Special Topics in Security and Privacy of Medical Information

Sujata Garera

Last lecture

- Audit based access control
  - How is this advantageous as compared to a-priori access control?

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
  - Allow medical staff the ability to deal with exception situations and justify them later on
Recap: Notation for framework

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

Recap: Notation

- Policies built using set of atomic predicates
  - \( \text{mayRead}(a,d) \) expressing the permission that \( a \) may execute the reads action on \( d \)
  - \( \text{isNurse}(a) \) condition expressing that agent \( a \) is a nurse

Recap: 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
- \( a \text{ owns } d \) Models ownership of data
- \( a \text{ says } \phi \text{ to } b \) Express permission to delegate policies
  - Any doctor can delegate to a nurse, the treatment of his patient.
  - \( \forall x,y,z. (\text{isDoctorOf}(x,y) \land \text{isNurse}(z)) \rightarrow \text{x says mayTreat}(x,y) \text{ to } z \)
Recap: 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

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
  \[ \forall a, d. \ (\text{isPatient}(a) \land \text{isPl}(a, d)) \rightarrow \text{owns}(a, d). \]

- 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
  \[ \forall a, b, c. \ (\text{isDoctorOf}(b, a)) \rightarrow \text{mayGiveDrug}(b, a, c) \]

- 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

$\forall a, b, c, d. \text{admin} (c) \rightarrow (\text{giveDrug}(b, a, d) \rightarrow \text{mayBill}(c, a, d))$. 

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
  
  $\text{comm(hospital, david, } \phi_h \text{)}$. 

- A2 Dr. David logs this for later

- A3 Alice becomes a patient of Dr. David
  
  $\text{comm(alice, david, isDoctorOf(david, alice)} \text{)}$. 

- 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
  \[ \text{read}(\text{david}, \text{md alice}) \]
- A7 Alice communicates her new policy to Dr. David
  \[ \text{comm}(\text{alice}, \text{david}, o_b) \]
- A8 Dr. David logs this communication for later
- A9 Dr. David updates the MD section of Alice’s record
  \[ \text{update}(\text{david}, \text{md alice}) \]

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?

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

\[ [A2, A4] \vdash_{david} mayRead(david, alice). \]

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
  \[\text{comm(natalie, diana, isOnShift(natalie, diana))}\].
- 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
  \[\text{bill(charlie, alice, qurol)}\].
- 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
  `comm(alice, diana, isDoctorOf(diana, alice))`
- B10 Dr. Diana logs this for later
  `comm(diana, natalie, mayGiveDrug(natalie, alice, qurol))`
- B11 Dr. Diana tells Nurse Natalie to give Alice the medicine Qurol
- B12 Natalie logs this for later
  `comm(natalie, alice, qurol)`

Accountability Proof

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

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

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