Availability vs Confidentiality of Electronic Health Records

Robert de Groote
University of Twente
Clinical vs Traditional systems

- Complex Rules defining Access
  - No simple “this user has access to this data”
  - Conditions under which access is granted are complex
    - “Analyst X can only access a patient’s record if the patient’s Cholesterol level exceeds Y mg/dL”
    - Access conditions may evolve as the patient is being treated
  - Emergency situations

- Highly heterogeneous
  - Data exchanged between various systems
  - All systems must respect the same security policy
Access control

- A priori: lower availability

- A posteriori: accessors must be able to justify their audited accesses

- “Audit-Based Access Control”
Traditional scheme

Access control

Data

User

authentication

data
A posteriori scheme

Audit Mechanism

Data

User

authentication

data
Data exchange and Security

- Traditional systems: data and access control are easily separatable
  - Security of data depends on security and compliancy of the environment it resides in

- Cryptographic access control: data and access control are inseparable
  - Access policy moves along with the data
The problem

- How can we have the availability of audit-based access control and the confidentiality of cryptographic access control?
Cryptographic scheme

- Authorized persons are known *a priori*
- In audit-based access control any* user should be able to access
- Keep the key at a “safe place” and allow recovery by any* user
Escrowed scheme

- Cryptogr. Keys
- Encrypted Data
- Data
- User

Authentication
Escrow by a single agency requires a high amount of trust in that agency.

Can we relax this requirement by using more agencies?

Yes we can.
Partial key escrow

- The idea: an escrowed key is not stored explicitly, but rather implicitly as something that can be reconstructed if a number of agencies collaborate.

- Required trust in a shareholder is less than when using a single escrow agency.
Secret sharing

- Secret: \( p(0) \)
- Reconstruction by interpolation
- Distribute \( (x_i, y_i) \) among group of m members \( (m > n, x_i \neq 0) \)

\[
p(x) = \sum_{k=0}^{n} a_k x^k
\]
Partial key escrow

- An attacker must gain access to all the shares. Can we trust that an agency never releases its share?
- Can we make it harder for the attacker to reconstruct the secret?
- Yes we can
Proactive secret sharing

- \( SS(X) : \)
  Secret-sharing scheme with secret \( X \)
- \( SS(X) + SS(0) = SS(X) \)
- In the new scheme only the shares have changed, \textit{not} the secret
Auditing

- Can be done at the escrow agencies
- Auditing only fails if $n + 1$ agencies fail to audit
Proposed scheme

- Cryptogr. Keyshares
  - Audit
  - Authentication
- Cryptogr. Keyshares
  - Audit
  - Authentication
- Cryptogr. Keyshares
  - Audit
  - Authentication
- Share Renewal
- Encrypted Data
  - Data
- User
Questions?