Introducing Privacy in a Hospital Information System

Stefano Braghin
joint work with:
Alberto Coen-Porisini - Pietro Colombo - Sabrina Sicari - Alberto Trombetta

Dipartimento di Informatica e Comunicazione
Università degli Studi dell’Insubria
Varese (Italy)

The 4th International Workshop on Software Engineering for Secure Systems
Overview

1. Introduction to the conceptual model
2. Introduction to Care2x HIS
3. Extending Care2x HIS
4. Future Work
Hospitals have increasingly adopted IT-supported healthcare solutions

Healthcare-related data are stored in a digital version of medical/healthcare records (EMR/EHR)

Sharing sensitive patients’ data introduces security and privacy risks

Legislative acts established standards for the security of digital healthcare information

To comply with such standards healthcare organizations have to define and manage privacy policies

At the moment there is a gap between functionalities offered by off-the-shelf healthcare information system and the privacy requirements
“The doctor may access the case history of the patient in order to evaluate his/her health condition and to possibly prescribe a therapy, under the obligation to report any contagious disease to the supervisor. The manager verifies that all the actions are compliant with the privacy policy of the hospital.”
It defines how data referring to individuals can be collected, processed and diffused according to the rights that individuals are entitled to.
Privacy Policy: User

- **Controller**
  - the authority which determines the purposes, obligations and means of the processing of data

- **Processor**
  - anyone processes data on behalf of the controller

- **Subject**
  - anyone owns data which are referred to
Privacy Policy: Data

- **Personal data**
  - any information relating to an individual

- **Sensible data**
  - data concerning specific *sensible* information like health, race, political opinions...
Privacy Policy: Action

- **Processing**
  - any operation performed upon personal data

- **Purpose**
  - a set of actions that specify the reasons for which data are processed

- **Obligation**
  - a set of actions that the processor guarantees to perform, after the data have been processed
The conceptual model

Subject

ConsenstRequest

ConsentRequest

Data

Control

ActionBehavior

Controller

FactoryAction

User

ConsentAcquisition

FactoryAction

Processor

ActionBehavior

Purpose

Obligation

Action

Sensible

Identifiable

Control
“The doctor may access the case history of the patient in order to evaluate his/her health condition and to possibly prescribe a therapy, under the obligation to report any contagious disease to the supervisor. The manager verifies that all the actions are compliant with the privacy policy of the hospital.”

- **Users:**
  - **Subject:** patient
  - **Processor:** doctor
  - **Controller:** manager

- **Data:** case history

- **Actions:**
  - **Processing:** access
  - **Purpose:** treatment
  - **Obligation:** communication
Privacy Policy Enforcement

- Verify the compliance of the actions with a given privacy policy
  - *ex-post* mechanisms
    - controls done after all the actions are performed
  - *run-time* mechanisms
    - the effect of every action is checked before its actual execution
A case study

- We have applied our model in a real world scenario
- Provided support for Privacy Policies extending an off-the-shelf Healthcare Information System
- Motivations of the choice:
  - Managing sensitive data is relevant in healthcare
  - It is required by legislation (e.g. HIPAA, Directive 95/46/EC of the European Parliament, Italian law DL n. 196/2003, ...)
- Such reasons make an HIS a perfect test-bench for the proposed model.
A brief overview of Care2x history

- An Open Source hospital information system
- Released under GNU GPL on May 2002
- Currently supported by a team of more than 300 programmers
- Deployed in more than 20 countries
- www.care2x.org
Care2x Components

- **HIS**: Hospital/Healthservice Information System
- **PM**: Practice Management
- **CDS**: Central Data Server
- **HXP**: Health Xchange Protocol
Care2x Components

- HIS: Hospital/Healthservice Information System
- PM: Practice Management
- CDS: Central Data Server
- HXP: Health Xchange Protocol
Care2x Components

- HIS: Hospital/Healthservice Information System
- PM: Practice Management
- CDS: Central Data Server
- HXP: Health Xchange Protocol
Care2x Components

- HIS: Hospital/Healthservice Information System
- PM: Practice Management
- CDS: Central Data Server
- HXP: Health Xchange Protocol
Care2x Components

- **HIS**: Hospital/Healthservice Information System
- **PM**: Practice Management
- **CDS**: Central Data Server
- **HXP**: Health Xchange Protocol
Web application characterized by a 4 layer structure
- Implemented in PHP
- Using standard relational DBMSs
- Deployed by common web servers
Goals:

- Implement a role-based privacy management mechanism
- Provide *run-time* and *ex-post* enforcement mechanisms
Goals:
- Implement a role-based privacy management mechanism
- Provide run-time and ex-post enforcement mechanisms

Proposed solution:
- **Extend the data layer:** add concepts taken from the conceptual model such as Role and Action
- **Extend the control layer:** introduce new services exploiting the extensions introduced in the data layer
Role-Based Privacy Management

- Requires the introduction of two types of elements:
  - roles
  - actions

- Three main roles:
  - Subject
  - Processor
  - Controller

- They differ from the role concept within Care2xHIS where role means function such as
  1. Physician
  2. Nurse
  3. ...

- Functions ≠ roles!!
Role-Based Privacy Management: the data layer (1/2)

- Introduction of a hierarchy among the existing functions exploiting the already existing data structure
- Introduction of a relationship between functions and actions
- Introduction of a complex structure to represent actions according to the conceptual model adopting the Composite design pattern
Implementation of two main classes

- **Action**
  - Implements the methods defined in the `ActionBehavior` interface
  - Access entities `care_role_person`, `care_action_C` and `care_action_S`

- **Role**
  - The instances specify a list of actions that defines the admitted or required behavior for the instance
Introduction of working classes as adapter for the currently existing interface
Introducing Privacy in a HIS

S. Braghin (DICOM)

SESS'08 22 / 25

Introduction of two new entities to provide a structured log mechanism to keep track of the execution of the actions.

The *ex-post* enforcement can be carried out by verifying the correctness of the log entries associated with the executed actions.
Class *Action* requires the interface *Control* to verify the compliance with the privacy policy.

Such interface is realized through different implementations.
Future Work

- Experiment the extended application in the real world
- Refine the privacy model
Questions?

stefano.braghin@uninsubria.it