CmpE 59B: Privacy in Online Social Networks
Lecture 2: Access Control

Pınar Yolum

Boğaziçi University, İstanbul, Turkey

February 14, 2016
Think about the OSN as a graph, where vertices are users and edges are relationships.
Access control: Regulate who can view, edit, use resources

Key concept is role

Users take up roles

Each role is allowed access to a set of transactions

Roles are organized in hierarchies
Role-Based Access Control (Ferraiolo and Kuhn, 1992)

- Role assignment: A user can execute a transaction if she has a role.
- Role authorization: A user’s role must be authorized for the user; i.e., users can only enact roles they are authorized.
- Transaction Authorization: A user can execute a transaction if her roles’ constraints allow it.
- Later extended by Sandhu, Ferraiolo, Kuhn into RBAC standard.
Attribute-Based Access Control

- Add attributes in addition to role
- Access to what, when, where, how?
- Consider the attributes of subject, resources, actions, environment to define access
Example Scenario

- A department has an application through which faculty can view, approve, or edit student schedules during registration period.

- Attribute
  - Faculty: Function? Department?
  - Student: Year? GPA?
  - Action: View? Approve?
  - Registration: Date? Time?
Attribute-Based Rules

- Giving access based on values of attributes
- "Any faculty can view the schedule of students with GPAs greater than 3.5"
- "Only advisers can approve the schedules"
- "An advisor who is a faculty in the department can approve schedules if they contain 18 credits and if the courses are all CmpE courses"
Policy-Based Access Control

- What happens if two rules give different outcomes?
- What if none of the rules cover a situation?
- Policies enable rules to work in harmony
- Need languages to specify rules and their relations as policies
eXtensible Access Control Markup Language (XACML)

- Structural Elements
  - PolicySet
  - Policy
  - Rule
- Tree structure with root either a Policy or a PolicySet
- PolicySets contain PolicySets or Policies
- Each Policy contains Rules that has an effect of Permit/Deny
- Policy Combining Algorithms for (used by PolicySet) and Rule Combining Algorithm (used by Policy)
- Ex: Deny Overrides: If any evaluation returns Deny or does not Permit, then the result is Deny
XACML Request-Response Protocol

- Example Request
  - Subject (User= Pınar; Role=Advisor)
  - Action (Type=Approve)
  - Resource (Type = Schedule, Student = Osman Ali)
  - Environment (Date = 1/2/2016)

- Example Response
  - Decision: Deny
  - Status: OK
  - Transport protocol not specified (XML or JSON exchanged)
XACML Example

https://community.emc.com/docs/DOC-7410
Platform for Privacy Preferences (P3P)

- W3C Initiative that was suspended in 2007
- Protocol to specify how a Website will use personal information
- Contains:
  - A data schema to identify the things a Web site might collect (e.g., name, IP address)
  - XML-based format for specifying a privacy policy
  - A handle to relate a privacy policy with a Web site
  - Transportation of the policies over HTTP
- Web browsers can enable P3P
- Example from https://www.w3.org/TR/P3P11/
When you come to our site to look for an item, we will only use this information to improve our site and will not store it with information we could use to identify you. CatalogExample, Inc. is a licensee of the PrivacySealExample Program. The PrivacySealExample Program ensures your privacy by holding Web site licensees to high privacy standards and confirming with independent auditors that these information practices are being followed. Questions regarding this statement should be directed to: CatalogExample 4000 Lincoln Ave. Birmingham, MI 48009 USA email: catalog@example.com Telephone 248-EXAMPLE (248-392-6753) If we have not responded to your inquiry or your inquiry has not been satisfactorily addressed, you can contact PrivacySealExample at http://www.privacyseal.example.org. CatalogExample will correct all errors or wrongful actions arising in connection with the privacy policy. What We Collect and Why: When you browse through our site we collect: the basic information about your computer and connection to make sure that we can get you the proper information and for security purposes. aggregate information on what pages consumers access or visit to improve our site. Data retention: We purge every two weeks the browsing information that we collect.
How to extend Policy-Based Access Control

- Adaptivity: What happens if things change quickly?
- Risk: Specify access based on how risky things are
- Semantics: Describe access to "important" things that can change over time
Semantic Access Control

- Represent access with semantic rules such that inference can be made
- Allow people in Istanbul to see a picture
  - Alin lives in Besiktas; can she see it?
  - What if the content is a video?
- Use RDF, OWL, SWRL to specify semantics
Trust-Based Access Control

- Compute how much a user trust others in the network
- Each edge in the graph is labeled with a trust value (based on previous interactions)
- Trust is calculated by propagating this value over nodes
- Define a rule based on the trust value; e.g., show pictures to users whose trust value is above 0.7
- Carminati, Ferrari, Perego (2009)
Computing Trust Values

OSN

Alice
Picture: only me: can see

Bob
Friend list: only me: can see

Dennis
Picture: friends: can see
Location: friends: cannot see

Charlie
Picture: everyone: can see

0.2
0.7
0.9

Pinar Yolum
CmpE 59B: Privacy in Online Social Networks
February 14, 2016 17 / 19
What else?

- Many policy languages: REI, Ponder, ...
- None of them widely accepted or used because of complexity
- Requirement: Simple yet powerful
How is Facebook doing it?