Privacy in e-Health

As highly sensitive patient information provides a promising goal for attackers, there is increasing social and political pressure regarding the prevention of health data misuse. Traditional data security and access control mechanisms have their limitations in that they are vulnerable against inside attacks by malicious administrators. The answer to this problem is to let the patient as data owner control the access rights of trusted third parties.

Challenges

- Nowadays, the protection of sensitive data is more important than ever before, because data is stored for longer periods of time and in a centralized way.
- It is the patient’s right to demand privacy (e.g., HIPAA, EC Directives, Domestic Acts) as disclosure of medical data can create serious problems for the patient.
- On their own, traditional access control, disassociation, and encryption techniques have their limitations.
- It is necessary to assure the availability of health data for secondary use to improve clinical studies.

Usage Scenarios

- In the local scenario, PERiMETER pseudonymizes only records stored in the local data repository. Both patient and health professional access the records via the same workstation using personal smart cards as authentication tokens. An optional server-side hardware security module provides cryptographic services with enhanced key protection.
- In the central scenario, PERiMETER is responsible for managing access to multiple records at multiple locations. While the pseudonymization metadata contain only references, the actual health records remain at the individual local storages. Through the PERiMETER server, the data owner can grant trusted persons from other environments access to selected records.

PERiMETER (Pseudonymization and pERsonal METadata EncRyption) utilizes a pseudonym-based access control mechanism and a layer-based security model with multiple cryptographic keys to grant access only to authenticated and authorized persons. The patient as data owner strictly controls all access rights to personal health data and is able to create access authorizations for trusted persons, while depersonalized and pseudonymized medical information is available for secondary use. Record fragment links are managed by personal encrypted metadata storages that provide privacy-preserving querying mechanisms using an XML Schema-aware searchable encryption scheme.

Pseudonyms

Root pseudonyms are known to the patient as data owner only and are used as references to represent the links between the document fragments. Fragment-specific shared pseudonyms created by the data owner provide trusted persons with this linking information and act as authorization tokens.