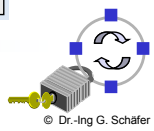
Protection of Communication Infrastructures

Chapter 1
Introduction

- Threats, Security Goals & Requirements
- Threat Analysis
- System Security Engineering
- Course Objectives & Overview

http://www.tu-ilmenau.de/telematik/protection/

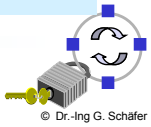


A Short Advertisement Before We Begin... :o)

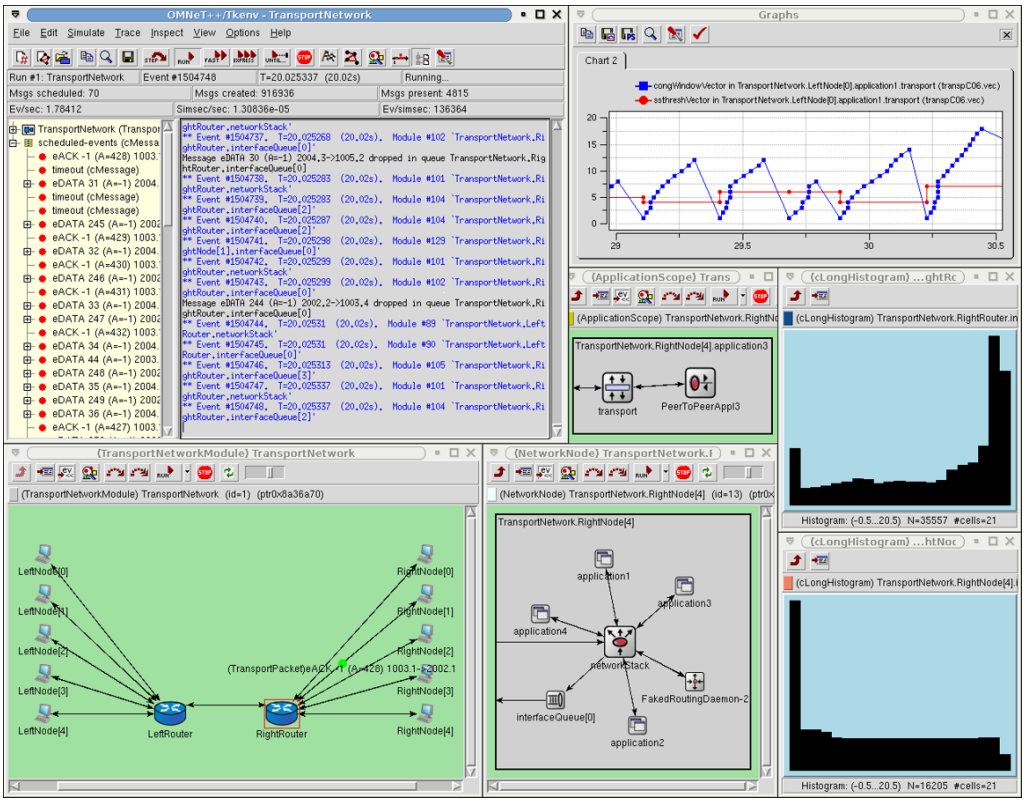
- There is an additional course – entitled „Simulative Evaluation of Protocol Functions" (project seminar, 4 SWS) – which is designed to give you a "hands-on" experience with network protocol functions and simulation studies:
  - Introduces a simulation environment and lets you add protocol functionality
  - Studied protocol functions: forwarding, routing, (interface queues), connection setup, error-, flow- and congestion control
  - Requires good programming skills
  - Knowledge of C++ is an asset (but not a pre-requisite)
  - Allows you to obtain in-depth knowledge of topics covered in Telematics I and the techniques and art of simulation studies – because afterwards "you did it!" :o)

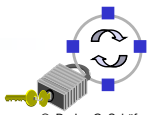
- For introduction and inscription email to:

  michael-jan.stoyke@tu-ilmenau.de



Example: Evaluation of TCP Congestion Control

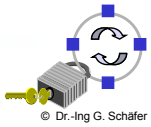




Motivation

- Mobile communication networks and ubiquitous availability of the global Internet have changed dramatically the way we
  - communicate,
  - conduct business, and
  - organize our society
- With developments in sensor networks and pervasive computing, we are 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



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:
  - 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

- Public Telecommunication Providers:
  - Protect subscribers privacy
  - Restrict access to administrative functions to authorized personnel
  - Protect against service interruptions
- Corporate / Private Networks:
  - Protect corporate / individual privacy
  - Ensure message authenticity
  - Protect against service interruptions
- 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
- *Controlled Access:*
  - Only authorized entities should be able to access certain services or information
- *Availability:*
  - Services should be available and function correctly

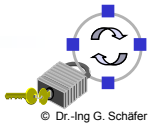
Threats Technically Defined

- *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 (Denial of Service):*
  - Any action that aims to reduce the availability and / or correct functioning of services or systems

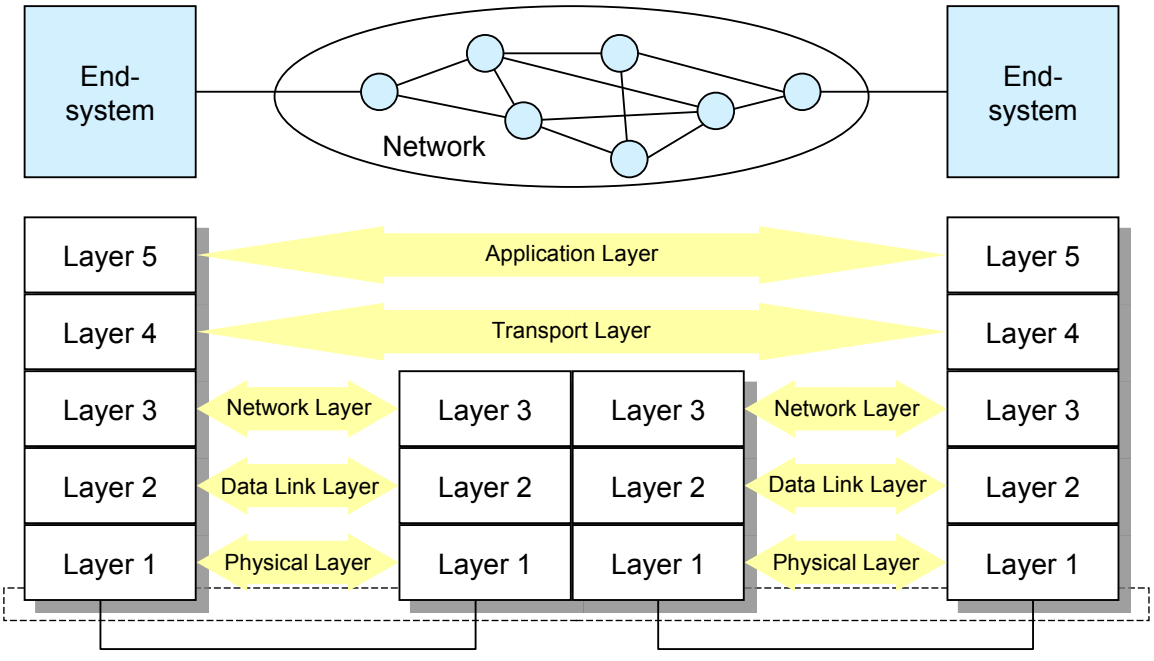
Threats and Technical Security Goals

Technical Security Goals	General Threats						
	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	
Availability	x		x	x			x
Controlled Access	x		x			x	

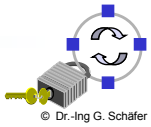
Threats are often combined in order to perform an attack!



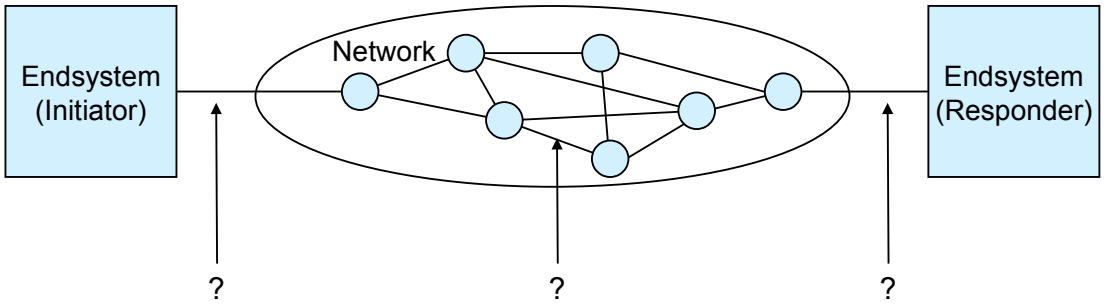
Architectural View of our “Object” to be Protected



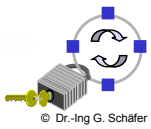
Communication in Layered Protocol Architectures



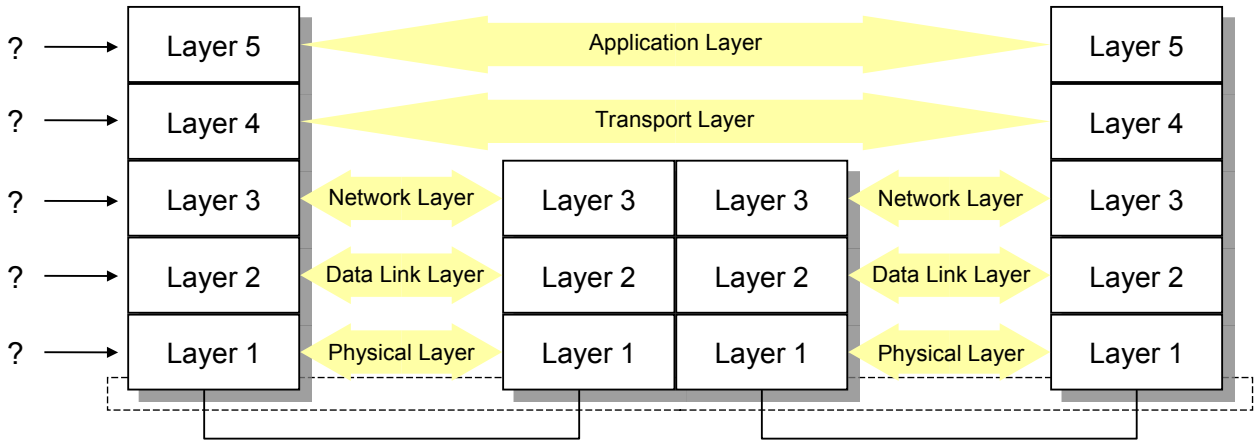
Security Analysis of Layered Protocol Architectures 1



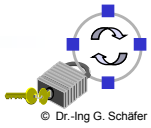
Dimension 1: At which interface could an attack take place?



Security Analysis of Layered Protocol Architectures 2

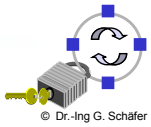


Dimension 2: In which layer could an attack take place?



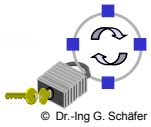
Systematic Threat Analysis on the Message Level

- A systematic security analysis of a layered protocol architecture has to consider the following attacking techniques:
  - Passive attacks:
    - Eavesdropping
  - Active attacks:
    - Delay of PDUs (Protocol Data Units)
    - 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



Security Analysis of Communication Infrastructures

- On the preceding slides, the analysis was basically concentrated on potential *attacks on the transmission of information*
- Of equal importance, however, are *attacks against the systems*, that are part of or making use of a communication network:
  - End systems
  - Routers
  - Important infrastructure servers: DNS, Email, WWW, file servers, etc.
- We, therefore, have to extend our analysis framework:
  - Dimension S.1: Which system could be attacked?
  - Dimension S.2: Which component of the system is attacked (OS, protocol stack, application process, etc.)?
- However, this introduces a new difficulty:
  - An active entity (system) offers much more different attacking opportunities than a passive data object (like a PDU)
  - It is, therefore, much harder to conduct a systematical analysis



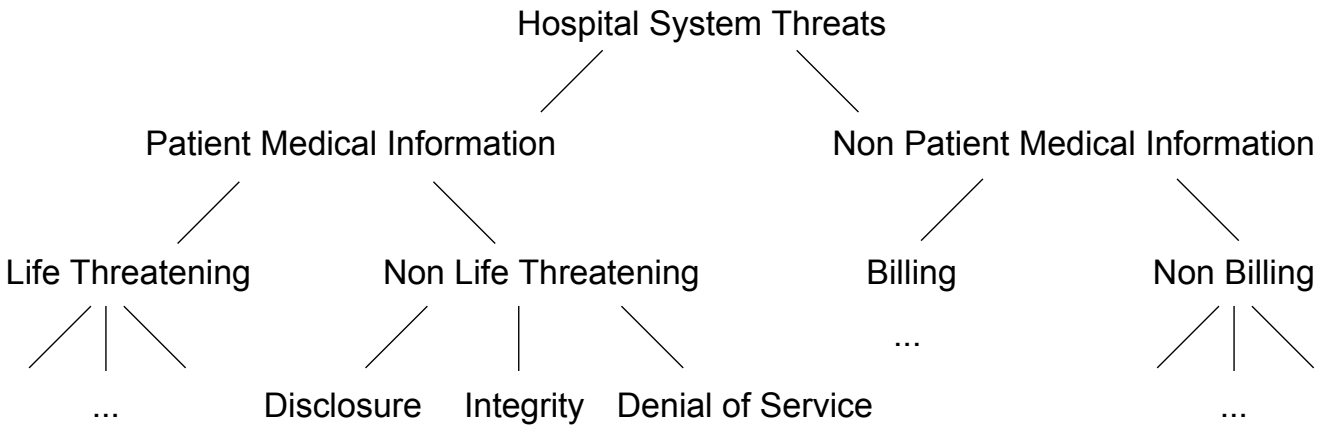
Towards Systematic Threat Analysis

- One not very systematic approach is producing of *arbitrary threat lists* by any ad-hoc brainstorming method
- Example: Hospital Information System
  - Corruption of patient medical information
  - Corruption of billing information
  - Disclosure of confidential patient information
  - Compromise of internal schedules
  - Unavailability of confidential patient information
  - ...
- Drawbacks of this approach:
  - Questionable completeness of identified threats
  - Lack of rationale for identified threats other than experience
  - Potential inconsistencies (e.g. disclosure vs. unavailability of confidential patient information in the example above)

Threat Trees: One Systematic Threat Analysis Approach

- Definition: *threat tree*
  - A *threat tree* is a tree with:
    - *nodes* describing threats at different levels of abstractions, and
    - *subtrees* refining the threat of the node they are rooted at,
    - where the child nodes of one node give a *complete refinement* of the threat represented by the parent node
- Technique for establishing threat trees:
  - Start with a general abstract description of the complete set of threats that exist for a given system (e.g. “security of system X compromised”)
  - Iteratively introduce detail by gradually refining the description with care
  - Each introduced node may itself become the root of a subtree further describing the threat represented by the node
  - Eventually, each leaf node of the tree provides a description of a threat that can be used for a (less arbitrary) threat list
- The main idea of this technique is to postpone the creation of (arbitrary) treat lists as much as possible

Example: A Hospital Information System Threat Tree

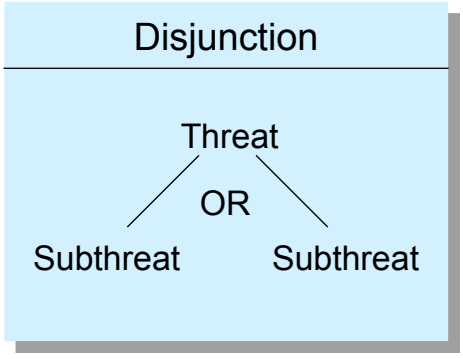


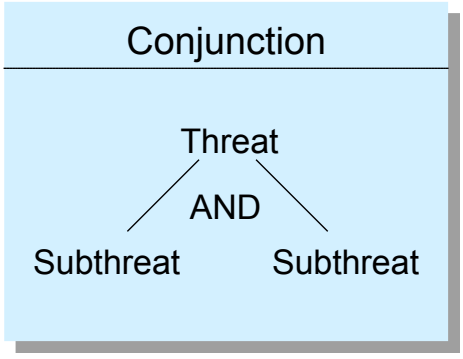
➡ It is important that at each level of refinement the child nodes of a node maintain *demonstrable completeness* so that one can be confident that nothing has been missed

(source: [Amo94])

Inferring Composed Threat in Threat Trees

- The child nodes of one node can actually be in different relations to their parent node with the two most common relations being:

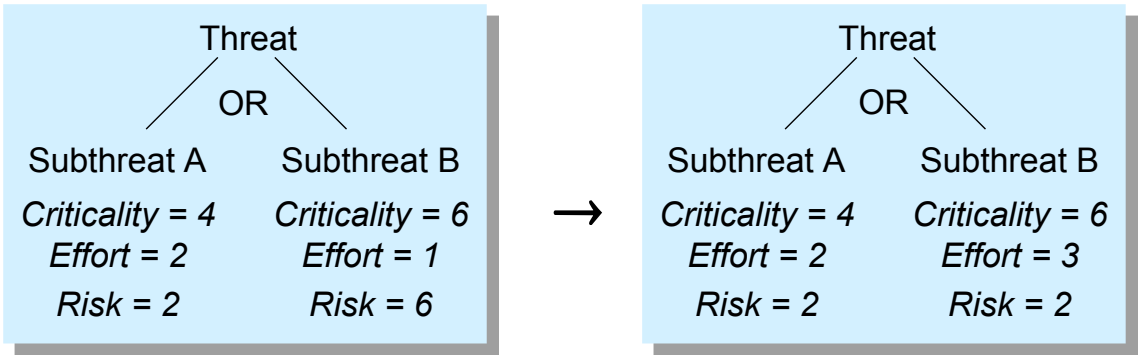




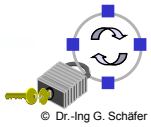
- These relations can be used to infer composed threat:
  - Augment nodes with effort estimations (e.g. easy, moderate, high)
  - Infer effort of an OR-related composed threat as the lowest effort value of its child nodes (the attacker will most likely take the easy way...)
  - For AND-related composed threats, the highest effort is inferred

Supporting System Security Engineering with Threat Trees

- When augmented with appropriate attributes (e.g. estimated criticality and attacker effort for individual threats), threat trees can help to gain insight where to spend resources to decrease the overall system's vulnerability:

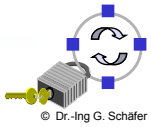


- The second threat tree re-evaluates risk after some protective measure has been taken to increase the attacker's effort for subthreat B
- In the above example, risk is assessed with the following formula:
  - Risk = Criticality / Effort

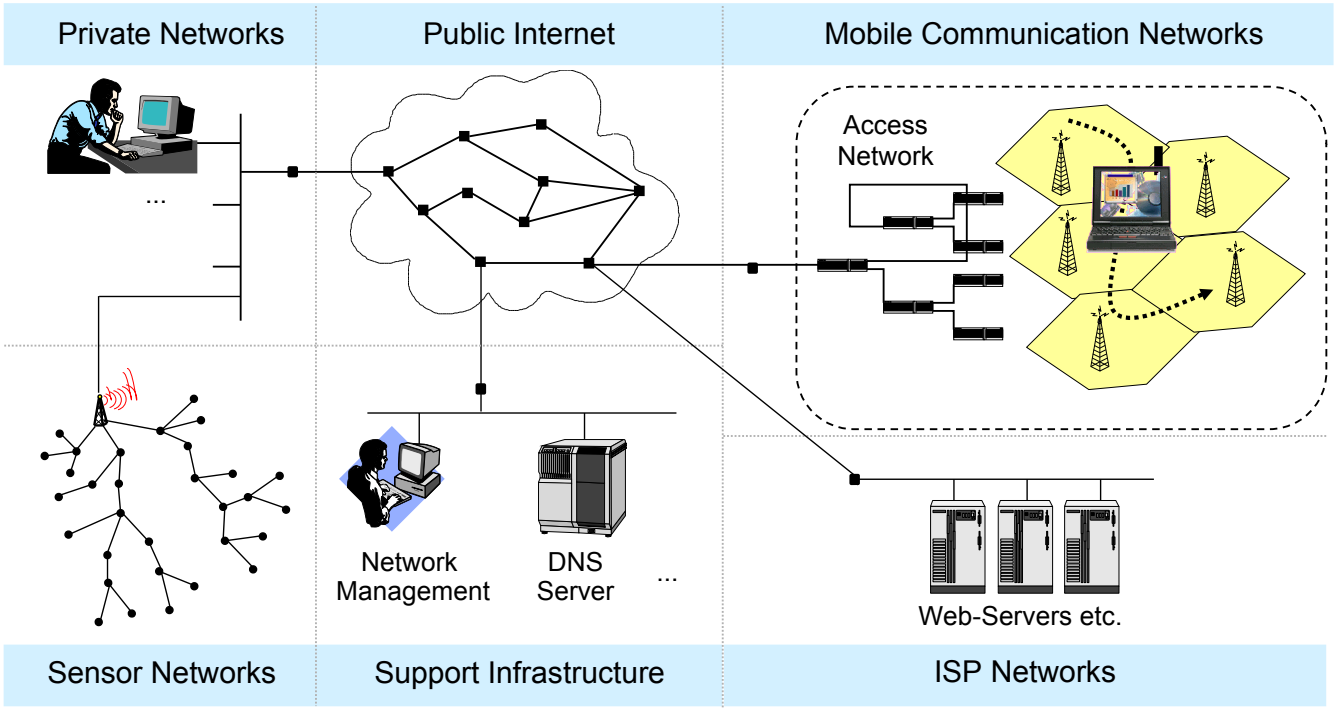


A High Level System Security Engineering Process

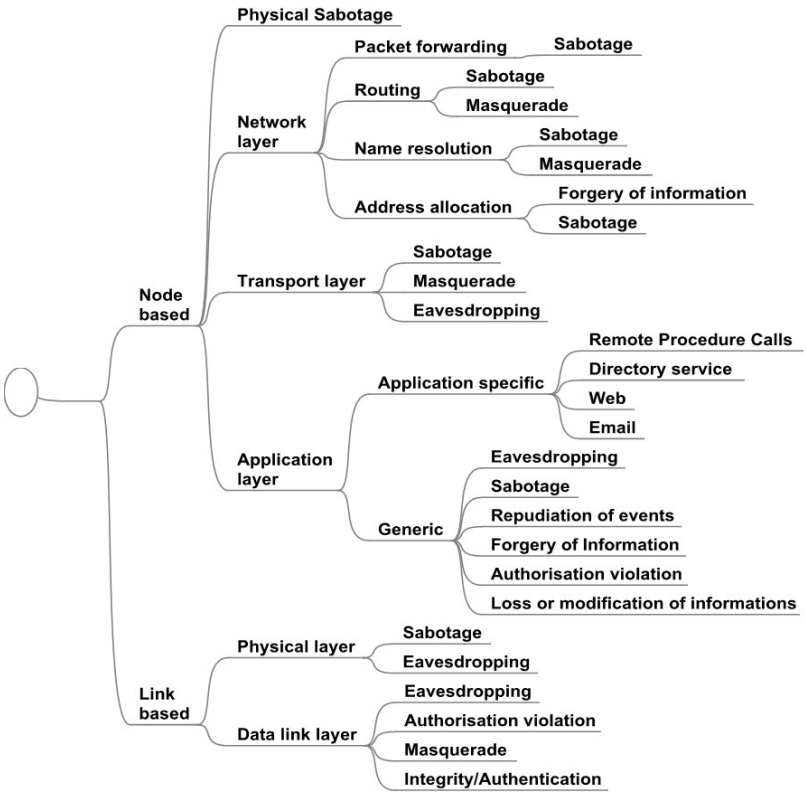
- Specify system architecture:
  - Identify components and interrelations
- Identify threats, vulnerabilities and attack techniques:
  - The threat tree technique provides help for this step
- Estimate component risks by adding attributes to the threat tree:
  - However, removing subjectivity from initial assessments is often impossible and other attributes than criticality and effort (e.g. risk of detection) might have to be considered as well
- Prioritize vulnerabilities:
  - Taking into account the components' importance
- Identify and install safeguards:
  - Apply protection techniques to counter high priority vulnerabilities
- Perform potential iterations of this process
  - Re-assess risks of the modified system and decide, if more iterations are required



A High Level Model for Internet-Based IT-Infrastructure

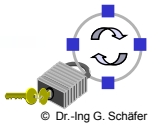


A High Level Threat Tree for Internet-Based IT-Infrastructure



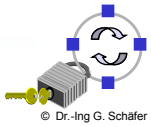
Countering Attacks: Three Principle Classes of Action

- *Prevention:*
  - All measures taken in order to avert that an attacker succeeds in realizing a threat
  - Examples:
    - Cryptographic measures: encryption, computation of modification detection codes, running authentication protocols, etc.
    - Firewall techniques: packet filtering, service proxying, etc.
  - Preventive measures are by definition taken *before an attack takes place*
- *Detection:*
  - All measures taken to recognize an attack *while or after it occurred*
  - Examples:
    - Recording and analysis of audit trails
    - On-the-fly traffic monitoring
- *Reaction:*
  - All measures taken in order react to *ongoing or past attacks*



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
- *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 2

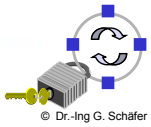
- *Media Security:*
  - Safeguarding storage of information
  - Controlling marking, reproduction and destruction of sensitive information
  - Ensuring that media containing sensitive information are destroyed securely
  - Scanning media for viruses
- *Lifecycle Controls:*
  - Trusted system design,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

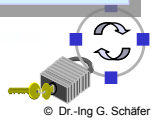
Security Services – Overview

- *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
- *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



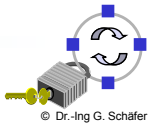
Course Objectives

- The course *Network Security* (held every fall term) focuses on:
  - Introduction to information security technology (incl. cryptology)
  - Network security protocols to ensure:
    - Entity authentication
    - Data confidentiality & data integrity
  - Some established techniques to realize access control in networks
- This course takes a complementary view on the following aspects:
  - Threats and measures concerning systems and their software
  - Threats to and measures for ensuring availability
  - How to protect Internet wide routing against common threats
  - Threats and security measures specific to the Domain Name System
  - Internet Firewalls
  - Measures for intrusion detection and response
  - Sensor network security
  - Protecting large scale VPNs against attacks with quantum computers



Course Overview

1. Introduction
2. Security Aware System Design and Implementation
3. Denial-of-Service Attacks and Countermeasures
4. Routing Security
5. DNS Security
6. Internet Firewalls
7. Intrusion Detection and Response
8. Security in Sensor Networks
9. Protecting VPNs against quantum computer attacks



General Course Bibliography

[Amo94] E. Amoroso. *Fundamentals of Computer Security Technology.* Prentice Hall. 1994.

[Amo99] E. Amoroso. *Intrusion Detection.* Intrusion.Net Books, 1999.

[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.

[GW03] M.G. Graff, K.R. van Wyck. *Secure Coding.* O'Reilly, 2003

[NN01] S. Northcutt, J. Novak. *Network Intrusion Detection - An Analyst's Handbook.* second edition, New Riders, 2001.

[SR14] G. Schäfer, M. Rossberg. Netzsicherheit - dpunkt.verlag, 676 Seiten, Gebunden, 49,90 Euro, 2014.

[VM02] J. Viega, G. McGraw. *Building Secure Software.* Addison-Wesley, 2003.