Chapter 1
Introduction

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

What is a Threat in a Communication Network?

- 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 for threats:
  - 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
  - ...
- What are security goals?
  - Security goals can be defined:
    - depending on the application environment, or
    - in a more general, technical way

Security goals depending on the application environment

- Banking:
  - Protect against fraudulent or accidental modification of transactions
  - Identify retail transaction customers
  - Protect PINs from disclosure
  - Ensure customers privacy
- Electronic trading:
  - Assure integrity of transactions
  - Protect corporate privacy
  - Provide legally binding electronic signatures on transactions
- Government:
  - Protect against disclosure of sensitive information
  - Provide electronic signatures on government documents

Security goals depending on the application environment

- Public Telecommunication Providers:
  - Restrict access to administrative functions to authorized personnel
  - Protect against service interruptions
  - Protect subscribers privacy
- Corporate / Private Networks:
  - Protect corporate / individual privacy
  - Ensure message authenticity
- All Networks:
  - Prevent outside penetrations (who wants hackers?)

- Sometimes security goals are also called *security objectives*

Security Goals Technically Defined

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

Threats Technically Defined

- *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
- *Denial of Communication Acts (Repudiation):*
  - An entity falsely denies its' participation in a communication act
- *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!

Network Security Analysis

- In order to take appropriate countermeasures against threats, these have to be evaluated appropriately for a given network configuration.
- Therefore, a detailed *network security analysis* is needed that:
  - evaluates the risk potential of the general threats to the entities using a network, and
  - estimates the expenditure (resources, time, etc.) needed to perform known attacks.

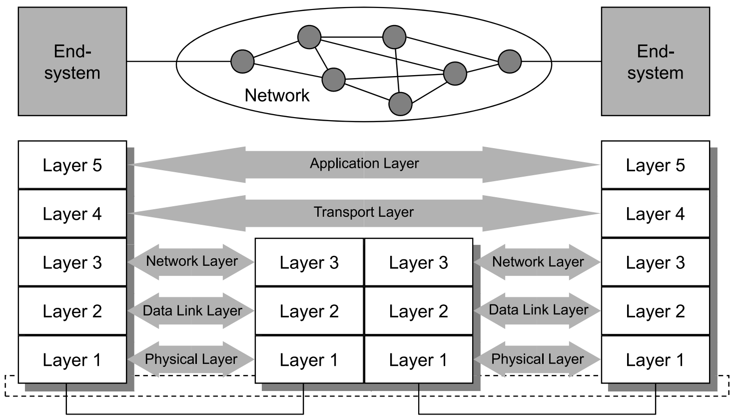
→ Attention: *It is generally impossible to assess unknown attacks!*

- A detailed security analysis of a given network configuration / specific protocol architecture:
  - might also be required in order to convince financially controlling entities in an enterprise to grant funding for security enhancements, and
  - can better be structured according to the more fine grained *attacks on the message level.*

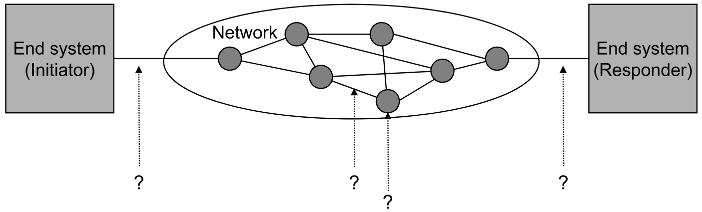
Attacking Communications on the Message Level

- Passive attacks:
  - Eavesdropping of PDUs (Protocol Data Units)
- Active attacks:
  - Delay of PDUs
  - Replay of PDUs
  - Deletion of PDUs
  - Modification of PDUs
  - Insertion of PDUs
- Successful launch of one of the above attacks requires:
  - There are no detectable side effects to other communications (connections / connectionless transmissions)
  - There are no side effects to other PDUs of the same connection / connectionless data transmission between the same entities
- A security analysis of a protocol architecture has to analyse these attacks according to the architecture's layers

Communication in Layered Protocol Architectures

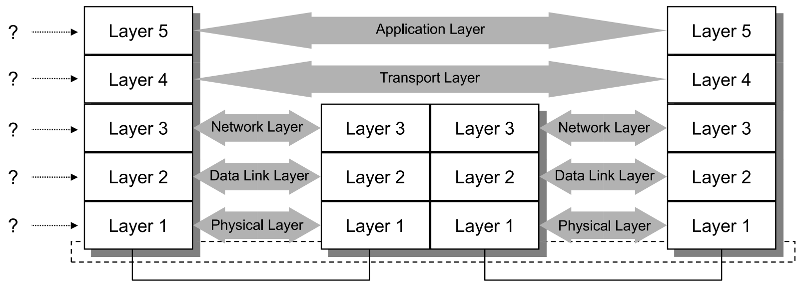


Security Analysis of Layered Protocol Architectures



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

Security Analysis of Layered Protocol Architectures



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

Safeguards Against Information Security Threats

- *Physical Security:*
  - Locks or other physical access control
  - Tamper-proofing of sensitive equipment
  - Environmental controls (e.g. motion detectors)
- *Personnel Security:*
  - Identification of position sensitivity
  - Employee screening processes
  - Security training and awareness
- *Administrative Security:*
  - Controlling import of foreign software
  - Procedures for investigating security breaches
  - Reviewing audit trails, reviewing accountability controls
- *Emanations Security:*
  - Radio Frequency and other electromagnetic emanations controls
  - Referred to as *TEMPEST protection*

Safeguards Against Information Security Threats

- *Media Security:*
  - Safeguarding storage of information
  - Controlling marking, reproduction and destruction of sensitive information
  - Ensuring that media containing sensitive information are destroyed securely
  - Scanning media for viruses
- *Lifecycle Controls:*
  - Trusted system design, implementation, evaluation and endorsement
  - Programming standards and controls
  - Documentation controls
- *Computer Security:*
  - Protection of information while stored / processed in a computer system
  - Protection of the computing devices 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

Communications Security: Some Terminology

- Security Service:
  - An abstract service that seeks to ensure a specific security property
  - A security service can be realised with the help of cryptographic algorithms and protocols as well as with 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
  - There are five fundamental security services:
    - Confidentiality
    - Authentication
    - Non-repudiation
    - Data Integrity
    - Access Control

Security Services – Overview

- *Confidentiality*
  - The most popular security service, ensuring the secrecy of protected data
- *Authentication*
  - The most fundamental security service which ensures that an entity has in fact the identity it claims to have
- *Non Repudiation*
  - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred
- *Data 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
- *Access Control*
  - Controls that each identity accesses only those services and information it is entitled to

Cryptographic Algorithm and Cryptographic Protocol

- 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 Supporting Mechanism:
  - Security relevant functionality which is part of a cryptographic protocol or of a security procedure

Security Supporting Mechanisms

- General mechanisms:
  - *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
- 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

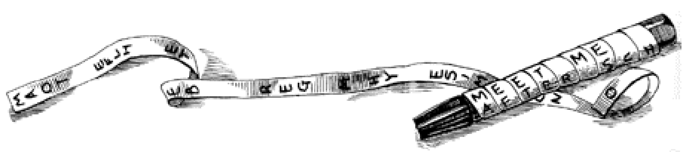
Cryptology – Definition and Terminology

- *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

(Source: Encyclopaedia Britannica)

Cryptology – Some Historic Remarks

- 400 BC: The Spartans employ a cipher device called *scytale* for communications between military commanders.
  - The scytale consisted of a tapered baton, around which was spirally wrapped a strip of parchment or leather on which the message was written
  - When unwrapped, the letters were scrambled in order and formed the cipher
  - When the strip was wrapped around another baton of identical proportions to the original, the plaintext reappeared



Cryptology – Some Historic Remarks

- During 4. century BC:
  - Aeneas Tacticus (Greek) writes *"On the defense of fortifications"*, with one chapter devoted to cryptography
  - Polybius (Greek) invents a means of encoding letters into pairs of symbols by a device called the *Polybius Checkerboard* which realizes a bi-literal substitution and prestages many elements of later cryptosystems

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i,j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

	2,6	0,3	1,5	7,9	4,8
6,8	a	b	c	d	e
1,4	f	g	h	i,j	k
0,9	l	m	n	o	p
2,7	q	r	s	t	u
3,5	v	w	x	y	z

Cryptology – Some Historic Remarks

- 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, ...)
- 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

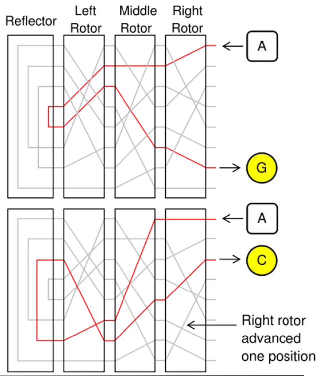
- European Cryptography: (cont.)
  - 1397: *Gabriele de Lavinde* of Parma writes first European manual on cryptography, containing a compilation of ciphers as well as a set of keys for 24 correspondents and embracing symbols for letters, numbers and several two-character code equivalents for words and 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
  - 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

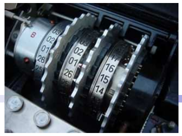
Cryptology – Some Historic Remarks

- Developments during World Wars 1 and 2:
  - During World War 1: cipher systems were mostly used for tactical communications and high level communication was protected using codes
  - 1920: The communication needs of telecommunications and the maturing of electromechanical technology bring 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* and two teleprinter ciphers and the American cryptanalysis of Japanese ciphers

Enigma Cipher – Rotor Machine

- The trick that made Enigma so powerful for its time though, was the spinning of the rotors.
- As the plain text letter passed through the first rotor, the first rotor would rotate one position. The other two rotors would remain stationary until the first rotor had rotated 26 times (one full rotation).
- Then the second rotor would rotate one position. After the second rotor had rotated 26 times (26X26 letters), the third rotor would rotate one position.
- The cycle would continue like this for the entire length of the message. The result was a shifting shift. In other words, an “S” could be encoded as a “B” in the first part of the message, and then as an m later in the message.
- This principle of the shifting rotors allowed for 26X26X26 = 17576 possible positions of the rotors.





Cryptology – Some Historic Remarks

- 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)*
  - 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*

Summary (what do I need to know)

- Basis knowledge of security objectives
  - Goals
  - Threats