Advanced Aspects of Hospital Information Systems: IT Security in Healthcare

Florian Fankhauser, Michael Schafferer, Christian Schanes

INSO – Industrial Software
Institute of Computer Aided Automation | Faculty of Informatics | Vienna University of Technology

Agenda

ESSE: Short Introduction

IT Security in Healthcare

Definition of Security/Risk

IT Security Foundations

Risk Analysis

Security Concept

Privacy

Literature

Summary

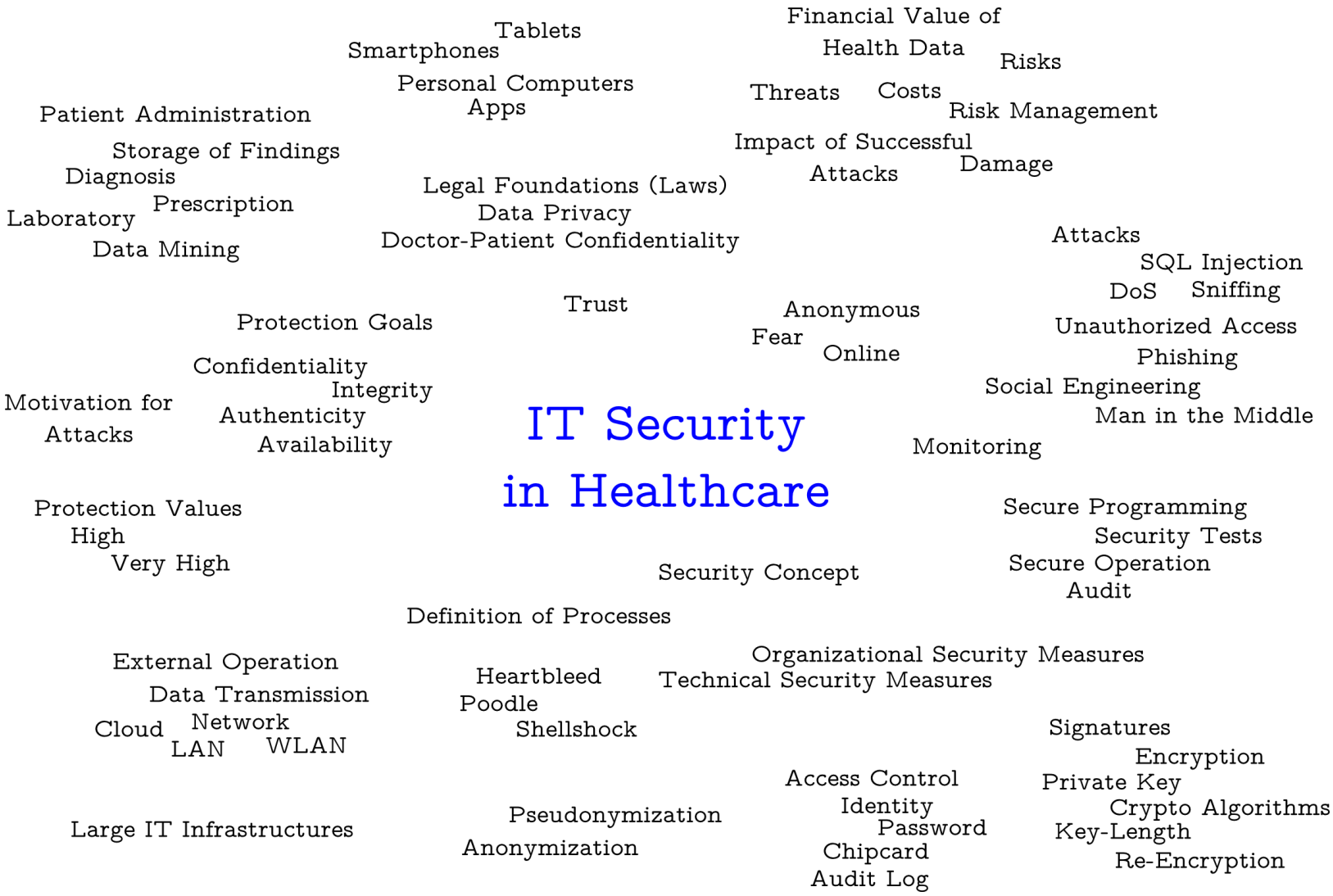
ESSE – Establishing Security

- IT Security is much too complex in order to teach it in 90 minutes :)
- Therefore, only selected topics today
- More ESSE lectures to deepen knowledge of IT Security
  - Introduction to Security *(WS, Bachelor)*
  - Security for Systems Engineering (CTF contest) *(SS, Bachelor)*
  - Advanced Security for Systems Engineering *(WS, Master)*
  - IT Security in Large IT Infrastructures (CTF contest) *(SS, Master)*
  - Seminar aus Security
  - Projects
  - Bachelor thesis, master thesis, thesis

IT in Healthcare

Tag Cloud IT Security in Healthcare

Tag Cloud IT Security in Healthcare



Case Example: Manipulation of Medical Devices at DeepSec 2013

- Live manipulation of a patient monitor
- Despite patient being dead, patient monitor shows normal vital parameters
- A way was found to get into the communication process and send information to the patient monitor system

- Man in the Middle (MitM)
- Vulnerabilities
  - Unencrypted Communication
  - Missing (client) Authentication

(See `http://futurezone.at/science/medizingeraete-lassen-sich-leicht-hacken/37.040.304`)

Definition Security/Risk

- Merriam-Webster Online Dictionary: *the quality or state of being secure: as a: freedom from danger*
- This means: There are no risks
- We know: There is nothing like 100% security
- Therefore, we have to
  - Find and measure the risks
  - Define a limit for acceptable risks
  - Eliminate all risks that are greater than the acceptable risk
- Risk = expected loss when a specific threat occurs $*$ probability of this specific threat

(See DIN VDE 31000)

Recap: Basic Protection Values

- Confidentiality
  - Access of data only for authorized persons
  - Avoid data theft
- Integrity
  - Unauthorized manipulation must be detectable
- Availability

(See Bundesamt fuer Sicherheit in der Informationstechnik (2005))

Recap: More Basic Protection Values

- Authenticity
  - Unambiguous link to an identity
- Non-Deniability
  - e.g., Digital Signature
- $\rightarrow$ Depending on the project more protection values can be defined

(See Bundesamt fuer Sicherheit in der Informationstechnik (2005))

Recap: IT Security Levels/Protection Needs Determination

- Most of the time the importance of data/components can't be exactly estimated
- Therefore, IT Security Levels got introduced

- Levels can be among others
  - small
  - normal
  - high
  - very high
  - normal
  - high
  - very high

Recap: Threat Level of Attackers

- Depending on multiple factors
  - Skill Level/Know How
    (Script Kiddies, *"hackers"*, white/black hat, crackers, staff,...)
  - Budget
  - Time
  - ...
- Medical data are (financially) valuable
  - $\rightarrow$ Threat potential is big

Motivation of Attackers/Implications of Attacks

- Financial Value of Medical Data
- Blackmail

- Financial Implications
  - Organization
  - Persons affected
- Social Implications

EN ISO 14971: Risk Management in Healthcare

- Application of risk management to medical devices
- Procedure by which a manufacturer can
  - identify threats,
  - estimate risks,
  - evaluate risks,
  - control risks,
  - monitor the effectiveness of the control.
- Applicable to all stages of the life cycle of a medical device

(See EN ISO 14971)

General Requirements for Risk Management

- Risk management process
- Management process
- Qualification of personnel
- Risk management plan
- Risk management file

Risk Analysis

- Risk analysis procedure must be established and conducted
- Identification and description of medical device regarding the safety of the device
- Identification of known or foreseeable threats
- Risk analysis
  - Different techniques are used
- Risk control
- (Overall) Residual risk evaluation
- Monitoring of the device during use
- Documentation of the process

Security Concept

- Details for security of medical device need to be documented
- $\rightarrow$ *Security Concept*

- Risk analysis
- Security requirements
- Technical measures
- Organizational measures
- Effectiveness analysis

Goals of a Security Concept

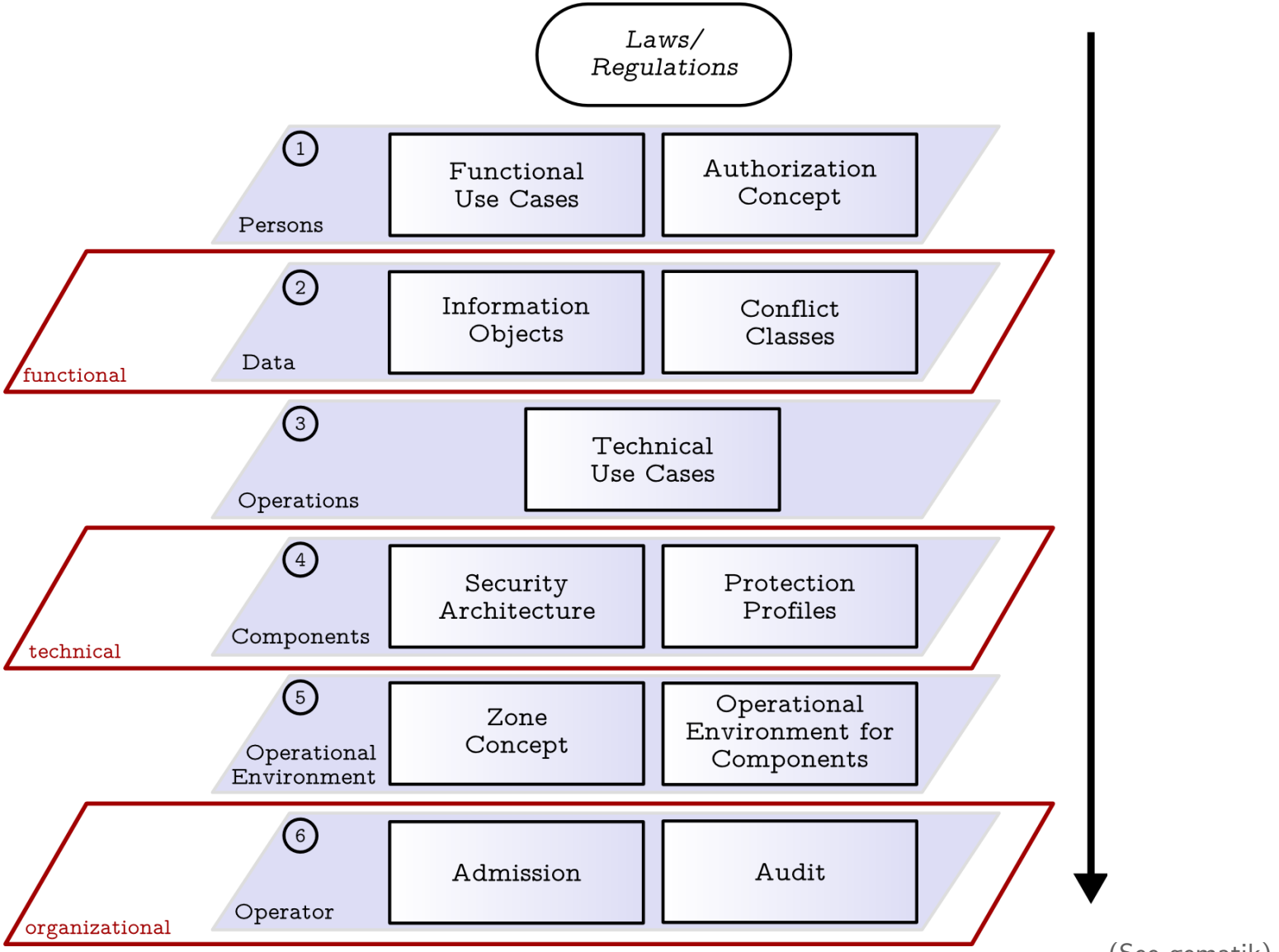
- Definition of framework conditions for...
  - Architecture
  - Functional services
  - Operators
  - ...
- Definition of all relevant security aspects of a project

Case Example: General Security Concept in German Health Infrastructure

There are many sections, among them are

- Privacy concept
- Authorization concept
- Cryptography concept (key management!)
- Zone concept
- Logging concept
- Protection needs determination
- Operating requirements, policies
- Requirements for specific security concepts
- Residual risk analysis

IT Security at Different Levels



(See gematik)

Different Aspects of a Security Concept

- Define information objects
  - Required basic protection values of objects (e.g. integrity, confidentiality,...)
- Conflict classes
  - Objects that are not allowed to be stored within one storage area
- Authorization concept
  - Roles for the system
  - Rights of roles to information objects
- Builds the base for a further design, e.g., for technical concepts

Privacy as Basis for Security Requirements

- *Doctor-patient confidentiality* as *trust principle* for treatments!
- *Data privacy* as *basis* for eHealth!
- $\rightarrow$ legal consequences!
- Operation of IT systems by external contractors (see, e.g., Biewald)
  - Doctor-patient confidentiality?
  - Anonymization, Pseudonymization
  - Encryption
  - Errors, Error Analysis?
- Deduction of organizational and technical security measures

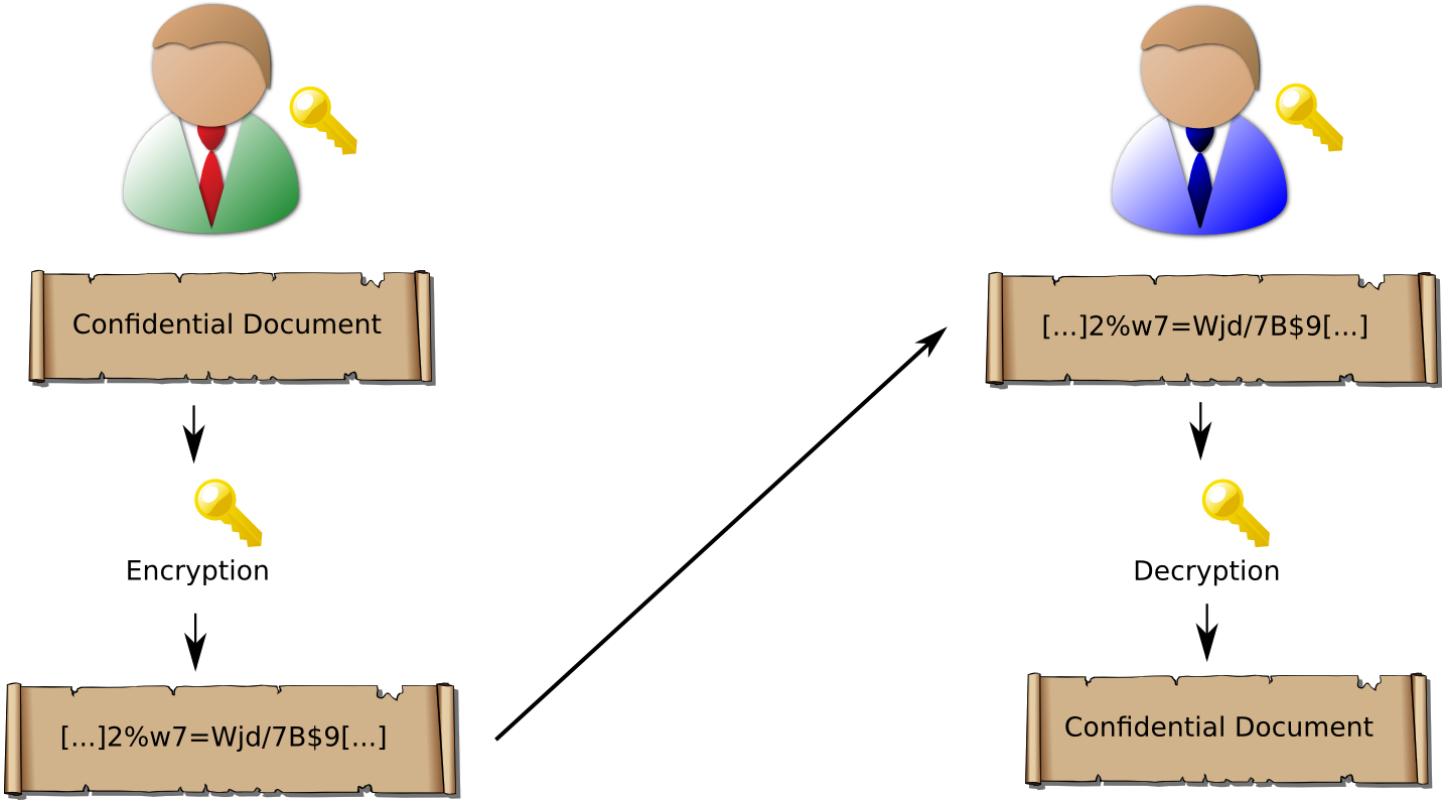
Data Privacy Principles of the eGK

- Assured can decide what is done with her data
- Voluntariness of the usage
- Transfer and deletion of data
- Transfer of data to citizens
- Right of information about data and right to read data
- Usual data privacy rights (data may only be used for specified purpose, only minimally needed data may be stored etc.)

Logging

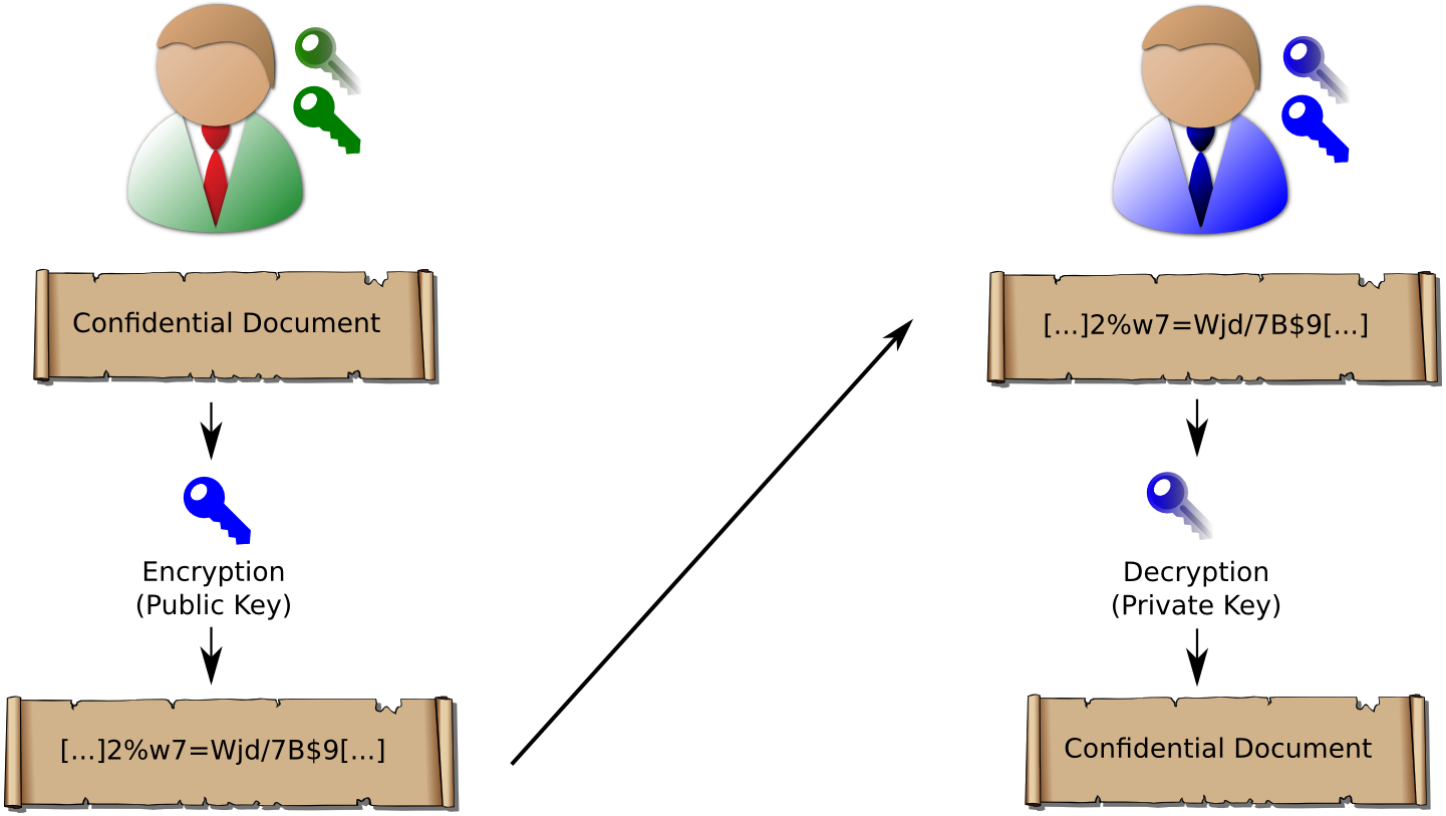
- Audit Server
- Each access to sensitive data must be logged
  - *Who* accessed
  - *what* information
  - *when*?
- Independent on whether the access was successful or unsuccessful
- Patient may read the protocols

Recap: Symmetric Cryptography



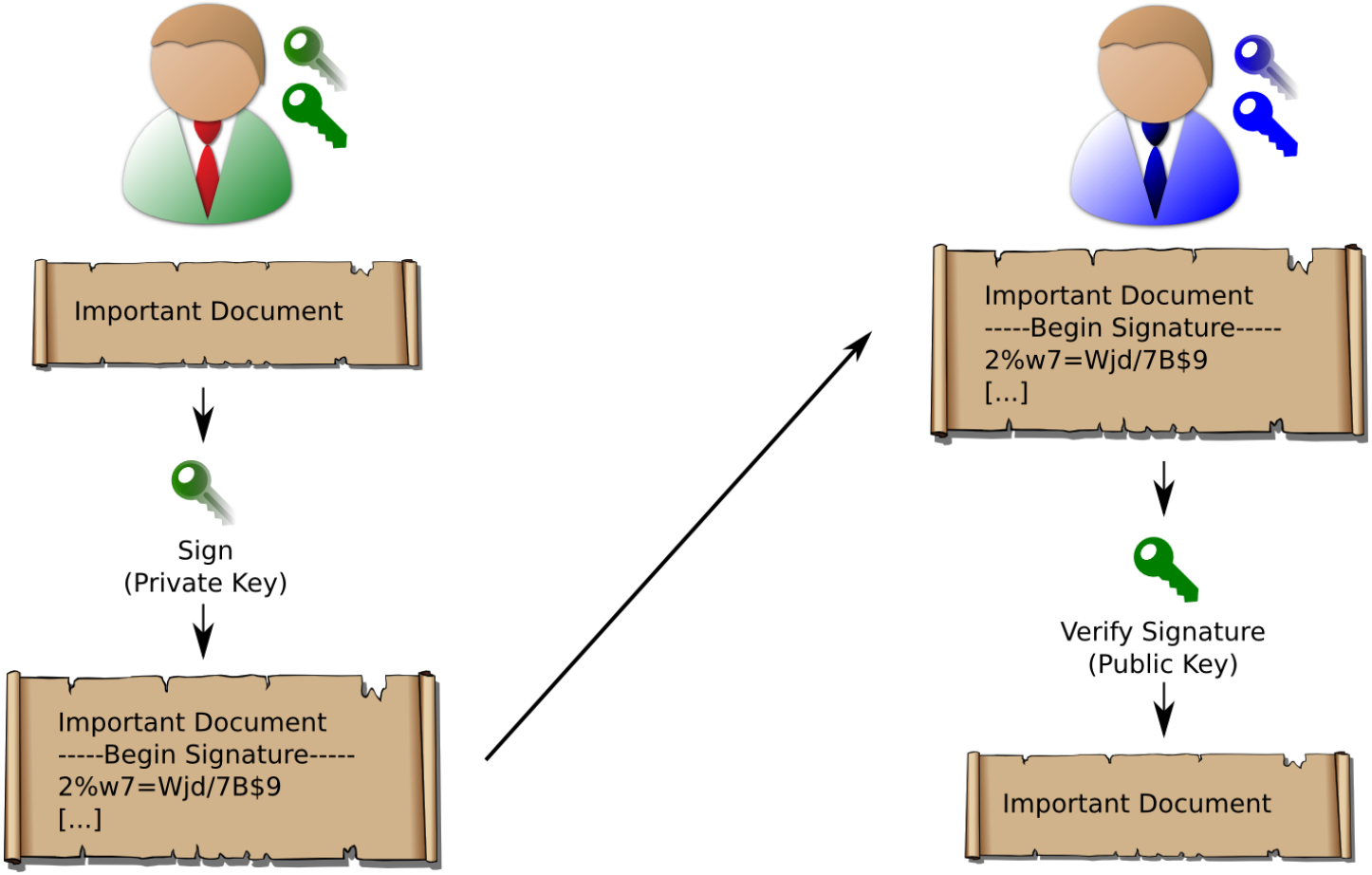
- Examples: Data Encryption Standard (DES), Triple-DES (3DES), Advanced Encryption Standard (AES)
- One problem is the key exchange when there are many participants

Recap: Asymmetric Cryptography: Encryption



- Examples: Rivest-Shamir-Adleman (RSA), ElGamal

Recap: Asymmetric Cryptography: Signature



Basics of Cryptography

- Encryption
- Signature

- Cryptography is complex $\rightarrow$ Complexity is the worst enemy of Security (B. Schneier)
- Aging of crypto algorithms/key lengths
  - Attacker can decrypt data without the knowlegde of the private key (e.g., using brute force attacks)
  - Periodically newly encrypt data with currently secure algorithm/key length

Availability Aspects of Cryptography

- Loss of the private key means loss of encrypted data
- Backup of the private key necessary $\rightarrow$ additional organizational measures needed
  - Key Escrow/Key Recovery
- If private key is only used for signatures $\rightarrow$ no backup necessary

Anonymization

- Status of non-identifiability within a set of subjects/persons called anonymity set
- Loss of information

- Useful for, e.g.,
  - Research
  - Statistical evaluations

Pseudonymization

- A pseudonym is a label that associates a data record with an unambiguous person without disclosing information about the person's identity
- In contrast to an anonymization there exists a location where the association of pseudonym and the person's identity is done!
- Data related to one case can be collected – even from different sources and over time
- Feedback to the patient is possible after depseudonymization

(See Pommerening et al.)

Examples for Attacks on Anonymization/Pseudonymization

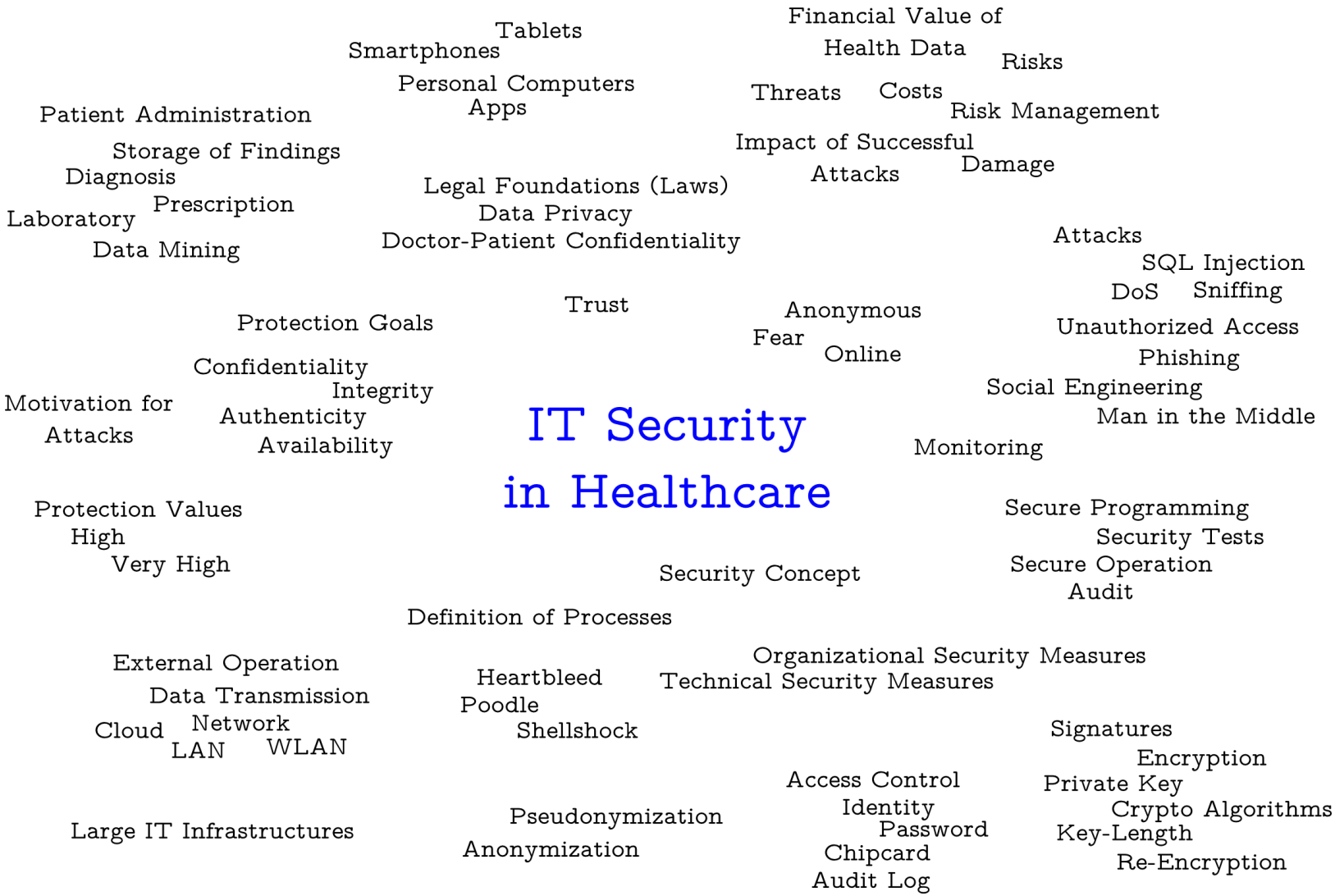
- Homogeneity attack
- Background knowledge attack

Input Validation as a Mechanism Against Many IT Security Attacks

- SQL Injection
- Command Injection
- Cross Site Scripting (XSS)
- Lightweight Directory Access Protocol (LDAP)
- Buffer Overflows
- Redirection Errors
- ...

- *Correct implementing* Input Validation *helps!*

Tag Cloud IT Security in Healthcare



Literature 1/5

- Florian Fankhauser, Christian Schanes, and Christian Brem. Sicherheit in der softwareentwicklung. In *Softwaretechnik - Mit Fallbeispielen aus realen Entwicklungsprojekten*, chapter 13, pages 589–646. Pearson Studium, München, 1 edition, 2009. `http://www.inso.tuwien.ac.at/publications/softwaretechnik/`
- Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World.* Wiley Publishing, Inc., Indianapolis, Indiana, 2004. ISBN 0-471-45380-3
- Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems*. Wiley Publishing, Inc., 2 edition, 2008. ISBN 978-0-470-06852-6. `http://www.cl.cam.ac.uk/~rja14/book.html`

Literature 2/5

- Hans-Joachim Menzel. Informationssysteme in krankenhaus und praxis und die selbstbestimmung des patienten. *Datenschutz und Datensicherheit - DuD*, 35:853–858, 2011. ISSN 1614-0702. doi: 10.1007/s11623-011-0201-0. 10.1007/s11623-011-0201-0
- Marco Biewald. Externe dienstleister im krankenhaus und ärztliche schweigepflicht — eine rechtliche unsicherheit. *Datenschutz und Datensicherheit - DuD*, 35:867–869, 2011. ISSN 1614-0702. doi: 10.1007/s11623-011-0203-y. 10.1007/s11623-011-0203-y
- Ralph Herkenhöner, Harald Fischer, and Hermann de Meer. Outsourcing im pflegedienst. *Datenschutz und Datensicherheit - DuD*, 35:870–874, 2011. ISSN 1614-0702. doi: 10.1007/s11623-011-0204-x. 10.1007/s11623-011-0204-x

Literature 3/5

- Klaus Pommerening, Michael Reng, Peter Debold, and Sebastian Semler. Pseudonymisierung in der medizinischen forschung – das generische tmf-datenschutzkonzept. *Biometrie und Epidemiologie*, 2005. ISSN 1860-9171
- Manuel Koch, Sven Marx, and Arno Elmer. Informationelle selbstbestimmung und patientensouveränität in einem vernetzten gesundheitswesen. *Datenschutz und Datensicherheit - DuD*, 37(3): 131–136, 2013. ISSN 1614-0702. doi: 10.1007/s11623-013-0048-7
- Wei Liu and Eun Kyo Park. e-healthcare security solution framework. In *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, July 2012. doi: 10.1109/ICCCN.2012.6289239

Literature 4/5

- Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, August 2010. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.p v0.34
- Klaus Pommerening, Michael Reng, Peter Debold, and Sebastian Semler. Pseudonymisierung in der medizinischen forschung – das generische tmf-datenschutzkonzept. *Biometrie und Epidemiologie*, 2005. ISSN 1860-9171
- Klaus Pommerening. Datenschutz in krankenhausinformationssystemen. In *VIS'95*, 1995

Literature 5/5

- CWE und SANS: TOP 25 Most Dangerous Programming Errors
- OWASP: Top Ten Web Vulnerabilities

Summary

- IT security and privacy are vital cornerstones for eHealth
- Legal requirements
- Risk analysis
- Security concept
- Examples for technical security measures
- Unfortunately (?), organizational security measures are required as well

- Only selected aspects of IT security today
- Visit more ESSE lectures :-)

Thank you!

Florian Fankhauser, ESSE – Establishing Security

esse@inso.tuwien.ac.at

http://security.inso.tuwien.ac.at/

INSO – Industrial Software

Institute of Computer Aided Automation | Faculty of Informatics | Vienna University of Technology