Sécurité des systèmes d'information et de communication dans le domaine de la santé

Anas ABOU EL KALAM, Yves DESWARTE
{Anas, deswarte}@laas.fr

Approach

Plan

- System security requirement definition
- Concepts for HCCS security policies
- Security model
- Conclusions and perspectives

Security model

Concepts for HCCS security policies

Security model

Conclusions and perspectives
Sensitive information

Inputs...
- General Assembly of the United Nations: A/RES/45/95
- European Community directives: 95/46 97/66, 2002/58 ...

What?
- Personal data
- Resources and services (e.g., payment, emergency)
- ...

Security requirements

HCCS Security (Security, Safety, Quality, Privacy)

Confidentiality: the non-occurrence of unauthorized disclosure
Secrecy: the non-occurrence of unauthorized disclosure
Privacy: the non-occurrence of unauthorized disclosure

Integrity: the non-occurrence of inadequate alterations
Consistency, accuracy of data
Verification of data-entry validity

Availability: the readiness for usage
Response time: e.g., emergency
Perenniarity: Medical records must be kept for a long time ...

Accountability

System security requirement definition

Concepts for HCCS security policies

Motivation
- Basic models
- Or-BAC
- The context

Security model

Conclusions and perspectives
Motivation

Security Policies?

- Rules that satisfy contextual permissions/prohibitions
  - e.g., the context of urgency
- Rules that satisfy P/F/O/R
- Rules that are specific to the organization
  - Each sub-organization may have its own SP, ...

Basic models: HRU

- Subjects: active entities
- Objects: (active + non-active) entities
- Actions

But...
- When new subjects/objects/actions are introduced in the system?
  - the updating of the SP is quite complicated! 
- Only permissions
  - F/O/R are not included !

Basic models: RBAC

Role: structure subjects

But...
- The concept of permission is primitive
  - For a given application, the RBAC model must be refined to make explicit the structure of permissions
- For the same role, authorizations can differ from an organization to another
- How to specify a P that depends on a given context?
  - All users that play a certain role will inherit the role permissions ...
  - but, if the physician does not treat the patient?

Or-BAC
**Or-BAC: subjects and roles**

- **Organizations**
  - An organized group of active entities (e.g., the intensive care unit of a given hospital)

- **Subjects**
  - Active entities, i.e., a user or an organization

- **Roles**
  - To structure the link between subjects and organizations
    - The roles “cardiologist,” “nurse” will be played by users
    - The roles “intensive care unit,” “rescue team” will be played by organizations
    - Make easier the update of the SP when new subjects are added to the system

**Or-BAC: Objects and views**

- **Objects**
  - Passive entities (e.g., data files, medical records)

- **Roles**
  - **structure subjects**
    - User $i$
    - Role $r$
    - Permission $p$
    - User $j$

- **View**
  - **structure objects**
    - **set of objects that satisfy a common property**
    - Logical criteria based on access rights
    - Characterize the ways objects are used in Orgs
    - Makes easier the update of the SP when new objects are added to the system

**Or-BAC: Actions and activities**

- **Action**
  - File Operations such as read, write, send, ...

- **Activity**
  - To abstract actions
    - To join actions that share the same principles
    - To be able to characterize organizations that structure differently the same activities

**Examples**

- Consider(Hospital A, read, consulting)
- Consider(Hospital B, select, consulting)

**The context**
Or-BAC: Contexts

- **What?**
  - Specify the concrete circumstances where organizations grant role permissions to perform activities on views
  - E.g., urgency, attending physician, etc.

- **Example**
  - Define(Hospital A, Bob, F1.doc, read, Urgency) = within the organization “hospital A”, the context “urgency” is true between the subject “Bob”, the object “F1.doc” and the action “read”.

The conditions required for a given context are formally specified by logical rules.

Context

- **Context of a role:**
  - Cardinality, static/dynamic mutual exclusion

- **Context of objects:**
  - Duration attribute for the storage of certain data; location attribute

- **User attributes:**
  - Specific authorization, temporary rights

- **Context of use**
  - Healthcare process
  - Purpose of use

  - the user’s team participates in the process treating the patient
  - Every access must belong to one of two cases
  - particular situation: declaration of a purpose

Healthcare process

Purpose of use

- **Purpose of use declaration**
  - role=healthcare provider
  - He has formerly treated the patient
  - Notification to patient

- **Diagnosis revision**
  - request made by an emergency ward patient wounded in a vital organ lack of personnel, ...
  - Read/Write PMF

- **Emergency**
  - High level Audit

FLEXIBILITY + RESPONSABILITY
**Or-BAC: the model**

- **Concrete Authorizations**
- **Subject** (User)
- **Object**
- **Organization**
- **Activity**
- **Role**
- **View**
- **Context**

**SP level Abstract entities**

**Plan**

- System security requirement definition
- Concepts for HCCS security policy

**Security model**

- New language
- Examples of rules
  - System description
  - Security properties
  - Security rules

**Conclusions and perspectives**

Tuesday, 01 July 03

**Formal System**

**Alphabet of the language**

- **Constants**
  - Instances of security policy entities: users, roles, teams...
- **Variables**
  - e.g.: $u \in$ Users ($u$ is a variable of type User), $r \in$ Roles, $o \in$ Groups of Objects
- **Functions**
  - Describing/building terms: deriving information about their properties
  - PMF(patient identity, CP identity, nurse report, diagnosis, prescriptions) → Record
- **Predicate**
  - E.g.: $\text{AURT}(u, r, t)$ is a relation symbol of type (user, role, team)
- **Actions**
  - E.g.: $\text{TRANSMIT}(u, f, u'), \text{CREATE}(u, t)$

**The language**

- $\text{Af}(t_1, \ldots, t_n) ::= \text{Predicate}(t_1, \ldots, t_n) \mid \text{Action}(t_1, \ldots, t_n)$
- $f ::= Af(t_1, \ldots, t_n) \mid -f \mid f \land f \mid f \lor f \mid \text{Of} \mid \text{Pf} \mid \text{Ff} \mid \text{Rf}$

**Truth conditions**

- $M, w \models \text{Of} \iff [\forall w', w R w'] \Rightarrow M, w \models f$
  - $f$ is true in every world $w'$ which $w$ is in relation with ($\ldots$ in all possible evolutions, $\ldots$)
- $M, w \models \text{Pf} \iff [\exists w', w R w'] \Rightarrow M, w \models f$
  - $f$ should be possible to reach a world in which $f$ is true ($\ldots$ in some possible cases)
- $M, w \models \neg f \iff [\forall w', w R w'] \Rightarrow M, w \not\models f$
  - None of the accessible worlds should allow to conclude that $f$ is true ($\ldots$ none of the $\ldots$)

- $\alpha[\text{WRITE}(\text{Sam, f1.txt})]$
- $\beta[\text{CREATE}(	ext{Bob, Prescription})]$
- $\gamma[\text{AR}(	ext{Alice, Nurse})]$

**Formal System**

**New System**

- $\text{WRITE}(\text{Sam, f1.txt})$
- $\text{CREATE}(	ext{Bob, Prescription})$
- $\text{AR}(	ext{Alice, Nurse})$
**System description**

**What?**
The functional aspects of the system that are relevant for security

**How?**
- Propositional logic operators
- Define the internal structure of the worlds
  - E.g.: q→r means in any world w where q is true, r is also true

**Example**
Role hierarchy
- AR(u, physician) ⇒ AR(u, Clinical Staff)
- AR(u, nurse) ⇒ AR(u, Clinical Staff)
  ...

**Security properties**

**What?**
Express security requirements (confidentiality, integrity and availability)

**How?**
- Modal operators (P/O/R/F)
- Allow modifying the properties of the accessibility relations between the worlds

**Example**
- F[AR(u, pharmacist) ∧ CREATE(u, prescription)]
  - ⇒ forbids a pharmacist to create prescriptions
  - ⇒ none of the possible evolutions of the system should allow to conclude that a pharmacist can create a prescription

**Conclusions and perspectives**

- What to protect? against whom/what? what do we need?

- Security policy
  - Structure objects according to access right criterias ⇒ Views
  - Job performed by the user ⇒ Role
  - The relation between the HCP and the patient ⇒ team/organization
  - Normal access: strong authorization ⇒ process of care
  - Flexibility and accountability ⇒ Purpose of use

- Security model
  - Extending/adapting deontic logic ⇒ P/O/R/F + actions
  - Describing the system, expressing the security properties and the security rules

- Reasoning about our security model by using analytic tableaux

- Implementation by using security mechanisms such as distributed capabilities (MAFTIA) or XML interpretation (univ. of Milan) ...
Thank you!

Questions?
Remarks?
Comments?
Advices?