Data Security and Data Protection in Medical Research Networks

Klaus Pommerening
Johannes-Gutenberg-Universität
Mainz
18. October 2000

Aspects of Data Protection

- Requirements:
  - Access to patient data only in treatment context
  - Research with anonymous/pseudonymous data
- Challenges:
  - Big data collections, matching, data mining
  - Inherent IT security problems, in particular with mass software

Security is instable and vulnerable.

IT security is *decreasing* continuously!

Protection needed for

- Communication
- Information flow from and to servers
- Remote Data Entry (RDE)
  - for multicenter clinical studies

Preferred: Open standardized protocols

- E-Mail
- http (WWW, Client-Server)

Basic Security Requirements

- Confidentiality
- Integrity
- Proof of origin/authorship, liability of/for patient data, medical guidelines and advices

  to varying extents

$\Rightarrow$ High degree of IT security strongly required

Cryptographic Basic Functions

Based on cryptographic primitives
(symmetric and public key algortihms,
hash functions, random generators)

- Encryption
- Digital signature
- Strong authentication (challenge-response)

The Health Professional Card (HPC) will perform these basic functions (in 2001/2?)

Pseudonyms

- Anonymize data records, but allow matching and allow reidentification
- Technical alternative:
  - “Code Book”
  - asymmetric encryption
- Trusted Third Party needed
  - generates pseudonyms
  - controls data matching
- Example: The german cancer registries

Public Key Infrastructure

- Private key = digital identity
  - but only if generated and stored by owner
- Public key = identity card
  - if certified by Trusted Third Party
  - certificate binds together name and public key
- Personal secure environment (Smart Card)
- Directory service

$\Rightarrow$ virtual private net on the public internet,
management of access rights

Security Infrastructure for Medical Networks

- **Step 1:** Use PGP for E-Mail communication *NOW* -

  extremely simple installation and use

Short introduction and sample policy:
`http://info.imsd.uni-mainz.de/kks/PGP/`

Security Infrastructure for Medical Networks

- **Step 2:** Use SSL for client-server applications in the Web, based on X.509 certicifates
  - Easy part: server certificates
    (start *THIS YEAR*)
    $\Rightarrow$ encrypted sessions,
    encrypted password transfer
  - Enable servers (web browsers know of SSL)
  - Beware of weak encryption

Security Infrastructure for Medical Networks

- **Step 3:** Use SSL ...
  - Difficult part: user certificates
    (start *NEXT YEAR*)
    $\Rightarrow$ strong authentication and digital signature
  - Certificate Service (CA)
  - CA/RA hierarchy
  - Directory Service (LDAP)
  - Certificate Revocation Lists (CRL)
  - Establish *user* tools for key generation

Security Infrastructure for Medical Networks

- **Step 4:** Use Smart Cards
  - Interoperability with applications ? Web browsers? RDE systems?
  - Compatibility of certificates ?
  - Upward compatibility with HPC ?

Discussion I

- *A PKI is an essential element of any medical network.*
- *Establishing a PKI in a nationwide network is a nontrivial organizational task.*
- *Commercial solutions are of use only when they follow open standards and support existing applications*
  - in particular the usual Web browsers -
  and single login.

Discussion II

- *It’s not justified to assume that we’ll master the security threats of medical networks soon.*
- *We should not rely on unproven assumptions about the benefit of medical networks and telemedicine, but evaluate cost and benefit as soon and as thoroughly as possible.*