Fachhochschule Gelsenkirchen

Information Security
→ Introduction

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
Gelsenkirchen University of Applied Sciences
http://www.internet-sicherheit.de

if(is) internet security.

Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- Change of meaning in IT systems
- IT security as a correlation of effect and action
- Possible threats in communication systems
- Possible damage
- Security and trustworthiness
- Summary

Content

- **Aim and outcomes of this lecture**

- Real World vs. Electronic World
- Change of meaning in IT systems
- IT security as a correlation of effect and action
- Possible threats in communication systems
- Possible damage
- Security and trustworthiness
- Summary

Information security - Introduction
→ Aims and outcomes of this lecture

Aims

- To create the motivation for the matter of information security
- To explore the information security as an correlation of effect and action
- To analyze the threads in communication systems
- To assess the possible damage and the need of trustworthiness

At the end of this lecture you will be able to:

- Understand the meaning of information security
- Know correlation of effect and action in the information security field.
- Know something about threats to our information society.
- Understand what security and trustworthiness is.

Content

- Aim and outcomes of this lecture
- **Real World vs. Electronic World**
- Change of meaning in IT-Systems
- IT security as a correlation of effect and action
- Possible threats in communication systems
- Possible Damage
- Security and trustworthiness
- Summary

Introduction
→ Overview

- We are currently turning into a **knowledge** and **information** society.
- Security and trustworthiness of information and communication technologies play an important role.
- The **communication networks** and the services that rely on them - the Internet - have developed rapidly and therefore they are today one of the **most important infrastructures** of our modern society.
- The services offered brought enormous advantages and the future will bring even more **potential** to manage **business processes more efficiently** and to open up new **business markets**.
- During the past years the impact of IT **security risks** hasn‘t been reduced but it gained in **importance.**

In a perfect world ...

- ... we have trust und friendliness
- ... information is freely accessible and free of charge
- ... no one gets rich at the expense of others
- ... all customers are willing to pay the desired price
- ... competition is transparent, fair and balanced

A perfect world doesn‘t exist

How does the real world look like?

- … information and knowledge is shared unequally
- … burglary and theft threaten property
- … fraud and betrayal effect on the business life
- … attacks and terror occur everyday

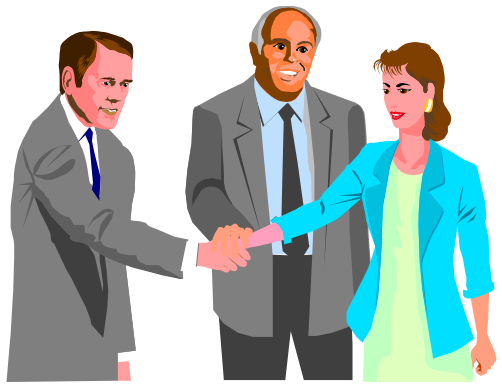
How do we protect ourselves … in the real world?

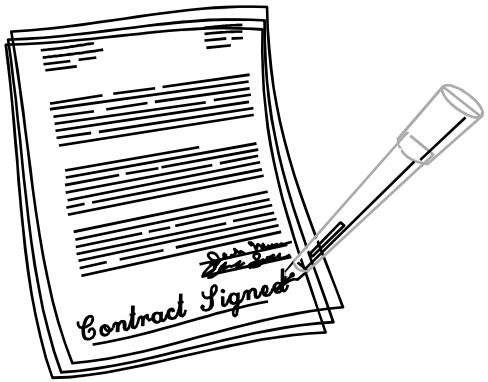
- **Gate keeper**
  makes sure that no stranger enters the company building
- **Armored Delivery Van**
  ensures the transport of enterprise values
- **Civil registry office / registration office**
  ensures that a human can clearly be identified and can verify the authenticity
- **Letters / "manual" signature**
  ensure the confidential exchange of information and the obligation of the referring actions
- **Safe-deposit box / locker**
  takes care of a safe keeping of values (information, strategy papers, citizen data)

Real vs. electronic world

„Trustworthiness in the electronic world"

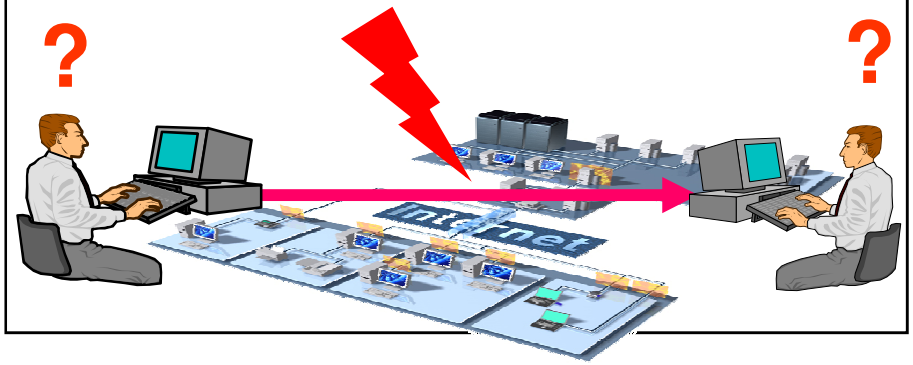
real world





electronic world needs

- confidentiality
- authentication
- data integrity
- reliability



How can the knowledge and information society protect itself in the future?

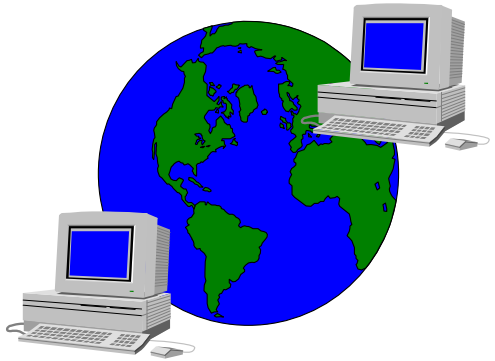
- **electronic gate keeper**
  like a **Firewall or PC security systems** which protect the internal IT systems against unauthorized access from the outside
- **electronic armored delivery vans**
  Virtual Private Networks (IPSec, TLS, ...) protect the transmission of electronic information (values) against eavesdropping and manipulation
- **electronic civil registry offices and registration offices**
  Public Key Infrastructure (PKI) and its applications provide a clear identification and verification of communications partners in the Internet
- **electronic mail / signatures**
  e-mail security and electronic signatures ensure the confidentiality of e-mail traffic, furthermore they guarantee the liability
- **electronic safe**
  file- and hard drive encryption create a safe storage for electronic information (values) on a computer system

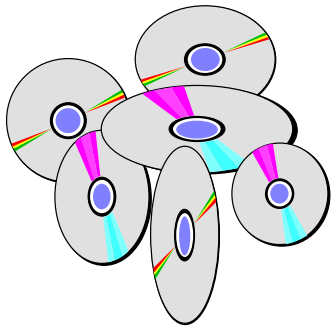
Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- **Change of meaning in IT systems**
- IT security as a correlation of effect and action
- Possible threats in communication systems
- Possible damage
- Security and trustworthiness
- Summary

Change of meaning in IT systems
→ Overview (1/2)

- **Increasing use of IT systems**
  - efficient processing
  - rational handling
  - tasks become more complex
  - global economic extension

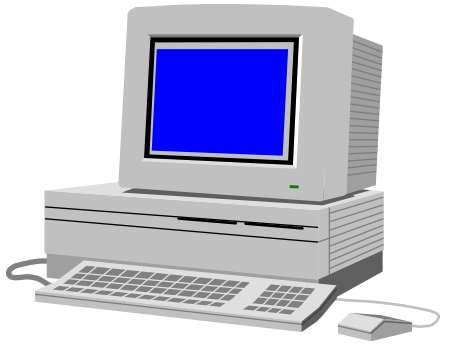




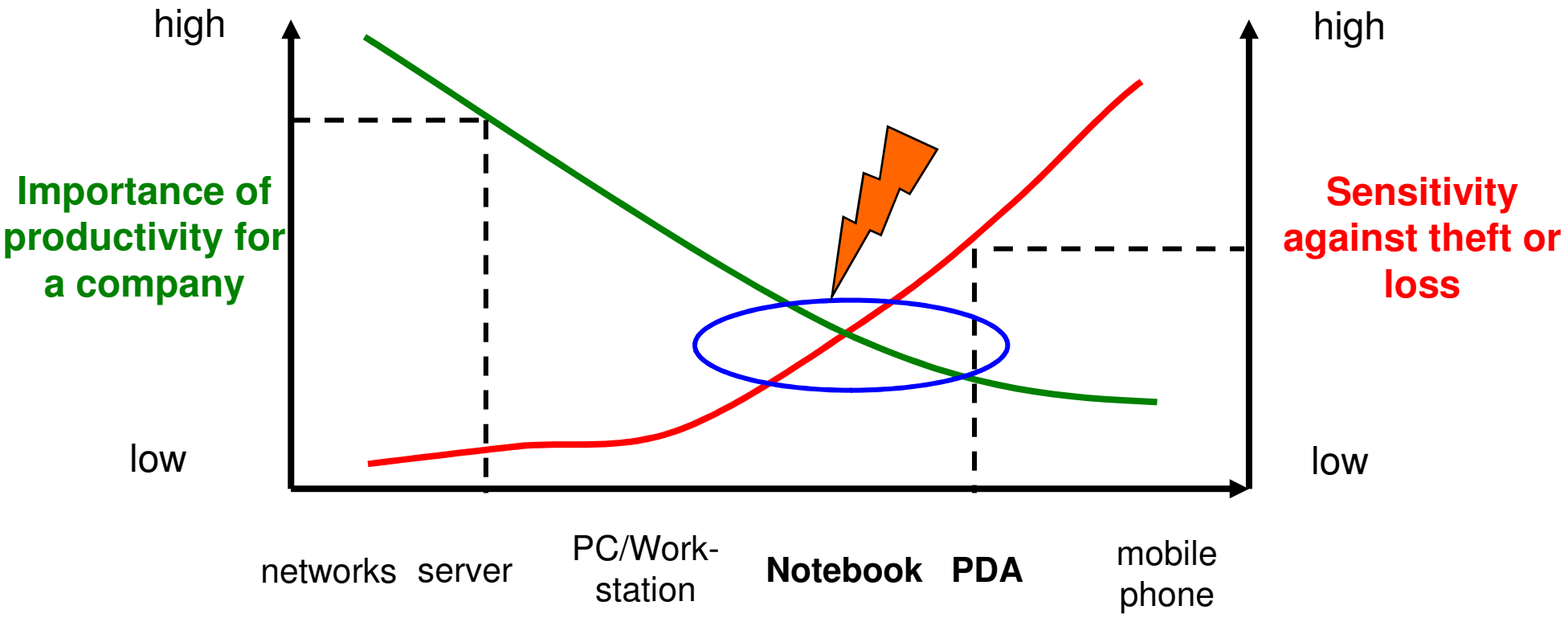
- **Rising dependencies between IT systems**
  - tasks can no longer be performed without IT systems
  - threats of economic performance
  - full circle of electronic data from input till deletion

Change of meaning in IT systems → Overview (2/2)

- **Increasing value of information based on IT systems**
  - complete development and production documents
  - Business reports, strategy papers
  - logistic information
  - customer details



Change of meaning in IT systems
→ New risks through enhanced mobility



IT and communication infrastructure components and their level of mobility

Change of meaning in IT systems
→ Having no awareness of wrongdoing

Electronic world:

- Enhanced operating range
- Strong abstraction between action and effect
- This requires a more sensitive awareness while handling the electronic world

Change of meaning in IT systems
→ Borders and cultures

- The Internet crosses all
  - **geographical borders**
  - **political / administrative borders**
  - **cultures**

    and therefore poses a new and unusual challenge for the international society.

- The speed at which new requirements are arising is increasing and along with it the security risks.

Change of meaning in IT systems
→ Time and place become overridden

- **Location transparency**
  - The place where data is stored or where an application is running stays invisible and is no longer relevant.
  - Location transparency enables the access on a resource without knowing the exact physical location.
- **Services are always available**
- Perfect communication / **„always best connected“:**
  Communication with anybody, anytime from everywhere on all channels, with any capacity in a desired service quality
- **Transmissions just take a few millisecond**

Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- Change of meaning in IT systems
- **IT security as a correlation of effect and action**
- Possible threats in communication systems
- Possible damage
- Security and trustworthiness
- Summary

Correlation of cause and effect → Values

- **Information and data**
  - Development documents, merger intentions, strategy papers, customer database, eMovies, eMusic, eBooks, etc.
- **Resources**
  - computer systems (HW and SW), printers, …
  - CPU time, special calculations (e.g. taxes)
- **Services**
  - database queries
  - Application Service Provider (CAD, SAP, ...)
- **Processes and workflows** (finance software, materials management, ...)
- **Reputation and trust** (very high value)
- **Business potential** (could be very high value)
- …

Correlation of cause and effect
→ Need for protection

- **Guarantee of confidentiality**
  Unauthorized individuals should not be able to read transferred or stored electronic information.
- **Guarantee of authentication**
  We should know the identity of our partner during electronic communication or transaction. Especially the identity of those having access to our electronic information and resources
- **Guarantee of integrity**
  We should be able to proof whether our electronic information is unchanged, that means original.
- **Guarantee of reliability**
  Having the certainty that our electronic processes and the involved actions are binding/reliable.
- **Guarantee of availability**
  Having the certainty that our electronic information and services are available

Correlation of cause and effect
→ Idea behind an attack

The attacker tries to intentionally affect communication to

- obtain specified information (values) without autorization
- trigger reactions that he isn't allowed / authorized to trigger
- use resources (values) that he isn't allowed to use.

The attacker does that to,

- gain profit from the information, reactions and use of resources, or
- without looking for any material profit
  (love of the game, recognition, destructiveness, ...)

Motivation for Criminal Act :

- lack of professional ethos: 27 %
- love of the game: 26 %
- personal benefit: 25 %
- revenge: 22 %

Correlation of cause and effect
→ Attackers (1/2)

- **Hacker**
  Hackers break into computer systems and networks, because they see it as a challenge and they want to use the success to improve their reputation.
  In most cases these hackers are young person that act for the love of the game without having a criminal intent.
  But their action is unpredictable and therefore it could cause enormous damage.

- **eSpy**
  Paid specialists, maybe with a high budget, trying to obtain information through targeted attacks.
  Their motivation mostly has a political or economic background.

- **eTerrorist**
  Terrorists may attack computer systems and networks to provoke fear and chaos for political reasons

Correlation of cause and effect
→ Attackers (2/2)

- **Company cracker**
  These employees try to access computer systems and networks of competitor companies to provide financial advantages for their companies.
  They spy out development documents or strategy papers for example.

- **Professional criminals**
  This people like to enrich themselves through attacks.
  For example by the use of unpaid services or by charging money from foreign bank accounts.

- **Vandals**
  Vandals are people that perform attacks to harm organizations or other individuals.

Correlation of cause and effect
→ Threat

- Potential attack on values
- Level of threat depends on
  - sort of values to be protected
    (attractiveness for competitors, attackers ...)
  - existing security risks
  - implementation opportunities
- Level of threat depends on the own vulnerability

Correlation of cause and effect
→ Security vulnerabilities

- The term security vulnerability is applied to a **weakness in a IT system** which **allows an attacker to violate the integrity** of that IT system.
- Vulnerabilities may result from
  - weak passwords,
  - software bugs,
  - a computer virus or other malware (with use the vulnerabilities),
  - a script code injection,
  - or a SQL injection.
- A vulnerability may **exist only in theory**, or may have a **known instance of an exploit**.

Correlation of cause and effect
→ Security mechanism

- Security software and/or hardware that can be used to protect electronic values
  - Firewall systems, personal firewalls
  - VPN, SSL (TLS)
  - E-mail security (digital signature, object encryption)
  - Anti-virus/anti-malware
  - Hard drive encryption, file or archive encryption
  - Intrusion detection
  - Public-Key-Infrastructure, digital signature, smartcards
  - Authentication
  - ...

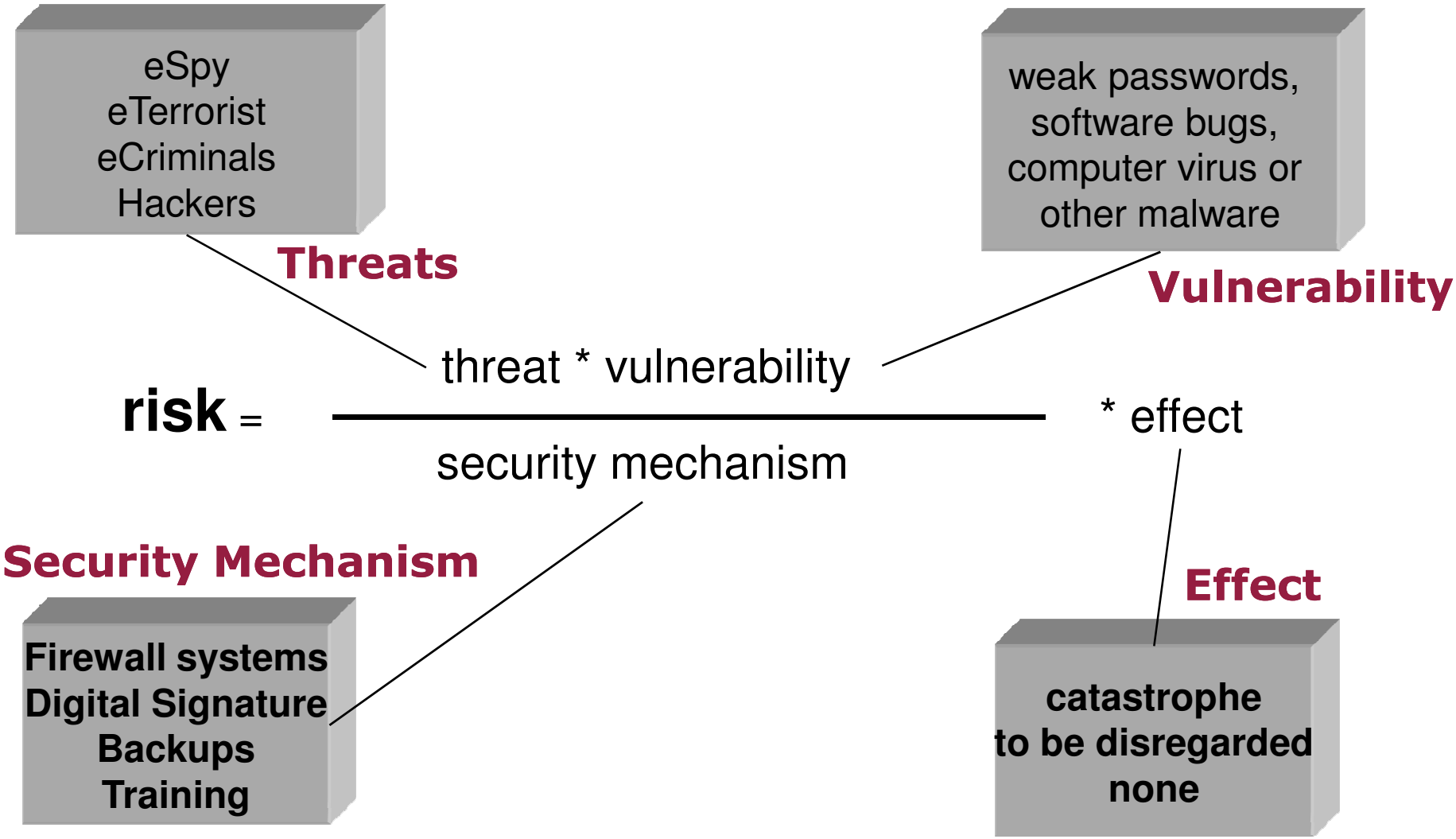
➔ but also non-technical security mechanism

  - Policies, awareness campaign, …

Correlation of cause and effect
→ Security risks

- Bugs in operating systems and applications
- Trap-Doors
  (security vulnerabilities that were intentionally build in by the developers)
- Conceptual vulnerabilities
- Wrong configuration
- Missing of needed IT security mechanism
- Users don't handle the existing security applications in the right way
- Users don't handle the existing IT opportunities and offers in a responsible manner (E-Mail addresses, …)
- …

Correlation of cause and effect
→ Risk that damage occurs

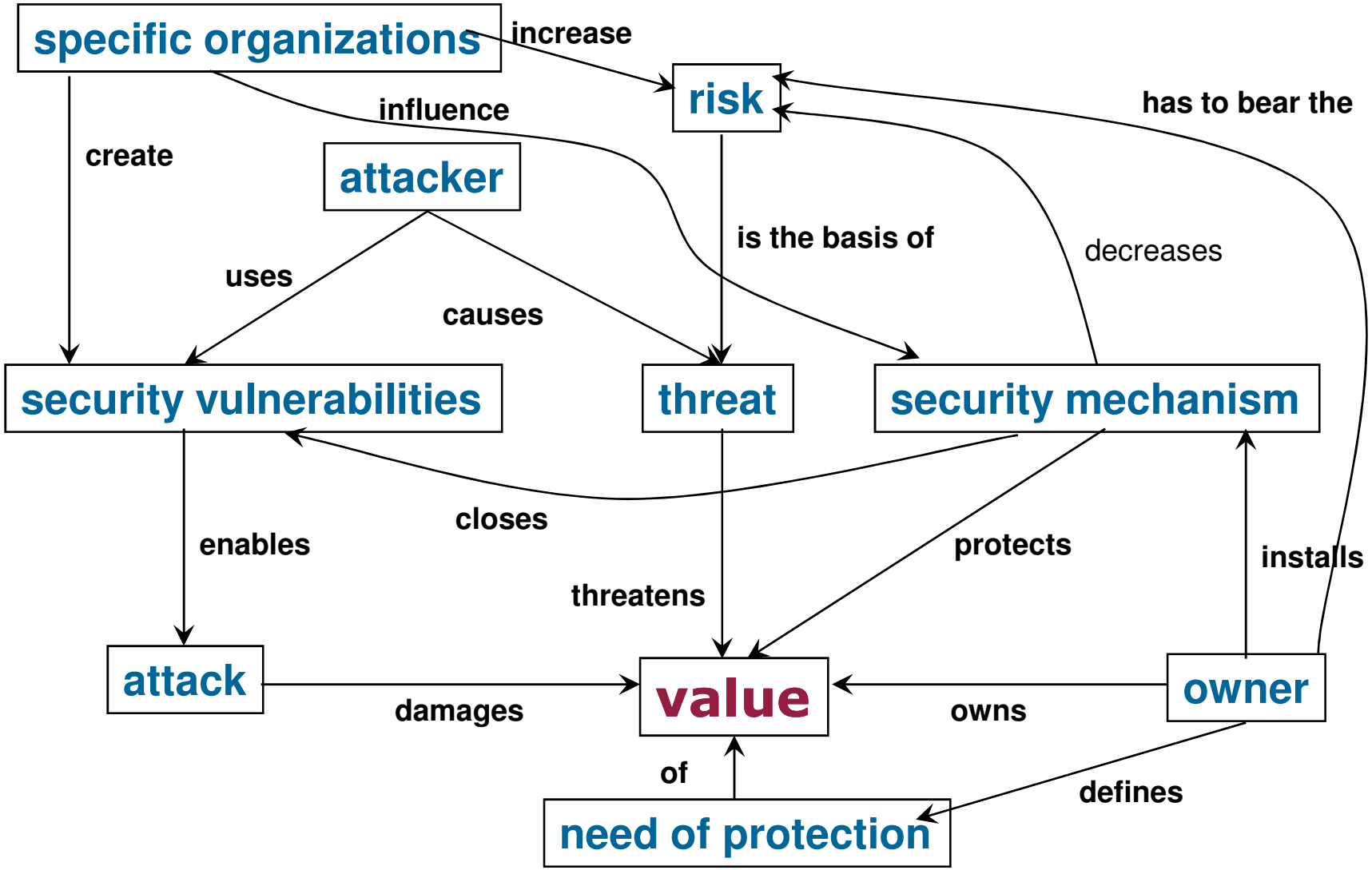


http://www.sans.org/infosecFAQ/securitybasics/risk.htm

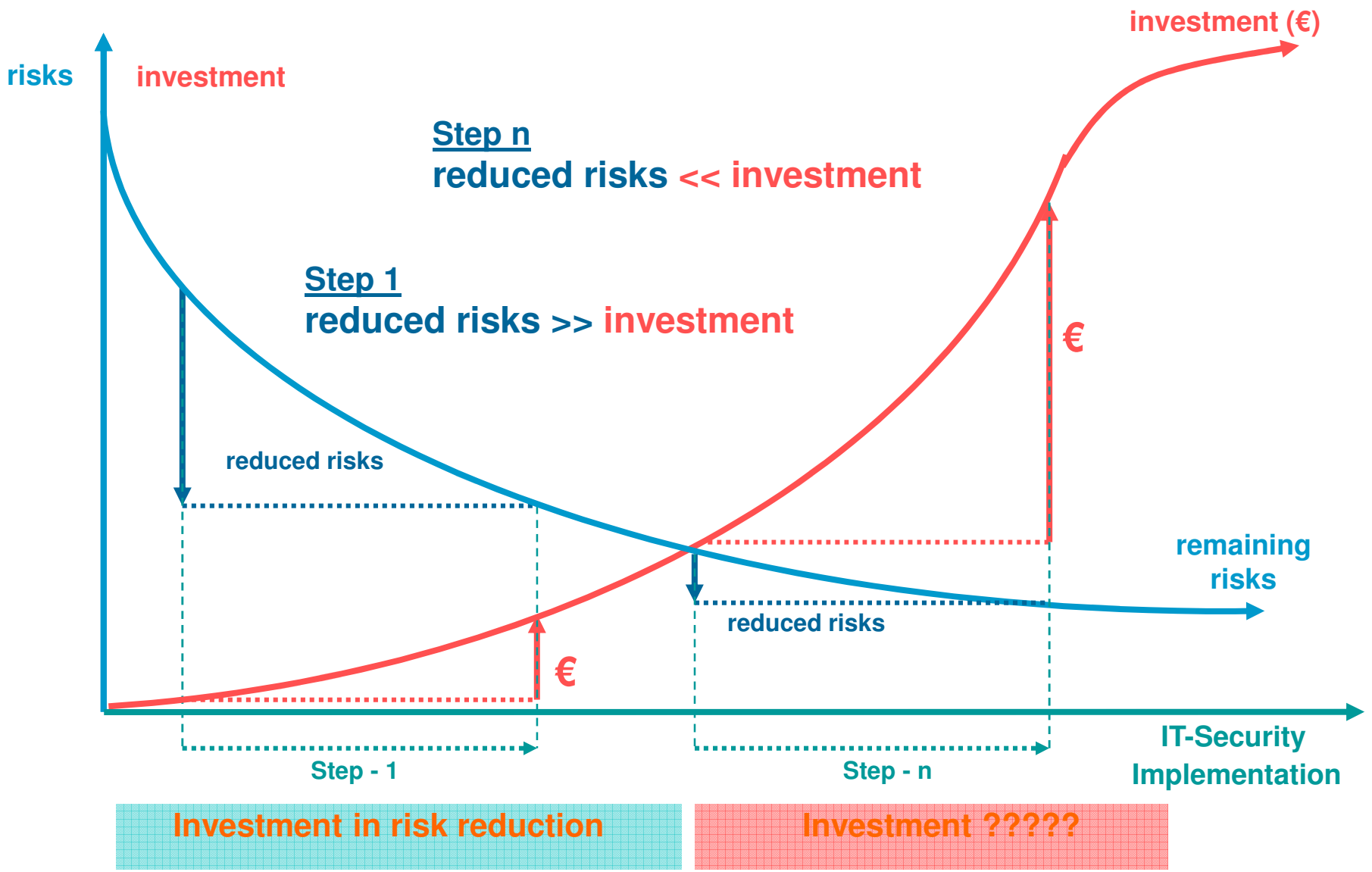
Correlation of cause and effect
→ Owner of values

- By attacking values the attackers also try to abuse the advantages of them and therefore they act against the owner of those values.
- The owner regards the attack as a reduction of his values – **as far as he notices the attack**
- The **owner is responsible** for the protection of his electronic values

IT security
→ As a correlation of effect and action



IT security risks & investment

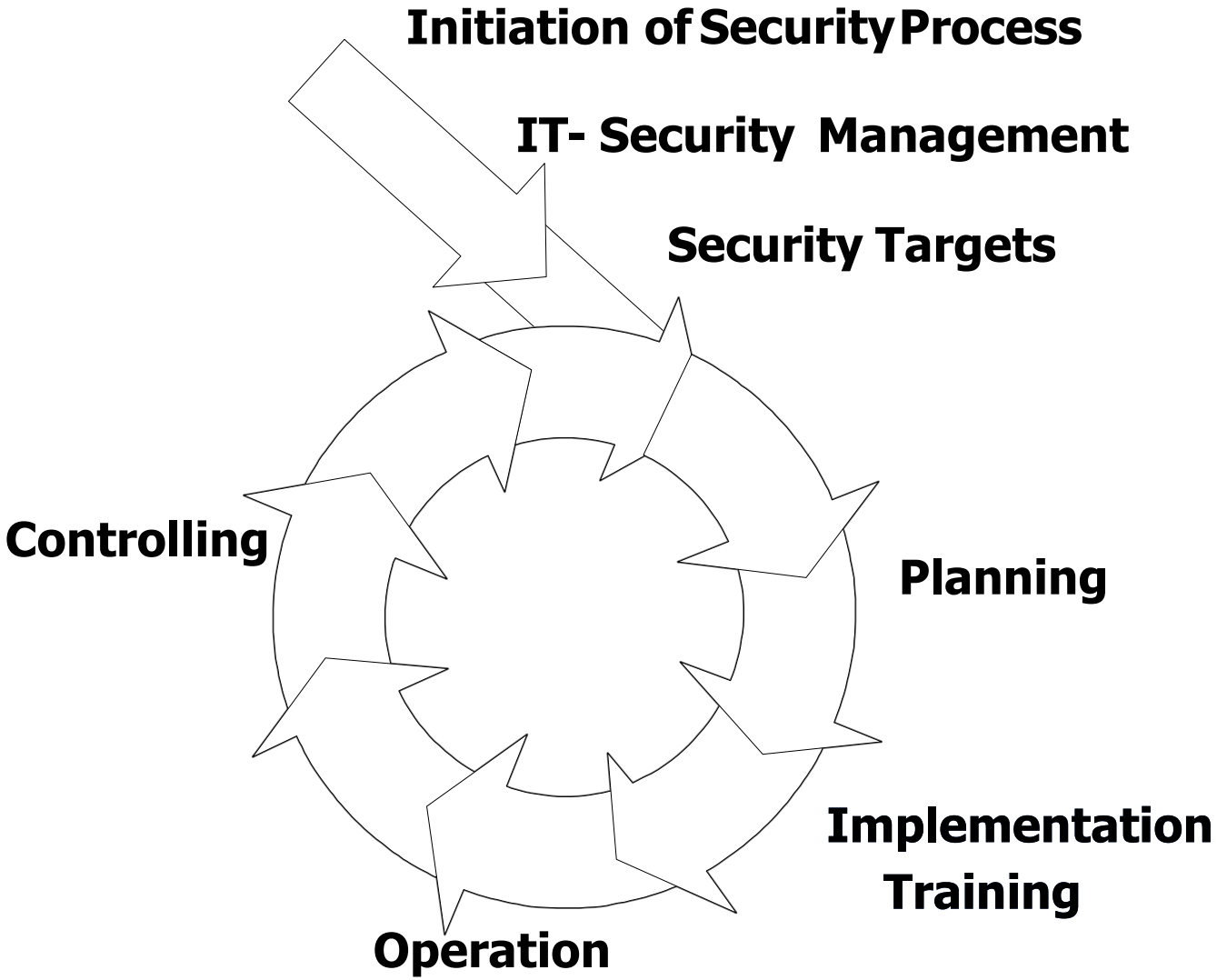


Baseline Security (fundamental security)

Pareto principle (**80-20 rule**, **Haddad's Theorem**,)
20% of the used security mechanisms enable a
80% protection against potential threats

- **In detail:**
  - by using the appropriate IT security mechanism
  - a reliable baseline security can be achieved
  - with small effort

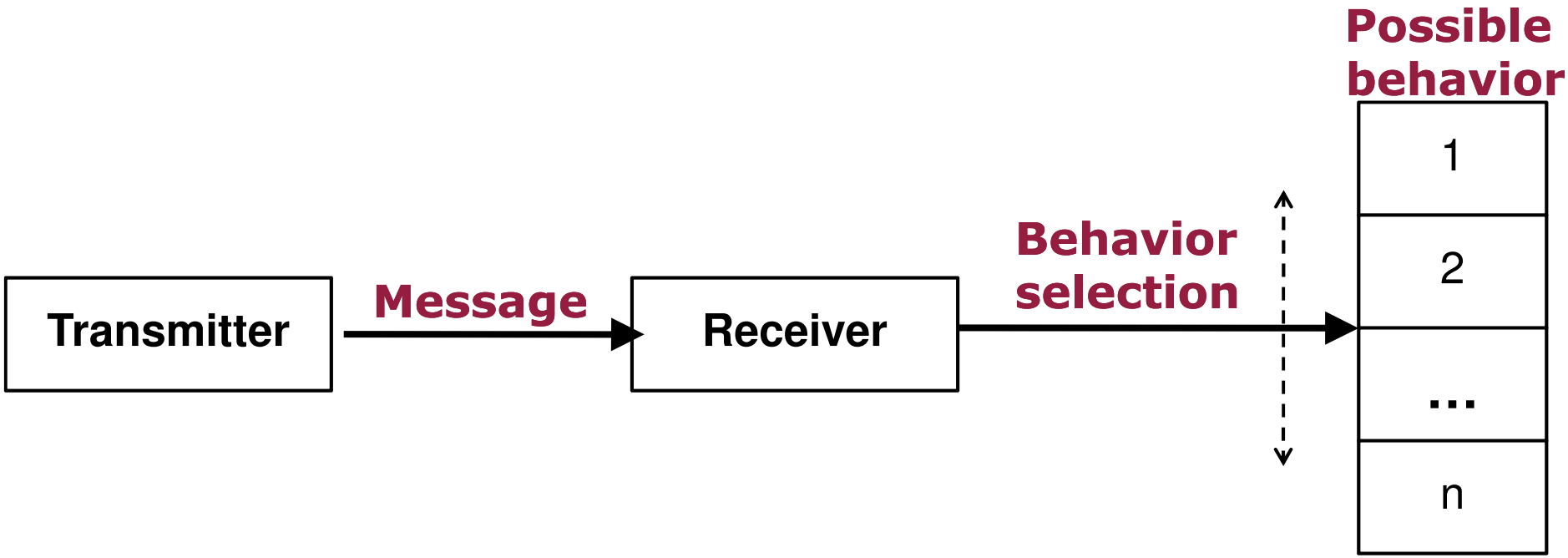
IT security management
→ IT security process



Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- Change of meaning in IT systems
- IT security as a correlation of effect and action
- **Possible threats in communication systems**
- Possible damage
- Security and trustworthiness
- Summary

Communication systems
→ Possible threats



Possible reactions by a receiver of a message

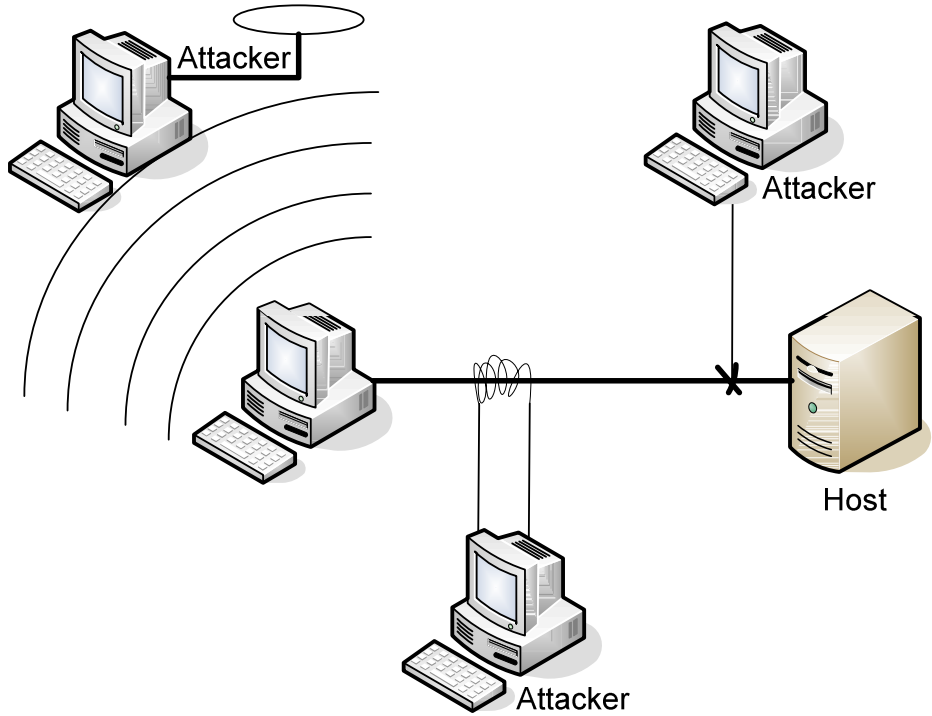
- An attacker is able to predict the recipients behavior (by tapping)
- The attacker may change the reaction/behavior of the recipient (by replaying, modifying or deleting the message)

Threats to communication systems
→ Passive attacks

Passive Attacks do not modify any transmitted messages nor do they make any changes to the operation of the communication system.

- **Interception of Data**
  The attacker acquires messages from the communication system and can abuse the data for his intentions.

- **Interception of User-Identities**
  The wire tapper gets to know which participants establish a data connection and share data with each other

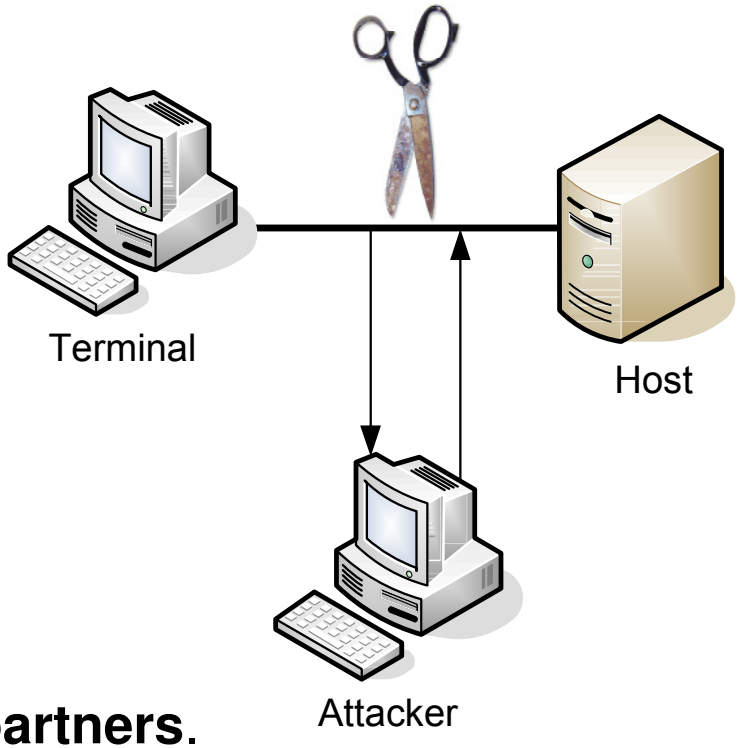


- **Traffic flow analyzing**
  Even when encryption is being used to secure messages from being intercepted, it is still possible for an attacker to gain useful information by analyzing the flow of traffic. Size, time, frequency and direction of messages can provide useful information.

Threats to communication systems
→ Active attacks (1/3)

Besides the danger of being tapped there are a couple of attack scenarios where the traffic flow and the communication system are being manipulated.

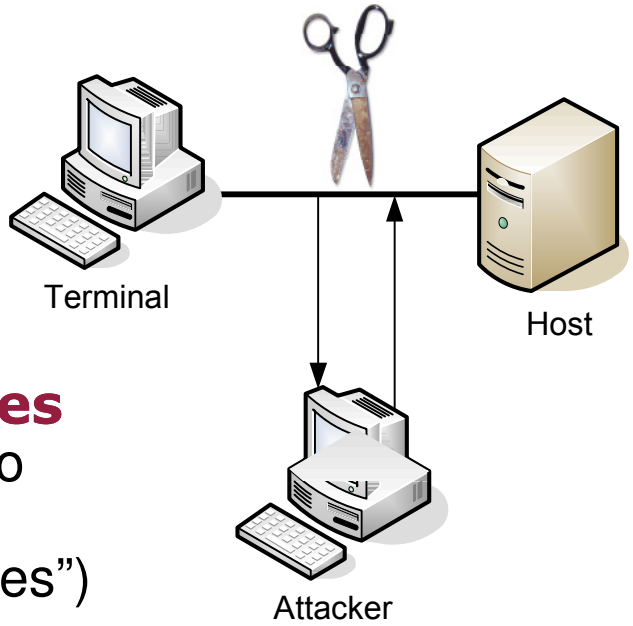
- Active attacks on the one hand **physically redirect all traffic** or on the other hand **emulate transfer protocols**.



- Active attacks can be divided roughly into two categories.
  - attacks **perpetrated by third parties**
  - attacks **performed by communication partners**.

Threats to communication systems
→ Active attacks (2/3)

Attacks performed by third party attacker



- **Repetition or delay of messages**
  In this form of attack, an aggressor records a message and replays it unchanged at a later time (e.g. multiple bank transfers)
- **Insertion and deletion of data in messages**
  To manipulate a system, an attacker inserts data into messages or deletes data from them.
  (e.g. email: “don’t buy new shares” in “buy new shares”)
- **Modifications of data in messages**
  This type of threat involves modification of data that is not detected by the communication partner (e.g. modification of bank account)
- **Denial of service / boycott**
  If the scope of data inserted or suppressed is too big the entire communication system can be blocked as a result.
- **Malware**
  Virus, Worms, Trojans, Spam, ...

Threats to communication systems
→ Active attacks (3/3)

Threat through the communication partner

- **Masquerading a false identity**
  Masquerading entails the assumption of a false identity by an aggressor. Thus, for example, he can obtain a false identity by spying out the user ID and password or by tampering with the sender field of a message or an address on the internet.

- **Unauthorized use of IT systems**
  Without mechanisms for the identification and authentication of users, any control over unauthorized use of IT systems is practically not possible.
  Even for IT systems which provide identification and authentication mechanisms in the form of user IDs and password verification, there is a risk of unauthorized use, if passwords and user IDs get disclosed.

- **Repudiation of a message**
  In any form of communication a communication partner can deny having received a message (repudiation of receipt).

Threats to communication systems
→ Opportunities for accidental Harm

- **Misrouting information**
  In Internet/Intranet routers, information can be misrouted, allowing it to fall into the hands of an outside party.

- **Transmission errors**
  Transmission errors can be caused by cross talk between neighboring channels or by dialing noise.

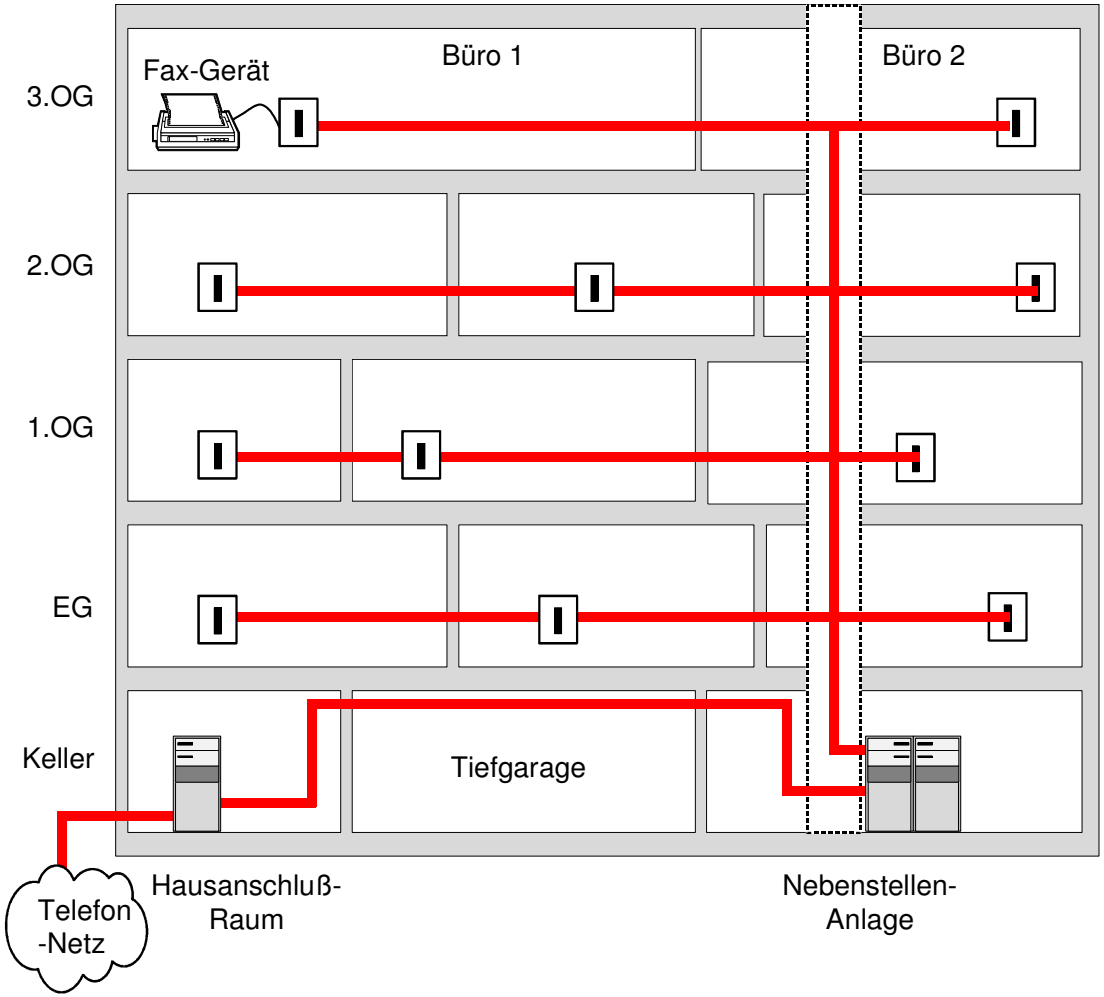
- **Software errors / bugs**
  It is in the nature of humans to make mistakes once in a while.

- **Hardware faults due to environmental influence**
  Environmental influences such as electromagnetic emissions can cause bit inversion in a computer system, which makes it behave incorrectly.

- **Human error**
  The user initiates actions he did not intend.

Possibility of an attack
→ Local circumstance could increase the risk

- The **motivation** for an attack **rises** with the **value of the transferred data**.
- Only **simple** and **cost efficient tools** are needed.
- Point of application:
  - neighbor offices
  - cable duct
  - room for service or house connections
  - interphone system
  - underground car park



very high

Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- Change of meaning in IT systems
- IT security as a correlation of effect and action
- Possible threats in communication systems
- **Possible damage**
- Security and trustworthiness
- Summary

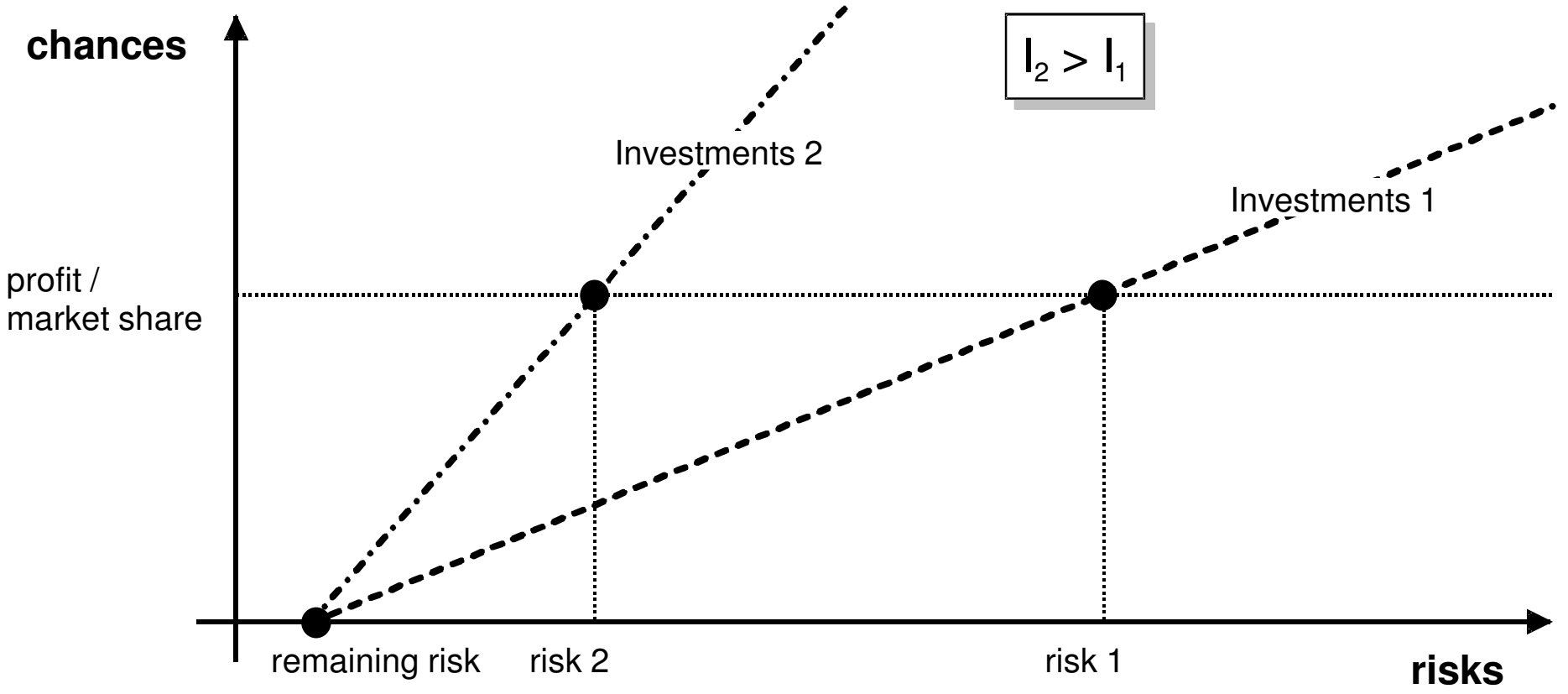
Possible damage
→ Overview

- **Violation of laws, regulations or contracts**
  Constitutional law, data privacy law, ...
- **Impairment of informational self-determination**
- **Physical injury**
  Injury or even death of individuals
- **Impaired performance of duties**
  Delayed processing, late or incorrect delivery, inadequate quality, …
- **Negative effects on external relationships (image loss)**
  Loss of reputation, loss of confidence, damage to business relations, …
- **Financial consequences (25.000,- $ up to 5 Mio. $)**
  Immediate and indirect financial losses

Possible damage
→ Protection need categories

Damage scenario	Description for category „Basic to moderate“	Description for category „High”	Description for category „Very High”
1. Violation of laws, regulations or contracts	- Violations of regulations and laws with minor consequences - Minor breaches of contract which attract little in the way of contractual penalties	- Violations of regulations and laws with major consequences - Major breaches of contract with high contractual penalties	- violation of fundamental regulations and laws - Breaches of contract with ruinous damage liabilities
2. Impairment of the right to informational self-determination	- Impairment of the right to informational self-determination would be assessed as tolerable by the individual. - Possible misuse of person related data has minimal effects on the social or financial standing of those concerned.	- Significant impairment of the individual's right to informational self-determination could be possible. - Possible misuse of person-related data would have considerable effects on the social or financial standing of those concerned.	- A particularly significant impairment of an individual's right to informational self-determination could be possible. - Possible misuse of person-related data would mean social or financial ruin for those concerned.
3. Physical injury	- Does not appear possible.	- Physical injury to an individual cannot be absolutely ruled out.	- Serious injury to an individual is possible. - Danger to life and limb.
4. Impaired performance of duties	- Impairment would be assessed as tolerable by those concerned. - The maximum acceptable down time is greater than 24 hours.	- Impairment of the performance of duties would be assessed as intolerable by some of the individuals concerned. - The maximum acceptable down time is between one and 24 hours.	- Impairment of the performance of duties would be assessed as unacceptable by all individuals concerned. - The maximum acceptable down time is less than one hour.
5. Negative effects on external relationships	- Minimal impairment of reputation / confidence, confined to within the agency/enterprise.	- Considerable impairment of reputation / confidence can be expected.	- A nation- or state-wide loss of reputation / confidence is conceivable, possibly even endangering the existence of the agencies/company.
6. Financial consequences	- The financial loss is acceptable to the agency/company/hospital. **(< 25.000 €)**	- The financial loss is considerable, but the agency/company/hospital can survive it. **(<5.000.000 €)**	- The agency/company/hospital may not be able to survive the financial loss. **(> 5.000.000 €)**

IT security
→ Reasonable investment



- IT Security means

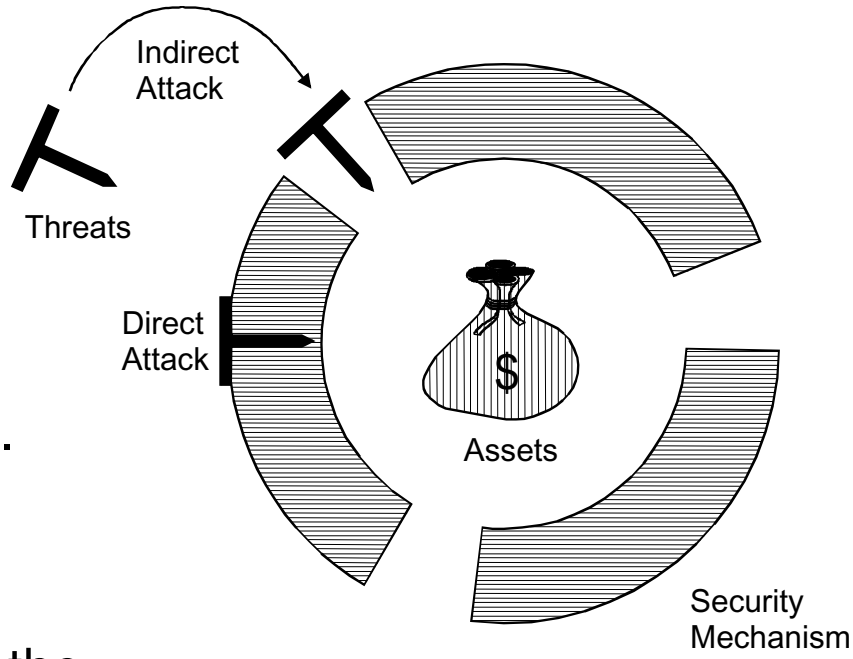
  ⇨ use opportunities + ⇨ reduce risks

Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- Change of meaning in IT systems
- IT security as a correlation of effect and action
- Possible threats in communication systems
- Possible damage
- **Security and trustworthiness**
- Summary

Security and trustworthiness
→ Effectiveness of security systems (1/2)

- One important aspect in evaluating the **effectiveness of security systems** is to decide whether the **security systems are suitable to handle a real attack** or not.
- The diagram shows the **assets** of an organization which needs to be protected against possible attack in the form of a **money bag filled with dollars**.
- The **threats** to which the system is exposed are represented as **nails** whose length is proportional power of the attacker.
- The **security mechanisms** used are represented as a **wall.**
- The thickness of this wall is proportional to the strength of the security mechanism.

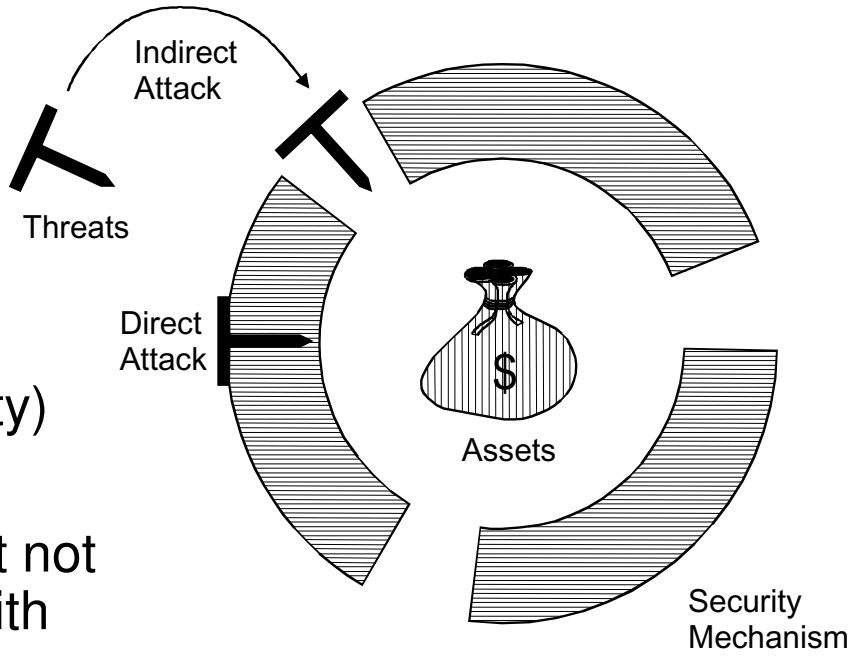


- **Security mechanism** are **secure** when the asset are **completely surrounded** by a wall and the wall is **at least as thick** as the length of the **longest nail**, even at is **weakest point**.

Security and trustworthiness
→ Effectiveness of security systems (2/2)

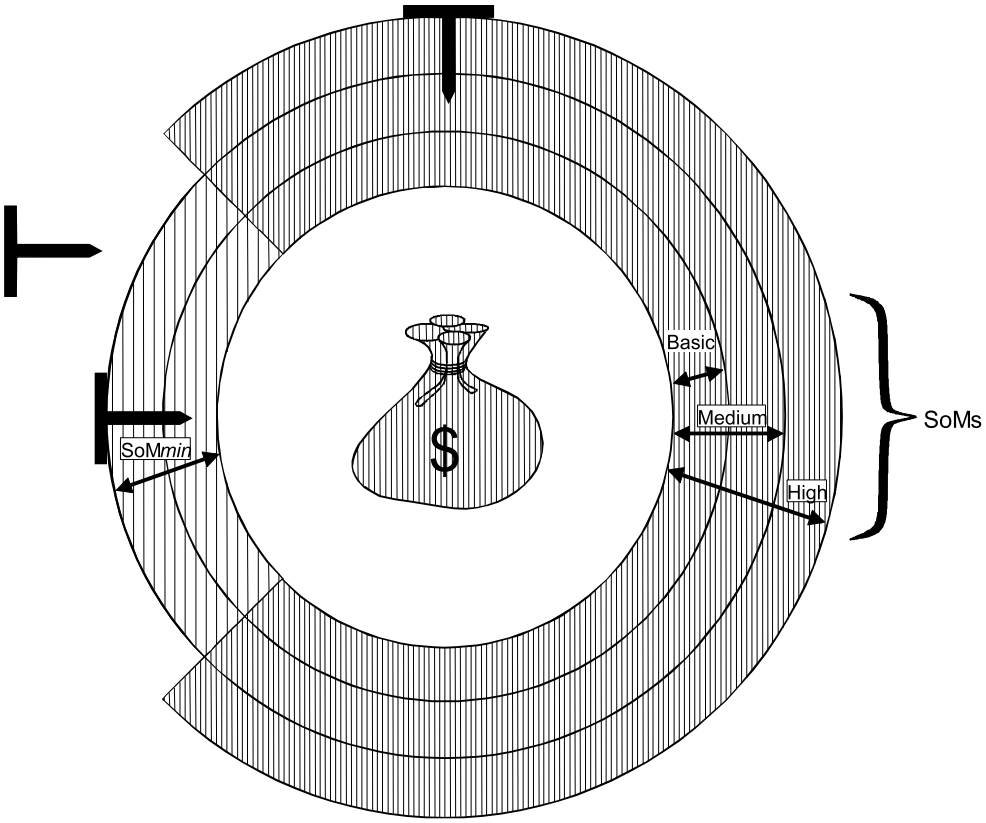
- However, it is possible for the security services to be inadequate even though their security mechanisms are actually strong enough.

- **Examples (indirect attack):**
  - Ability of an attacker, for example, to alter the access rights management module of the firewall system through the operation system used.
  - Use of IP forwarding (kernel functionality) from the outside.
    - So the firewall system is secure, but not the underlying operations system with its functions.



Security and trustworthiness
→ Strength of security mechanisms

- Another important aspect in evaluating security mechanisms is the strength of the security mechanism that is needed to successfully block all attacks.



These are the criteria to evaluate the strength:

- **technical know-how** (beginner, advanced, expert)
- **resources** (time, equipment)
- **situation** (together with user, together with administrator, …)

Security and trustworthiness
→ Correctness of security mechanisms

- Correctness of security mechanisms refers to whether the implemented security mechanisms
  - are **correctly implemented** and
  - to the **degree of assurance** provided by the implemented solution.

- **IT systems are only secure when**
  - **effectiveness**
  - **strength and**
  - **correctness**

  are adequately available!

Security and trustworthiness
→ Objectives of security mechanism

Security objectives when implementing security mechanism

- **1.** Elimination of all uncertainties with highest possible probability
  → **Good planning**

- **2.** Countering as many uncertainties as possible with appropriate security mechanisms in order to minimize the probability of loss and damage to a unimportant level
  → **Trusted Computing** (Anti-Malware, Firewall, VPN, ...)

- **3.** Recognition of weak points that cannot be eliminated in order to be able to react adequately in case of attack
  → **Early Warning System** (Spam-, Anti-Malware-LogData, ...)

- **4.** Recognition of attack attempts as early as possible in order to prevent loss and damage
  → **Early Warning System** (Intrusion Detection/Response, ...)

Security and trustworthiness
→ What does trustworthiness mean?

- **Security** means in our terms that we are able to use IT products and solutions with low-risk.
- **Reliance** in a way that producers, network and service operators provide a reliable and secure IT technology. That hasn't always been the case in the earlier days of the IT business.
- **Trustworthiness** means that IT products and solutions only behave in the desired way and this with 100 percent reliability.
- **Certainty** in a way that someone cares about security issues and other aspects of trustworthiness.
- **Authenticity** in a way that we believe in the promises that were made, regarding the improvement of IT security.
- More aspects of trustworthiness are e.g. sense of duty, preciseness and above all responsibility.

Security and trustworthiness
→ The basic trust principle

- We all understand trust, but what does it really mean?
- **Trust is an expectation of behavior**
- People use methods of trust instinctively, and most of us have never consciously thought about them!

Security and trustworthiness
→ Trust is …

- Something can be trusted if **it behaves** in an **expected manner** in **given circumstances.**
- All trust is ultimately derived from people (and hence organizations)
- Trusted behavior isn't necessarily desired (good) behavior!

Security and trustworthiness
→ What's necessary for trust?

- **It is safe to trust something** when
  - (it can be clearly identified)
  - **&** (it operates unhindered)
  - **&** ([the user has first hand experience of consistent, good, behavior] **or** [the user trusts someone who has provided references for consistent, good, behavior])

Security and trustworthiness
→ What's necessary for trust?

- **clear identification**
  - People need to recognize things in order to be able to trust them (we recognize a person's looks, voice and walk, for example)
  - "Trusted platforms" identify themselves (via cryptography) and the software in use (via measurements) - (see "Trusted Computing" lecture)

Security and trustworthiness
→ What's necessary for trust?

- **Unhindered operation**
  - A person might not behave normally if the environment is adversely affecting him (we check that people aren't ill and don't have guns pointed at them, for example)
  - "Trusted Platforms" isolate processes, because we don't know how to ensure that a process operates as implemented unless it is isolated from other processes (see "Trusted Computing" lecture)

Security and trustworthiness
→ What's necessary for trust?

- **References**
  - In the absence of personal experience, people need references in order to be able to trust something
  - "Trusted platforms" include references (attestation) for the platform and for the software that executes on the platform (see "Trusted Computing" lecture)

Content

- Aim and outcomes of this lecture
- Real World vs. Electronic World
- Change of meaning in IT systems
- IT security as a correlation of effect and action
- Possible threats in communication systems
- Possible damage
- Security and trustworthiness
- **Summary**

Information security - Introduction
→ Summary

- We live in **an information society** in which the role of IT is increasingly important.
- IT devices, IT processes and electronic values are **economic goods** that must be adequately protected and secured.
- The security of IT (all processes and electronic values) are under **responsibility of the owner**.
- The correlation of cause and effect of **IT security is highly complex** and needs a precise analysis and evaluation.
- The opportunities for attacks, the occurrence probability and the damages are multifaceted and therefore show the necessary need for action.
- This lecture is mainly about the build-up, the principles, the architecture and the functionality of technical IT security measures in the area of the Internet (electronic communication, services, applications, ...).

Fachhochschule Gelsenkirchen

Information Security

→ Introduction

Thank you for your attention!
Questions?

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
Gelsenkirchen University of Applied Sciences
http://www.internet-sicherheit.de

if(is) internet security.

Information security - Introduction
→ Literature

- [1] T. Crothers, N. Pohlmann “Firewall Architecture for the Enterprise”, Wiley Publishing, NY 2002

Links:

AiconViewer: http://www.internet-sicherheit.de/aiconviewer/