Special Topics in Security and Privacy of Medical Information

Sujata Garera

Modifications

- Grading scale:
  - Assignments: 30%
  - Participation: 40%
    - Discussion sessions 30%
    - General Participation 10%
  - Project 30%

- Project Part 3 (option)
  - Design methods for integration of OpenMRS with PHR
  - Choose any PHR, Google Health for example
  - Study how the system works
  - Discuss how you might modify the PHR and OpenMRS to provide a unified system to the user
    - Keep the advantages of both intact
  - Observe security issues and discuss ways of combating them
Modifications

- Project part 3
  - Grading:
    - Writeup
    - Description of PHR you chose
    - Quality of design and integration methods proposed
    - Challenges considered
    - Security issues considered
    - Presentation

Due dates

- Part I: Due on Feb 23rd
- Part II: Due on March 25th
- Part III: Due on April 27th

Last week

- Threats to medical information
  - Privacy, identity, integrity, availability
- Medical record
  - EPR vs PHR
- Security Requirements
  - Authentication, access control, confidentiality, non-repudiation
Last week

- Access control types
  - Why access control?
  - Discretionary
    - How does this work?
  - Mandatory
    - How does this work?
  - RBAC
    - How does this work?
- Which of these is mostly applicable in Electronic Health Record setting?

Access control

- A-priori access control
  - Traditional systems work in this manner
  - Illegal actions are prevented prior to occurrence
  - What are some disadvantages of this paradigm when applied to the health care setting?

Audit based access control

- Need for a-posterior access control
  - Immediate health care
  - Urgent situations
  - Complex situations may be difficult to model
  - Allow medical staff the ability to deal with exception situations and justify them later on
Audit based access control
- Work by Dekker and Etalle, 2007
  - System relies on use of Audit Logic
  - A-priori access control is minimized to authentication of users and objects
  - Complex security procedures performed in a-posteriori auditing mechanism

Notation for framework
- Group of agents executing actions
- Actions modeled by set of predicates Act
  - Basic:
    - create(a,d): Creation of a piece of data d by agent a
    - comm(a,b,ϕ): Denotes communication of policy ϕ from agent a to agent b
      - Communication allows for delegation
  - Scenario specific:
    - read(a,d): Agent a reads data d
    - giveDrug(a,b,c): Agent a administers b a drug c

Notation
- Policies built using set of atomic predicates
  - Permissions or conditions
    - Basic:
      - owns(a,d): expresses a owns d
      - Scenario specific:
        - mayRead(a,d): expressing the permission that a may execute the reads action on d
        - isNurse(a): condition expressing that agent a is a nurse
Grammar for framework

- $\phi \land \phi$  AND of various policies
- $\forall o. \phi$  For All objects $o$ policy $\phi$ applies
- $\phi \rightarrow \phi$  A policy implies another policy
- $a$ owns $d$  Models ownership of data
  - Any patient has ownership over his health record
  - $\forall x,y.(\text{isPatient}(x) \land \text{isHealthRecord}(x,y)) \rightarrow x$ owns $y$
- $a$ says $\phi$ to $b$  Express permission to delegate policies
  - Any doctor can delegate to a nurse, the treatment of his patient.

Grammar for framework

- $!\alpha \rightarrow \phi$  Each time action alpha is executed policy $\phi$ applies
- $?\alpha \rightarrow \phi$  The first time action alpha is executed policy $\phi$ applies
- Each time a nurse gives drug to a patient agent $c$ can bill that patient
  - $\forall x,y,z.(\text{isDoctorOf}(x,y) \land \text{isNurse}(z)) \rightarrow x$ says $\text{mayTreat}(z,y)$ to $z$

Grammar

- Derivations
  - Permissions may be derived from certain actions
  - If $a$ says $\phi$ to $b$ then $b$ can assume $\phi$ to hold
    - It is $a$’s responsibility to show that it had permission to give $\phi$ to $b$
    - Written as $a$ says $\phi$ to $b$ $\phi$ $\phi$
  - $\forall x,y,z.(\text{isDoctorOf}(x,y) \land \text{isNurse}(z)) \rightarrow x$ says $\text{mayTreat}(z,y)$ to $z$
Logging and Accountability

- On audit, agent has to provide justification proof for an action

Formal Proofs

- For example, suppose that the proof-obligation for the action \( read(a, d) \) is the formula \( mayRead(a, d) \), then to justify the action \( read(a, d) \) to an auditor, agent \( a \) has to supply a proof that is

\[ \epsilon \vdash_a mayRead(a, d) \]
Formal Proofs

∀x,y,z. (isDoctorOf(x,y) ∧ isNurse(z)) → x says mayTreat(y,z) to z

Electronic Health Record setting

- Agents: Doctors, Patients, Nurses and Administrative Employees
- Data: Medical Records
- Actions: Reading, updating, administering medicines, billing patient for medicines
Medical Record

- PI: Personal Information, records all non-medical information related to the patient
  - Billing information for example
- MD: Medical Data, medical information about the patient
  - Diagnosis and prescriptions for example
- Updates performed by appending new information together with name of agent making the update

Hospital Policies $\phi_h$

- H1: A patient may read and update the PI section of his medical record and authorize others to do so
  \[ \forall a, d. (\text{isPatient}(a) \land \text{isPI}(a, d)) \rightarrow \text{owns}(a, d). \]
- H2: A patient may read and update the MD section of his medical record and authorize others to do so

Hospital Policies $\phi_h$

- H3: A doctor may read the PI section of the medical records of his patients
- H4: A doctor may read and update the MD section of the medical records of his patients
Hospital Policies $\phi_h$

- **H5**: A doctor may give medicines to his patients
  \[ \forall a, b, c. \text{isDoctor}(b, a) \rightarrow \text{mayGiveDrug}(b, a, c) \]

- **H6**: A doctor can delegate to a nurse on his staff the administering of medicines
  - ?

Hospital Policies $\phi_h$

- **H7**: An administration employee may bill a patient each time someone has given medicines to that patient
  \[ \forall a, b, c, d. \text{isAdministration}(c) \rightarrow (\text{giveDrug}(b, a, d) \rightarrow \text{mayBill}(c, a, d)) \].

Example Scenario

- Patients Alice and Bob, doctors David and Diana, a nurse Natalie and an administrative employee Charlie
- Alice trusts doctor David to give her medical file to other doctors to read it
  - Dr. David can delegate the permission to read the MD section of Alice’s medical record.
- How may this policy be formalized?
- Compared to H4 Alice’s policy is more specific
Sequence of Actions

- A1 The hospital gives its policy to Dr. David
  \[\text{comm}(\text{hospital, david, } \phi_h)\].
- A2 Dr. David logs this for later
- A3 Alice becomes a patient of Dr. David
  \[\text{comm}(\text{alice, david, isDoctorOf(david, alice)})\].
- A4 Dr. David logs this for later

Sequence of Actions

- A5 Alice meets Dr. David in his office
- A6 Dr. David reads the MD section of Alice’s record, to remind himself of her details
  \[\text{read(david, mdalice)}\].
- A7 Alice communicates her new policy to Dr. David
  \[\text{comm}(\text{alice, david, } \phi_a)\]
- A8 Dr. David logs this communication for later
- A9 Dr. David updates the MD section of Alice’s record
  \[\text{update(david, mdalice)}\]

Logging

- What action would help Dr. David show that he is allowed to show Alice’s file to another doctor?
Audit trails

- Hospitals privacy officer routinely monitors queries to database with medical records
  - Check for anomalies
  - Check for adherence to policies
  - Should the officer be allowed to monitor emails between Alice and her doctor?

Justification

- How might Dr. David give justification for having accessed Alice’s file?

Justification

- Dr. David needs to show the auditor the log entries corresponding to A2 and A4 and prove that he may read Alice’s file

\[ [A2, A4] \vdash_{\mathit{david}} \text{mayRead}(david, alice). \]
**Unexpected event**

- Alice arrives injured at the hospital while Dr. David is off duty
- Dr. Diana who is on a shift with nurse Natalie treats Alice

**Sequence of actions**

- **B1** Dr. Diana logs that Natalie is a nurse on her shift
  
  \[\text{comm(natalie, diana, isOnStaffOf(natalie, diana))}\]

- **B2** Dr. Diana reads the MD section of Alice’s medical record
  
  \[\text{read(diana, md, alice)}\]

- **B3** Dr. Diana updates the MD section of Alice’s record
  
  \[\text{update(diana, md, alice)}\]

**Sequence of actions**

- **B4** Natalie administers Qurol
  
  \[\text{giveDrug(natalie, alice, qurol)}\]

- **B5** Natalie notifies billing that Qurol was given to Alice
  
  \[\text{notify(natalie, charlie, qurol, alice)}\]

- **B6** Charlie logs this for later
Sequence of actions

- B7 Charlie bills Alice for the medicine `bill(charlie, alice, qurol)`.
- B8 Charlie logs this, together with a reference to Natalie’s notification.

Sequence of actions for accountability

- Half hour later
- B9 Alice becomes a patient of Dr. Diana `comam(alice, diana, isDoctorOf(diana, alice))`.
- B10 Dr. Diana logs this for later.
- B11 Dr. Diana tells Nurse Natalie to give Alice the medicine `Qurol comam(diana, natalie, mayGiveDrug(natalie, alice, qurol))`.
- B12 Natalie logs this for later.

Accountability Proof

- Natalie if asked can prove the authorization to administer the drug `\[B12] \vdash \text{natalie mayGiveDrug(natalie, alice, qurol)}.`
Additional scenario

- C1 Natalie administers the medicine
- C2 Natalie notifies billing that Qurol was given to Alice
- C3 Charlie logs this for later
- C4 Charlie bills Alice
- C5 Charlie logs this together with a reference to Natalie’s notification

Which policy (H1 -- H7) allows Charlie to bill Alice?

A-posteriori vs A-priori

- Medical staff can go ahead with their duties without worrying about authorization details
- Logs are maintained for accountability
- Logs can be verified by multiple auditors
  - A-priori authorization typically involves a single authority providing access

A-posteriori vs A-priori

- Drawback is that misuse of the access permissions are possible since access is not restrictive in nature
  - Cannot be used in situations where the cost of misuse is higher than cost of too preventive security mechanisms e.g. in military information systems
This lecture

- Suggested reading
  - Access Control Requirements for Processing Electronic Health Records by Alhaqbani and Fidge
  - Audit based access control for electronic health records by M.A.C Dekker and S. Etalle
    available on the website