Privacy in Business Processes
- Identifying Non-Authorized Disclosure of Personal Data to Third Parties -

Austria-Japan Workshop 2010
October 18, 2010

Dr. Sven Wohlgemuth
Prof. Dr. Isao Echizen
Prof. Dr. Noboru Sonehara
National Institute of Informatics, Japan

Prof. Dr. Günter Müller
University of Freiburg, Germany
Privacy and Disclosure of Personal Data to Third Parties

Privacy legislation:
„Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others.“
(Westin, 1967 → regulations of Germany/EU, Japan and HIPAA)

Access control

No usage control for the disclosure of personal data

User

DP

DC / DP

Services

DC / DP

DC / DP

DC

Disclosure of personal data to third parties

DP = Data provider
DC = Data consumer
d, d’ = Personal data

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N. and Müller, G., 2009

Dr. Sven Wohlgemuth

Privacy in Business Processes
Agenda

1. Shift to a new Scenario
2. User becomes a Target
3. Usage Control by Data Provenance
4. DETECTIVE: Data Provenance with Digital Watermarking
5. Safety of Data and Liveness of Services
1. Shift to a new Scenario
(e.g. Electronic Health Records, Gematik in Germany)

Current scenario

Patient’s data is stored in many medical systems.

Each medical system is in charge of patient’s data.

New scenario

All data about the patient stored in one location:
A central EHR

Patient is in charge of this data.
2. User becomes a Target
(e.g. Patient)

Patient “inherits” responsibility and risk.

Dishonest parties may modify or disclose personal data to 3rd parties without authorization.

Privacy Problem

How can the patient control the disclosure of medical data to 3rd parties?

Different data protection legislations (e.g. EC 95/46/EC, Japan, HIPAA)
3. Usage Control by Data Provenance (1/2)

**Policies**
- Enterprise Privacy Authorization Language (EPAL)
- Extended Privacy Definition Tools (ExPDT)

**Mechanisms & Methods**

**Preventive**
- Before the execution
  - Process Rewriting
  - Workflow Patterns
  - Vulnerability Analysis

**Reactive**
- During the execution
  - Execution Monitoring
  - Non-linkable Delegation of Rights

- After the execution
  - Model Reconstruction
  - Audits / Forensics
  - Architectures for Data Provenance

Müller, G., Accorsi, R., Höhn, S. and Sackmann, S., 2010
- Data provenance
  - Information to determine the derivation history

- In an audit, data provenance can be used to restore the information flow.

Example
4. DETECTIVE: Data Provenance with Digital Watermarking

Watermarking is a method to bind provenance information as a tag to data.

The EHR/Medical system must enforce that
- disclosed data is tagged with updated provenance information
- provenance information is authentic.

Steps of a disclosure:

1) Access request
2) Fetch data
3) Apply tag
4) Deliver tagged data
Digital Watermarking and Disclosure of Personal Data

Both service providers have same digital watermark

⇒ No identification of last data provider
DETECTIVE: Digital Watermarking Scheme

Data provenance information
- Linking identities of data provider and data consumer with access to personal data.

Detection by the patient via delegated rights (privacy policy) to personal data.
**DETECTIVE: Protocol Tag**

Data provider

1. $\text{pk}_{DP\_COM}$ for commitments

Commitments

2. commit to $k_{DC}$ & blinding: $\text{com}_{DC\_BLIND}(k_{DC})$

3. confirm $\text{com}_{DC}(k_{DC})$: $\text{signature}_{DC}(\text{com}_{DC\_BLIND}(k_{DC}))$

Digital signature

4. $\text{com}_{DC\_BLIND}(k_{DC})$, $\text{signature}_{DC}(\text{com}_{DC\_BLIND}(k_{DC}))$

Data consumer

5. verify $\text{signature}_{DC}$

6. blind $\text{com}_{DP}(k_{DP})$: $\text{com}_{DP\_BLIND}(k_{DP})$

7. link commitments to $d$: $\text{tag}' := \text{embed}_{sym}(\text{anonCredential}_{DC}, \text{com}_{DP\_BLIND}(k_{DP})\text{com}_{DC\_BLIND}(k_{DC}), d)$

8. $\text{tag}'$, $\text{signature}_{DP}$

9. reveal $\text{tag} := \text{tag}' / \text{blinding factor}_{DC}$

Commitments to identity of DC

Digital watermarking

Computing with commitments
DETECTIVE: Protocol Verify

User

CA

Data provider

Data consumer

Reconstruct delegation chain

1: request anonCredentials (rights$_{DC}$) for delegated rights

2: request com$_{DP\_BLINDED}(k_{DP})$, pk$_{DP\_COM}$, and signature$_{DC}$

3: com$_{DP\_BLINDED}(k_{DP})$, pk$_{DP\_COM}$, and signature$_{DC}$

4: request open(com$_{DP\_BLINDED}(k_{DP})$)

5: blinded $k_{DP}$

6: verify com$_{DP\_BLINDED}(k_{DP})$

7: verify signature$_{DC}$

8: extract com$_{DC}(k_{DC})$ from tag

9: check correctness of com$_{DC}(k_{DC})$ by zero-knowledge proof

PKI

Commitments

Digital signature

Zero-knowledge proof
Case study: Telemedicine – Consulting a clinic abroad
5. Safety of Data and Liveness of Services

Safety: Authorized execution

Liveness: Reachable states

Provisions: cover the time up to the access ("past and present")

Obligations: cover the time after the access ("future")

Transparency by Policy Enforcement Mechanisms (e.g. DETECTIVE)