Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Network Security
IN2101

Prof. Dr.-Ing. Georg Carle
Dipl.-Inform. Heiko Niedermayer

Institut für Informatik
Technische Universität München
http://www.net.in.tum.de

Georg Carle

- Studium Elektrotechnik, Universität Stuttgart
- Master of Science in Digital Systems, Brunel University, London, U.K. (Master Thesis bei General Electric Corporation, Hirst Research Centre, London)
- Projekt bei Telecom Paris - Ecole Nationale Supérieure des Télécommunications (ENST), Paris
- Promotion in Informatik an der Universität Karlsruhe, am Institut für Telematik; Stipendium im Graduiertenkolleg 'Beherrschbarkeit komplexer Systeme'
- Postdoktorand am Institut Eurecom, Sophia Antipolis, France
- Fraunhofer Institut FOKUS (GMD FOKUS), Berlin
  Leiter des Competence Center Global Networking
- Universität Tübingen, Lehrstuhl für Rechnernetze und Internet
- Seit 1. April 2008: Lehrstuhl für Netzarchitekturen und Netzdienste, TU München

Chair for Network Architectures and Services
Department of Informatics
TU München – Prof. Carle

Network Security

Chapter 1
Introduction

Course organization

- Lecture
  - Wednesday, 14:15-15.45, MI 00.08.038
  - Typically Bi-weekly Thursday, 14:15-15.45, MI 00.08.038
- Exercises
  - Typically Bi-weekly Thursady 14:15-15.45, MI 00.08.038
- Students are requested to subscribe to lecture and exercises at
  http://www.net.in.tum.de/de/lehre/ws0910/vorlesungen/network-security/
- Email list
  - for subscribers to lecture and exercises
- Questions and Answers / Office hours
  - Prof. Dr. Georg Carle, carle@net.in.tum.de
    - After the course and upon appointment
  - Dipl.-Inform. Heiko Niedermayer, niedermayer@in.tum.de
  - Dipl.-Inform. Ralph Holz, holz@net.in.tum.de
- Course Material
  - All slides are available online. Slides may be updated during the course.
  - This course is based to a significant extend on slides provided by Prof. Günter Schäfer, author of the **book "Netzsicherheit - Algorithmische Grundlagen und Protokolle"** by Günter Schäfer, available in German from **dpunkt Verlag**. (An English version is also available.) We gratefully acknowledge his support.

Fragen

- Wer studiert was?
  - Bachelor Informatik? / Wirtschaftsinformatik?
  - Master Informatik? / Wirtschaftsinformatik?
  - Diplom?
- Welche Vorkenntnisse?
  - Grundlagen Rechnernetze und Verteilte Systeme?
  - Was noch?
  - Kryptografie etc?
- Wer will an den Übungen teilnehmen?

Chapter 1
Introduction

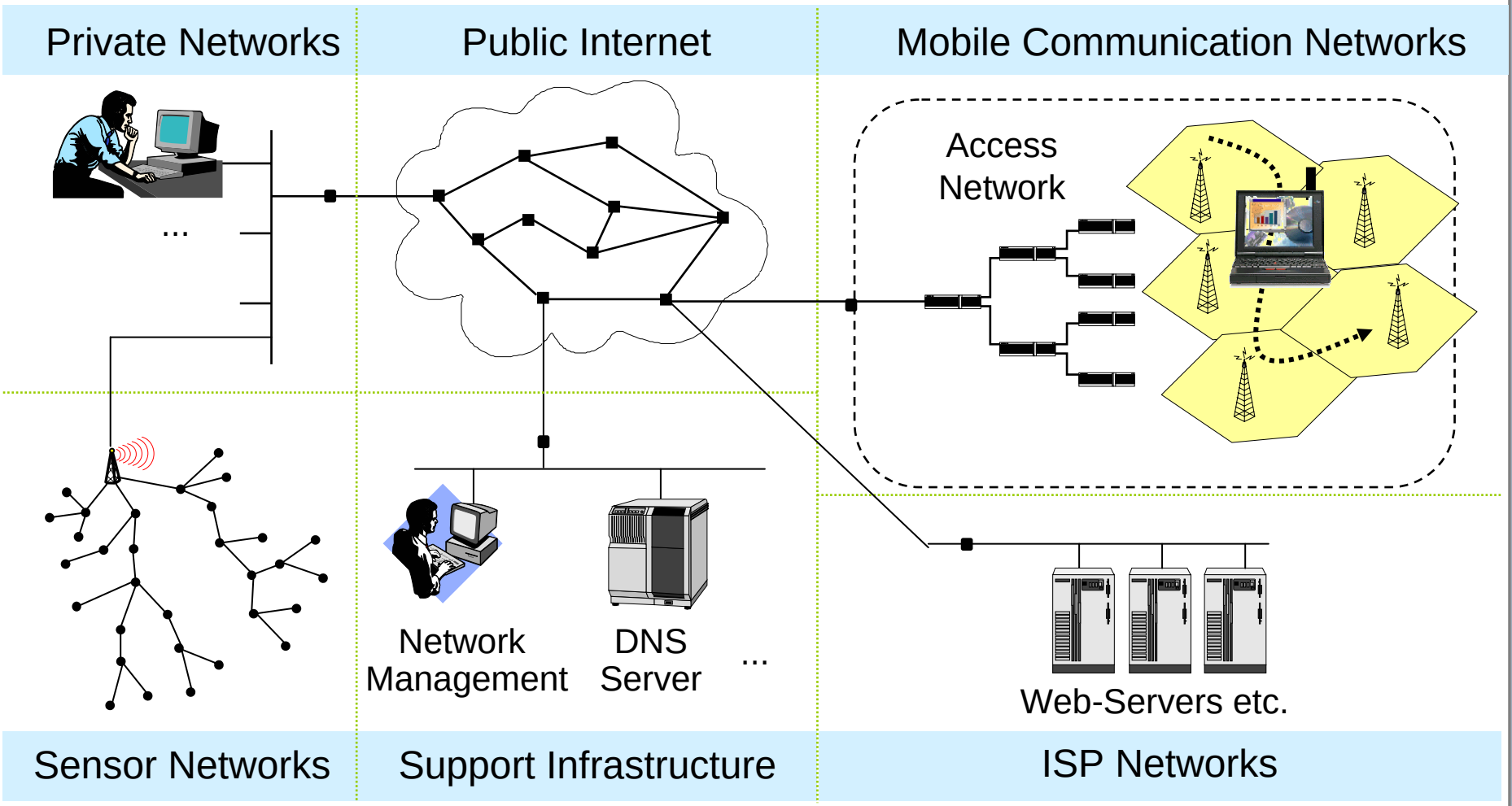
- Motivation
- Threats in communication networks
- Security goals & requirements
- Network security analysis
- Security measures
- Bibliography

Motivation: A Changing World

- Mobile communication networks and ubiquitous availability of the global Internet have already changed dramatically the way we
  - communicate,
  - conduct business, and
  - organize our society
- With current research and developments in sensor networks and pervasive computing, we are even creating a new networked world
- However, the benefits associated with information and communication technology imply new vulnerabilities

➡ Increasing dependence of modern information society on availability and secure operation of communication services

A High Level Model for Internet-Based IT-Infrastructure



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 (1)

- 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 (2)

- 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?)

- Security goals are also called *security objectives*

Security Goals Technically Defined

- *Confidentiality ("Vertraulichkeit"):*
  - Data transmitted or stored should only be revealed to an intended audience
  - Confidentiality of entities is also referred to as *anonymity*
- *Data Integrity ("Datenintegrität"):*
  - It should be possible to detect any modification of data
- *Accountability ("Zurechenbarkeit"):*
  - It should be possible to identify the entity responsible for any communication event
  - Accountability directly supports non-repudiation ("Nicht-Abstreitbarkeit"), and also deterrence, intrusion prevention, security monitoring, and others
- *Availability ("Verfügbarkeit"):*
  - Services should be available and function correctly
- *Controlled Access ("kontrollierter Zugang"):*
  - Only authorized entities should be able to access certain services or information

Threats Technically Defined (1)

- *Masquerade:*
  - An entity claims to be another entity (also called “Impersonation”)
- *Eavesdropping:*
  - An entity reads information it is not intended to read
- *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/Denial of Service*
  - Any action that aims to reduce the availability and / or correct functioning of services or systems
- *Authorization Violation:*
  - An entity uses a service or resources it is not intended to use

Threats and Technical Security Goals

- The realization of a threat (attack) will try to break one or more security goals:

Technical Security Goals	General Threats						
	Masquer-ade	Eaves-dropping	Authori-sation Violation	Loss or Mo-dification of (transmitted) information	Denial of Communi-cation acts	Forgery of Infor-mation	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x	x	x	x	
Availability	x		x				x
Controlled Access	x		x	x		x	

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

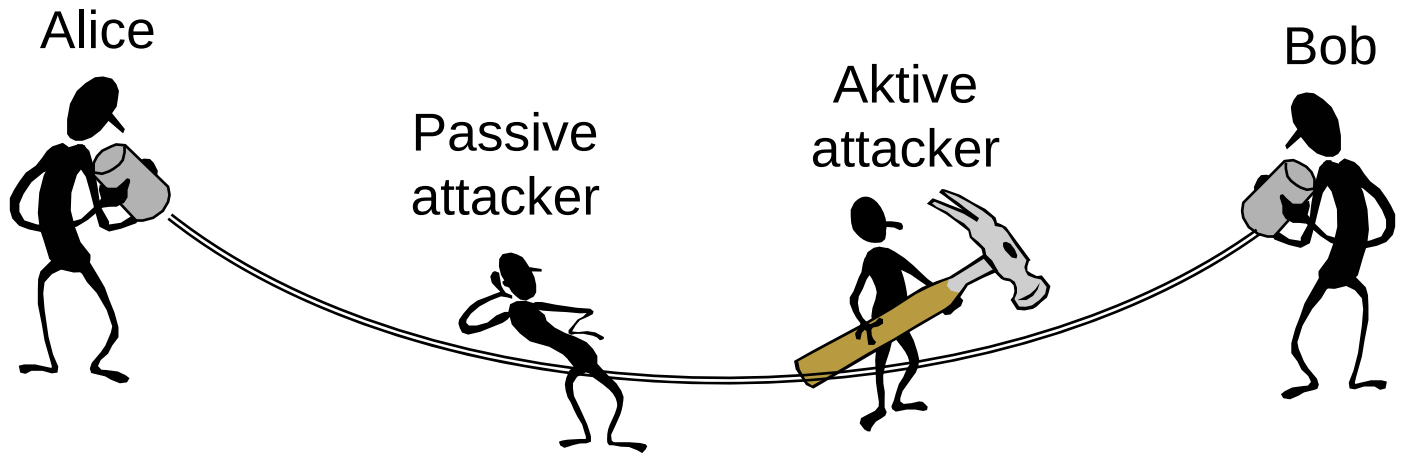
Network Security Analysis

- 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 potential risk of the 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 / a specific protocol architecture:
  - may be required to convince financially controlling entities in an enterprise to grant funding for security enhancements
  - can be structured according to the more fine grained *attacks on the message level.*

Attacks on Communication Networks



Eavesdropping of messages/
Recognition of communication parties

Replay/delay messages

Masquerade

Message forging

Passive attacks

Aktive attacks

Traffic analysis

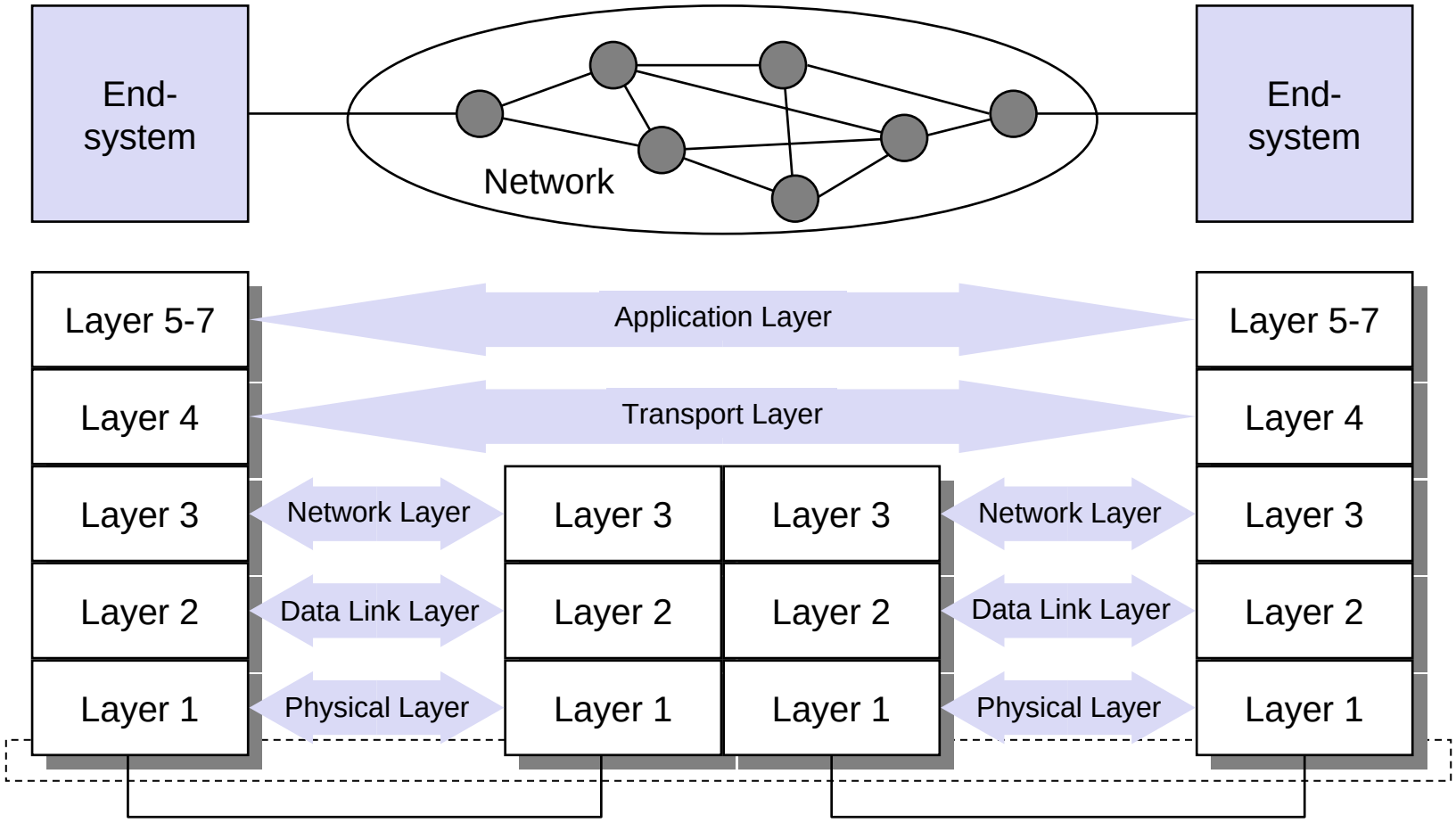
Insert / delete messages

Sabotage („Denial of Service“ attacks)

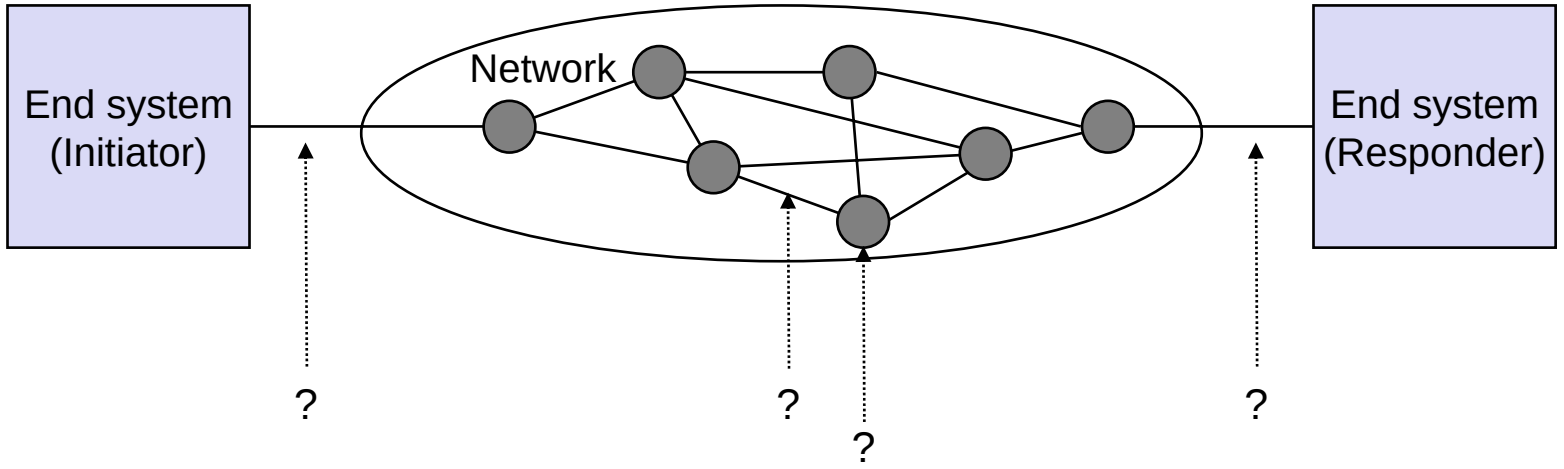
Attacking Communications on the Message Level

- Passive attacks:
  - Eavesdropping of messages
- Active attacks:
  - Delay of messages
  - Replay of messages
  - Deletion of messages
  - Modification of messages
  - Insertion of messages
- A security analysis of a protocol architecture has to analyse these attacks according to the architecture's layers

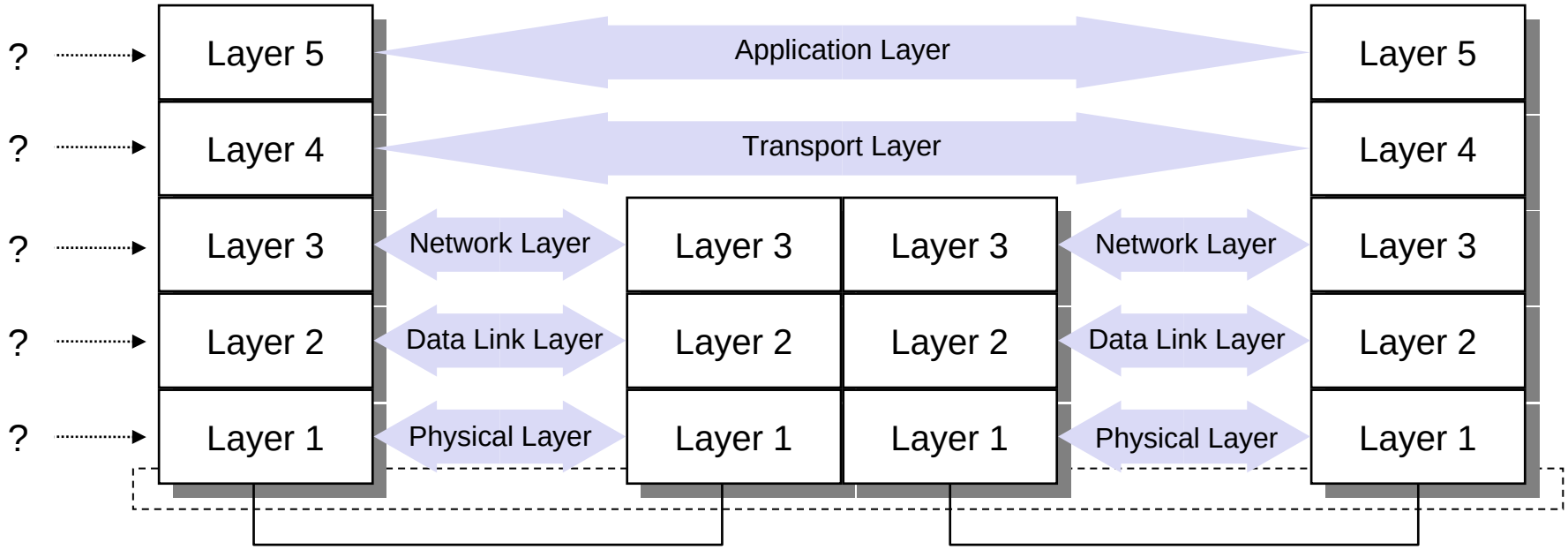
Communication in Layered Protocol Architectures



Security Analysis of Layered Protocol Architectures (1)

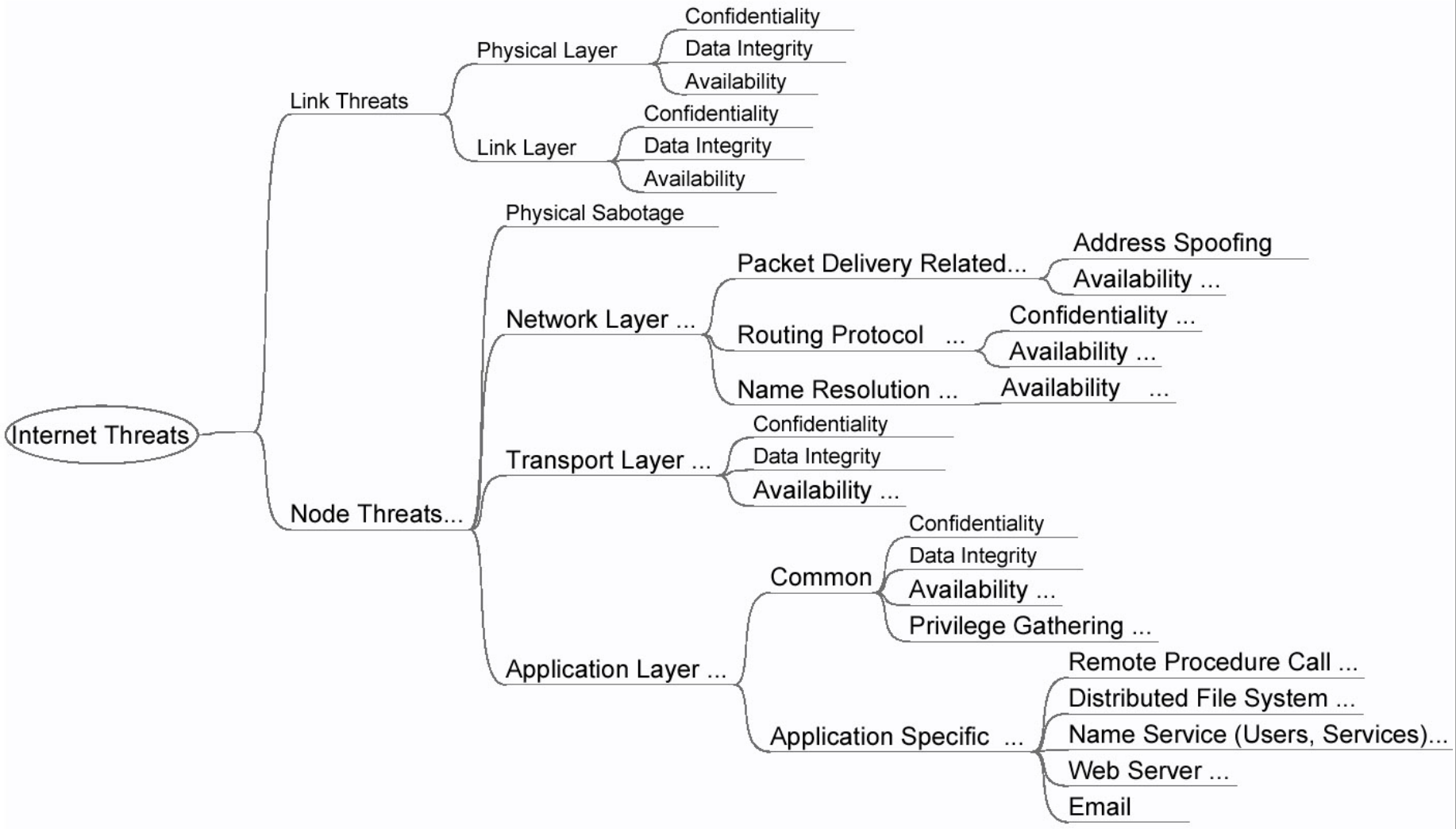


Dimension 1: At which interface does the attack take place?



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

A High Level Threat Tree for Internet-Based IT-Infrastructure



Measures against Information Security Threats (1)

- *Physical Security:*
  - Locks or other physical access control
  - Tamper-proofing of sensitive equipment
    (c.f. Tamper resistance and tamper-evident systems)
- *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

Measures against Information Security Threats (2)

- *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 *security goal*
  - 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
  - Fundamental security services:
    - Confidentiality
    - Entity authentication
    - Message authentication
    - Access control
    - Intrusion detection

Security Services – Overview

- *Confidentiality*
  - The most popular security service, ensuring the secrecy of protected data
- *Entity Authentication*
  - The most fundamental security service which ensures that an entity has in fact the identity it claims to have
- Message Authentication
  - This service ensures that the source of a message can be verified (*data origin authentication*) and that data can not be modified without detection (*data integrity*)
- *Access Control*
  - Controls that each identity accesses only those services and information it is entitled to
- Intrusion detection

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 messages in a network

Course Overview (to be updated during the course)

2. Basics
   1. Symmetric cryptography
   2. Asymmetric cryptography
   3. Modification check values
   4. Random numbers for cryptographic protocols
3. Cryptographic protocols
4. The IPSec architecture for the Internet Protocol
5. Security protocols of the transport layer
6. Link Layer Security (also Wireless LAN Security
7. Middleboxes
8. System Vulnerabilities and Denial of Service Attacks
9. Intrusion Prevention, Detection and Response

Bibliography

- Main books:
  - [Bless05] R. Bless, S. Mink, E.-O. Blaß, M. Conrad, H.-J. Hof, K. Kutzner, M. Schöller: "Sichere Netzwerkkommunikation", Springer, 2005, ISBN: 3-540-21845-9
  - [Ferg03] Niels Ferguson, B. Schneier: “Practical Cryptography”, Wiley, 1st edition, March 2003
  - [Sch03] G. Schäfer. Netzsicherheit – Algorithmische Grundlagen und Protokolle. Soft cover, 422 pages, dpunkt.verlag, 2003.

- Additional references will be provided for each chapter depending on the topic.