multiple Choice
 - Date: Determined by “Prüfungsamt”
- International Studies of Engineering (ISE)
 - Computer Engineering (CE)
 - Computer Science and Communication Engineering (CSCE)

Helper Tool: CrypTool

- Demonstrating/learning cryptography
- Freeware (available in English and German)
 - Developed by Universität Darmstadt and Siegen
 - Sponsored by Deutsche Bank
- Supports classical + modern cryptography
- Can be used to verify most presented examples
- Get it at <http://www.cryptool.de>

CrypTool: Example Caesar Cipher/Vigenere



Distributed Systems
University Duisburg-Essen

Arno Wacker

11

Network Security Chapter 1 Introduction

Arno Wacker
University Duisburg-Essen

Overview

- Threats in Communication Networks
- Security Goals & Requirements
- Network Security Analysis
- Safeguards
- Historic Remarks

Threats in Communication Networks

- Abstract Definition
 - A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*
 - The actual realization of a threat is called an *attack*
- Examples
 - A hacker breaking into a corporate computer
 - Disclosure of emails in transit
 - Someone changing financial accounting data
 - A hacker temporarily shutting down a website
 - Someone using services or ordering goods in the name of others

Thread != Threat

- Attention non-native English speakers 😊
- Security
 - A threat is a possible menace for your system
- Operating Systems
 - A thread is a flow of control

Overview

- Threats in Communication Networks
- **Security Goals & Requirements**
- Network Security Analysis
- Safeguards
- Historic Remarks

Security Goals

- Two ways of speaking about security goals
 - Application-specific
 - That is what managers talk about
 - Technical Specification
 - That is what engineers talk about

Application-specific Security Goals (1)

- Banking:
 - Protect against fraudulent or accidental modification of transactions
 - Identify customers
 - Protect PINs from disclosure
 - Ensure customers privacy
- Electronic trading:
 - Assure source and integrity of transactions
 - Protect corporate privacy
 - Provide legally binding electronic signatures on transactions

Application-specific Security Goals (2)

- **Government:**
 - Protect against disclosure of sensitive information
 - Provide electronic signatures on government documents
- **Public Telecommunication Providers:**
 - Restrict access to administrative functions to authorized personnel
 - Protect against service interruptions
 - Protect subscribers privacy

Application-specific Security Goals (3)

- **Corporate / Private Networks:**
 - Protect corporate / individual privacy
 - Ensure message authenticity
- **All Networks:**
 - Prevent outside penetrations (who wants hackers?)
- **Other terminus technicus ...**
 - ... but same meaning
 - Security objectives

Security Goals Technically Defined (1)

- Confidentiality
 - Data transmitted or stored should only be revealed to an intended audience
 - Confidentiality of entities is also referred to as anonymity
- Data Integrity
 - It should be possible to detect any modification of data
 - This requires to be able to identify the creator of some data

Security Goals Technically Defined (2)

- Accountability
 - It should be possible to identify the entity responsible for any communication event
- Availability
 - Services should be available and function correctly
 - Safety & Liveness
- Controlled Access
 - Only authorized entities should be able to access certain services or information

Threats Technically Defined (1)

- **Masquerade**
 - An entity claims to be another entity
- **Eavesdropping**
 - An entity reads information it is not intended to read
- **Authorization Violation**
 - An entity uses a service or resources it is not intended to use
- **Loss or Modification of (transmitted) Information**
 - Data is being altered or destroyed

Threats Technically Defined (2)

- **Denial of Communication Acts (Repudiation)**
 - An entity falsely denies its' participation in a communication act
 - Important for E-Commerce, E-Banking, E-Government
- **Forgery of Information**
 - An entity creates new information in the name of another entity
- **Sabotage**
 - Any action that aims to reduce the availability and / or correct functioning of services or systems

Threats and Technical Security Goals

Technical Security Goals	General Threats						
	Masquerade	Eavesdropping	Authorisation Violation	Loss or Modification of (transmitted) information	Denial of Communication acts	Forgery of Information	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	

These threats are often combined in order to perform an attack!

Overview

- Threats in Communication Networks
- Security Goals & Requirements
- **Network Security Analysis**
- Safeguards
- Historic Remarks

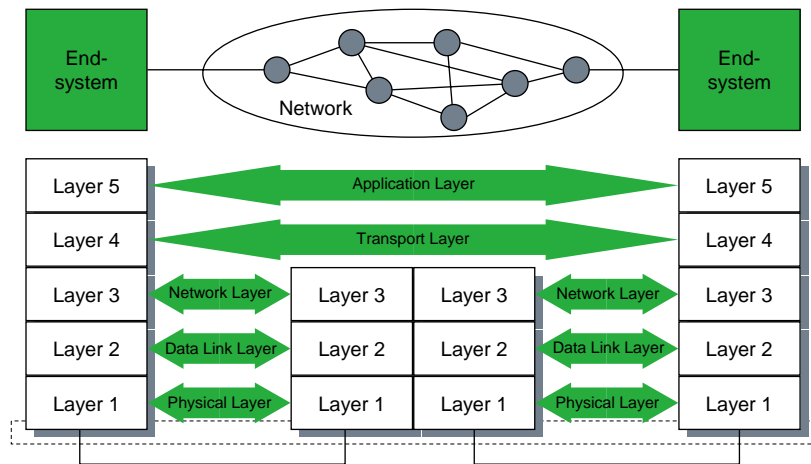
Network Security Analysis

- Countering a threat means analyzing the threat
- Attention: It is generally impossible to assess unknown threats or attacks!
- Detailed network security analysis required
 - Evaluate the risk potential of a threat to the entities using a network
 - Estimate the expenditure (resources, time, etc.) needed to perform known attacks
- Economic aspects
 - Security analysis might be required to convince business partners and investors

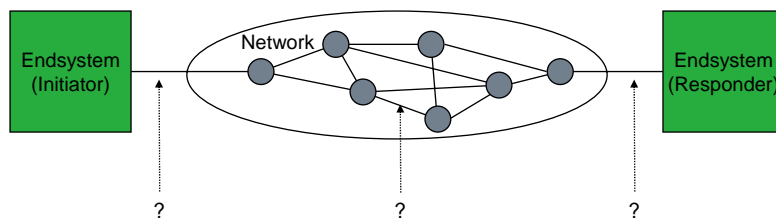
Attacks on the Message Level

- Passive attacks
 - Eavesdropping
- Active attacks
 - Delay of PDUs (Protocol Data Units)
 - Replay of PDUs
 - Deletion of PDUs
 - Modification of PDUs
 - Insertion of PDUs
- Successful attacks require a combination of the above primitives
- A security analysis of a layered architecture (OSI Model) requires checking every layer

Communication in Layered Protocol Architectures

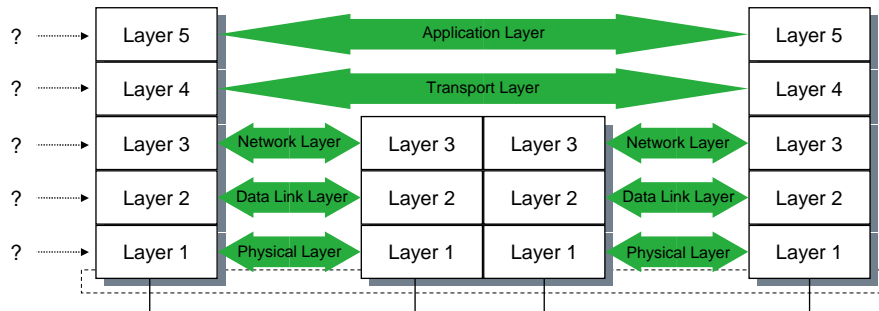


Security Analysis of Layered Protocol Architectures (1)



Dimension 1: At which interface does the attack take place?

Security Analysis of Layered Protocol Architectures (2)



Dimension 2: In which layer does the attack take place?

Overview

- Threats in Communication Networks
- Security Goals & Requirements
- Network Security Analysis
- Safeguards
- Historic Remarks

Safeguards Against Information Security Threats (1)

- Physical Security:
 - Locks or other physical access control
 - Tamper-proofing of sensitive equipment
 - Environmental controls
- Personnel Security:
 - Identification of position sensitivity
 - Employee screening processes
 - Security training and awareness

Safeguards Against Information Security Threats (2)

- Administrative Security
 - Controlling import of foreign software
 - Procedures for investigating security breaches
 - Audit relevant events
 - Reviewing accountability controls
- Emanations Security
 - Radio Frequency and other electromagnetic emanations controls
 - Referred to as TEMPEST protection

Safeguards Against Information Security Threats (4)

- Computer Security
 - Protection of information while stored / processed in a computer system
 - Protection of the computing device itself
- Communications Security
 - (The main subject of this course)
 - Protection of information during transport from one system to another
 - Protection of the communication infrastructure itself

Communication Security Terminology (1)

- Security Service
 - An abstract service that seeks to ensure a specific security property
- A security service can be realised with:
 - cryptographic algorithms and protocols
 - conventional means
 - One can keep an electronic document on a floppy disk confidential by storing it on the disk in an encrypted format as well as locking away the disk in a safe
 - Usually a combination of cryptographic and other means is most effective

Communication Security Terminology (2)

- **Cryptographic Algorithm:**
 - A mathematical transformation of input data (e.g. data, key) to output data
 - Cryptographic algorithms are used in cryptographic protocols
- **Cryptographic Protocol:**
 - A series of steps and message exchanges between multiple entities in order to achieve a specific security objective

Security Services – Overview (1)

- **Authentication**
 - The most fundamental security service which ensures that an entity has in fact the identity it claims to have
- **Integrity**
 - In some kind, the “small brother” of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- **Confidentiality**
 - The most popular security service, ensuring the secrecy of protected data

Security Services – Overview (2)

- Access Control
 - Controls that each identity accesses only those services and information it is entitled to
- Non Repudiation
 - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred

Security Mechanisms (1)

- Key management
 - All aspects of the lifecycle of cryptographic keys
- Random number generation
 - Generation of cryptographically secure random numbers
- Event detection / security audit trail
 - Detection and recording of events that might be used in order to detect attacks or conditions that might be exploited by attacks
- Intrusion detection
 - Analysis of recorded security data in order to detect successful intrusions or attacks
- Notarization
 - Registration of data by a trusted third party that can confirm certain properties (content, creator, creation time) of the data later on

Security Mechanisms (2)

- Communication specific mechanisms
 - Traffic Padding
 - Creation of bogus traffic in order to prevent traffic flow analysis
 - Routing Control
 - Influencing the routing of PDUs in a network

Cryptology

- Science concerned with communications in secure and usually secret form
- The term is derived from the Greek *kryptós* (hidden) and *lógos* (word)
- Cryptology encompasses:
 - Cryptography (*gráphein* = to write): the study of the principles and techniques by which information can be concealed in ciphertext and later revealed by legitimate users employing a secret key
 - Cryptanalysis (*analýein* = to loosen, to untie): the science (and art) of recovering information from ciphers without knowledge of the key

Cipher

- Method of transforming a message (plaintext) to conceal its meaning
- Also used as synonym for the concealed ciphertext
- Ciphers are one class of cryptographic algorithms
- The transformation usually takes the message and a (secret) key as input

Cryptology – Some Historic Remarks (1)

- 400 BC
 - The Spartans employ a cipher device called *scytale* for communications between military commanders
 - Relied on batons with secret radius
 - We will come back to the scytale in chapter 2
- During 4. century BC
 - Aeneas Tacticus (Greek) writes *“On the defense of fortifications”*, with one chapter devoted to cryptography
 - Polybius (Greek) invents means of encoding letters into pairs of symbols by a device called the *Polybius Checkerboard*
 - Identifies a letter by its position in a table

Cryptology – Some Historic Remarks (2)

- The Romans used monoalphabetic substitution with simple cyclic displacement of the alphabet
 - Julius Caesar employed a shift of three letters (A giving D, ..., Z giving C)
 - Augustus Caesar employed a single shift (A giving B, ...)

Cryptology – Some Historic Remarks (3)

- The Arabs were the first people to understand the principles of cryptography and to discover the beginnings of cryptanalysis:
 - Design and use of substitution and transposition ciphers
 - Discovery of the use of letter frequency distributions and probable plaintext in cryptanalysis
 - By 1412 AD Al-Kalka-Shandi includes an elementary and respectable treatment of several cryptographic systems and their cryptanalysis in his encyclopaedia Subh al-a'sha
- European Cryptography:
 - Development started in the Papal States and the Italian city-states in the middle age
 - First ciphers used only vowel substitution

Cryptology – Some Historic Remarks (4)

- European Cryptography: (cont.)
 - 1397: *Gabriele de Lavinde* of Parma writes first European manual on cryptography, containing a compilation of ciphers as well as a set of keys for 24 correspondents and embracing symbols for letters, numbers and several two-character code equivalents for words and names
 - Code vocabularies, called *Nomenclators* became the mainstay for several centuries for diplomatic communications of most European governments
 - 1470: *Leon Battista Alberti* publishes *Trattati In Cifra*, which describes the first cipher disk and already prescribes to regularly reset the disk, conceiving the notion of polyalphabeticity

Cryptology – Some Historic Remarks (5)

- European Cryptography: (cont.)
 - 1563: *Giambattista della Porta* provides a modified form of a square table and the earliest example of a digraphic cipher (2-letter-substitution)
 - 1586: *Blaise de Vigenère* publishes *Traicté des chiffres* containing the square table commonly tributed to him
 - By 1860 large codes were used for diplomatic communications and ciphers were only used in military communications (except high command level) because of the difficulty of protecting codebooks in the field

Cryptology – Some Historic Remarks (6)

- Developments during World Wars 1 and 2:
 - 1920: The maturing of electromechanical technology brings about a true revolution in cryptodevices
 - the development of *rotor cipher machines*:
 - The rotor principle is discovered independently by *E. E. Hebern* (USA), *H. A. Koch* (Netherlands) and *A. Scherbius* (Germany)
 - Rotor cipher machines cascade a collection of cipher disks to realize polyalphabetic substitution of high complexity
 - Cryptanalysis of tactical communications plays a very important role during World War 2 with the greatest triumphs being the British and Polish solution of the German *Enigma*

Cryptology – Some Historic Remarks (7)

- Developments after World War 2:
 - Modern electronics allow even more complex ciphers, initially following the rotor principles (and including their weaknesses)
 - Most information about electronic cipher machines used by various national cryptologic services is not publicly available
 - By the end of the 1960's commercially available cryptography was poorly understood and strong cryptography was reserved for national agencies
 - 1973–1977: Development of the Data Encryption Standard (DES)

Cryptology – Some Historic Remarks (8)

- 1976–1978: Discovery of Public Key Cryptography
 - 1976: W. Diffie and M. Hellman publish “New Directions in Cryptography” introducing the concepts of public key cryptography and describing a scheme of exchanging keys over insecure channels
 - R. Merkle independently discovers the public key principle, but his first publications appear 1978, due to a slow publishing process
 - 1978: R. L. Rivest, A. Shamir and A. M. Adleman publish “A Method for Obtaining Digital Signatures and Public Key Cryptosystems”, containing the first working and secure public key algorithm RSA

Appendix

Bibliography

- [Amo94] E. G. Amorosi. Fundamentals of Computer Security Technology. Prentice Hall, 1994.
- [Cha95] Brent Chapman and Elizabeth Zwicky. Building Internet Firewalls. O'Reilly, 1995.
- [For94b] Warwick Ford. Computer Communications Security – Principles, Standard Protocols and Techniques. Prentice Hall, 1994.
- [Gar96] Simson Garfinkel and Gene Spafford. Practical Internet & Unix Security. O'Reilly, 1996.
- [Men97a] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. CRC Press Series on Discrete Mathematics and Its Applications, Hardcover, 816 pages, CRC Press, 1997.
- [Sch03] G. Schäfer. Netzsicherheit – Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 435 Seiten Broschur, 44.– Euro, 2003.
- [Sch96] B. Schneier. Applied Cryptography Second Edition: Protocols, Algorithms and Source Code in C. John Wiley & Sons, 1996.
- [Sta98a] W. Stallings. Cryptography and Network Security: Principles and Practice. Hardcover, 569 pages, Prentice Hall, 2nd ed, 1998.
- [Sti95a] D. R. Stinson. Cryptography: Theory and Practice (Discrete Mathematics and Its Applications). Hardcover, 448 pages, CRC Press, 1995.