eHealth ….. How to trust a cloud?

Enabling trust in distributed eHealth applications

Dr. Mario Drobics
Thematic Coordinator
Safety & Security Department
AIT Austrian Institute of Technology GmbH
mario.drobics@ait.ac.at
+43 50 550 4810

http://www.ait.ac.at/ehealth

AUSTRIAN INSTITUTE OF TECHNOLOGY

Overview

1. Specifics of eHealth applications in the cloud
2. Enabling trust in distributed eHealth environments
3. IHE as a framework for enabling trust
4. Open issues & outlook

AUSTRIAN INSTITUTE OF TECHNOLOGY

Distinctive Feature of Distributed/Cloud Applications

- Not all tasks can be secured using cryptography (e.g. access control, decision-making)
- Additional interface and areas of attack (e.g. administration interfaces, virtual networks, account management)
- Legal restrictions when hosting medical data in foreign countries
- Legal construction of subcontractors not very transparent
- Security policies hard to audit

⇒ **High level of trust to the provider necessary**

Distinctive Features of eHealth Application

- Processed data is very sensitive
  - Highly personal data
  - Potentially large number of effected persons
- High number of active users and (geographically) distributed nodes and sub-networks
- Specific use-cases (i.e. user might need to provide approval for data access)
- Need to access data in case of (personal & technical) emergency

⇒ **Standard approaches are not directly applicable**

Challenges for eHealth Applications

- Local nodes have highly varying security levels (clinics, surgeries, laboratories, etc.)
- Distribution of nodes hinders physical protection

⇒ **Take-over of (privileged) nodes not preventable**

Legal framework for eHealth Applications

- European Level
  - ENISA (Directive 2013/40/EU)
  - Patients' Rights in Cross-border Healthcare (Directive 2011/24/EU)
  - Protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC)
  - Protection of individuals with regard to the processing of personal data (Regulation (EC) No. 45/200)
  - etc.
- National Level
  - E.g. data privacy laws, EHR related laws, …

Reasons for establishing eHealth Services in the Cloud

- Scalability of the service
- Providing centralized data storage in the cloud
  - Geo-redundancy is easier to establish
  - Easier to operate and more cost-efficient
- Provide Software as a Service
  - Homogeneous level of security
  - Cost reduction due to centralized maintenance

AUSTRIAN INSTITUTE OF TECHNOLOGY

Vulnerability to Attacks

Currently, only few attacks with sever impact to system or user data known to the public

- No underlying business-model
- High degree of penalty if critical infrastructures are attacked
- Low acceptance of these attacks in the community

This might change …

- Social or military conflicts, terrorism
- Unspecific attacks to cloud services might also infringe eHealth applications
- Increasing use of mobile devices and wireless communication

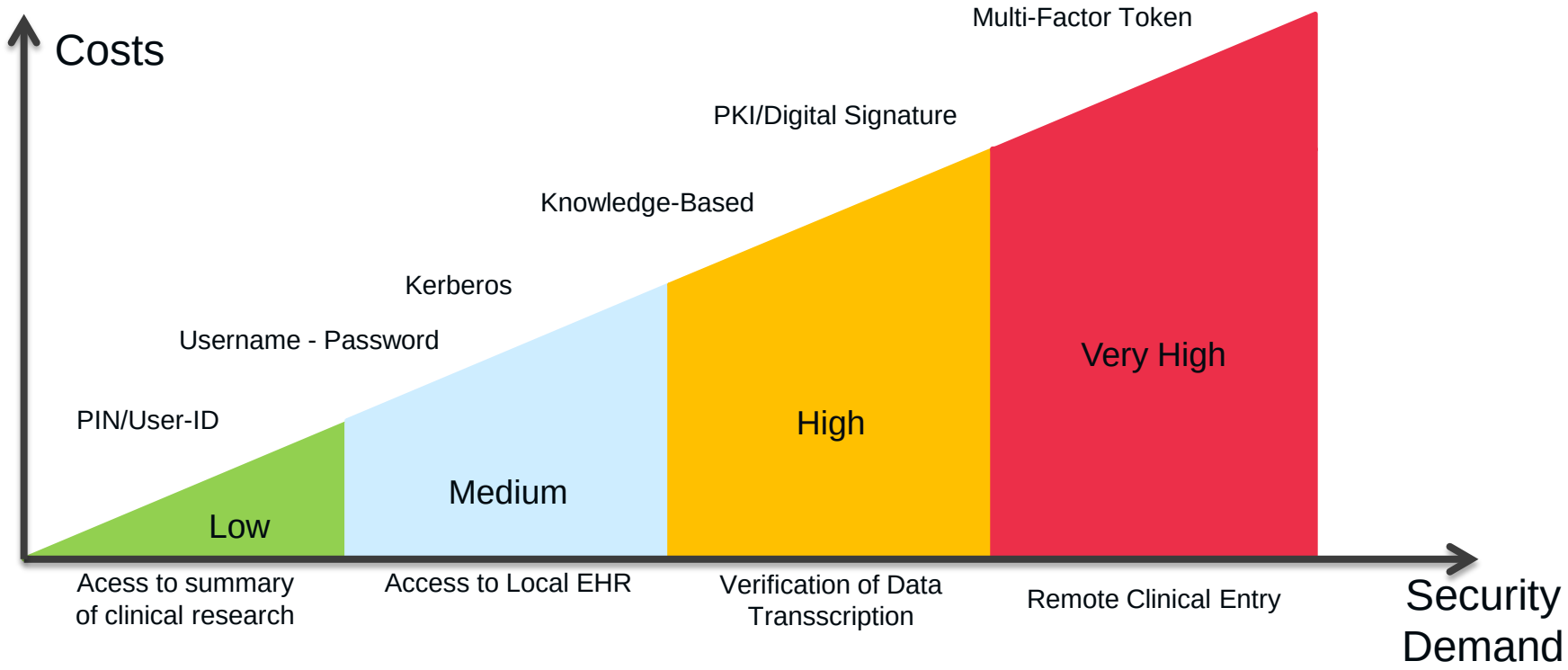
AUSTRIAN INSTITUTE OF TECHNOLOGY

Ensuring Security By Design

- Compromise of nodes in large-scale networks is inevitable
- System design should limit effects of compromise
  - **Via cryptography**
    Prevent forgery of data by using appropriate algorithms and transactions (e.g.. „bearer" vs "holder-of-key" model)
  - **Via system-policies**
    Limit the amount of data retrievable by attacker, e.g. by limiting the access rights or the number of requests the attacker could perform.
  - **Via security systems**
    IDS (Intrusion Detection Systems) may detect anomalies from the outside, even when attacker uses correct authentication.

Enabling trust in (healthcare) networks

- Authentication of users (role-based access)
- Authentication of nodes
- Authentication of transactions



Security Concepts for Cloud Services

- Encrypted data transfer
  - \+ Easy to set-up
  - \+ High transaction security
  - \- Intrusion to data storage critical
- Separate (virtual) networks
  - \+ Fraud detection on network level easy to set-up
  - \+ Requires similar level of trust throughout the network
- Encrypted data transfer & storage
  - \+ High security
  - \+ Full access control to data
  - \+ Supports distributed storage
  - \- Access to emergency data difficult

Security Concepts for Cloud Services

Encrypted data transfer & storage

- Data is de- / encrypted at the client
- High level of control can be established
  (e.g. access only with personal eCard)
- Homomorphic encryption supports limited computations on encrypted data
- Enables “need-to-know” principle

IHE – Integrating the Healthcare Enterprise

- Non-profit organization aiming to improve interoperability
- Provides interoperability-profiles based on use-cases
- Defines how established standards (e.g. HL7, DICOM) should be applied to these use-case
- IHE specifies
  - How to enable interoperability
  - Protect that interoperability mechanism from security risks
  - NO security policies

IHE Profiles mapped to Security & Privacy Controls

IHE Profile / Security & Privacy Controls	Profile Issued	Audit Log	Identification and Authentication	Data Access Control	Secrecy	Data Integrity	Non-Repudiation	Patient Privacy
Audit Trails and Node Authentication	2004	✓	✓	✓	✓	✓	✓	✓
Consistent Time	2003	✓	•				✓	
Enterprise User Authentication	2003		✓	•			•	•
Cross-Enterprise User Assertion	2006		✓	•			•	•
Basic Patient Privacy Consents	2006			•				✓
Personnel White Pages	2004		✓	✓			•	
Healthcare Provider Directory	2010		✓	•			•	
Document Digital Signature	2005		✓			✓	✓	
Document Encryption	2011			✓	✓	•		

IHE Summary

- IHE does not support „encryption on storage“

  i.e. encrypted cloud-storage has to be set-up „outside“ of IHE
- IHE design not optimized for cloud-infrastructures

  (e.g. need-to-know principle not considered)
- Limitations in trans-organizational / -national infrastructures

⇒ Separate solutions necessary to guaranty security if not all nodes are perfectly trustworthy

Outlook

- Cloud services need to adopt to eHealth requirements
  - Establish relationship of trust between heath care and cloud service provider
    - Ensure privacy and confidentiality of hosted data
    - Transparent handling of data and policies
    - Ensure long-term availability & security of the data
  - Support eHealth standards
  - Confirm to (inter-) national laws

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Your Ingenious Partner!

Dr. Mario Drobics
Thematic Coordinator
Safety & Security Department
AIT Austrian Institute of Technology GmbH
mario.drobics@ait.ac.at
+43 50 550 4810

http://www.ait.ac.at/ehealth