perMIT

Paul B. Hill

MIT
Deployment at MIT

- MIT Roles has been in use since at least 1998
- perMIT is the next generation
- End of FY10 – perMIT and Roles will coexist, Roles will act as the master
perMIT is

- A privilege management system
- Its precursor has been in use at MIT for well over a decade
- Supports
  - Inheritance
  - Explicitly granted privileges
  - Privileges defined as the result of evaluating enterprise data
  - Delegated administration
  - Starting and ending dates for each privilege
- Includes a master department hierarchy system
- Accessible via:
  - a SOAP based web service
  - Flat files
  - Exporting data to LDAP groups
Guiding principles

- Central privilege repository – data can be fed to downstream systems, or accessed in realtime via a web service
- Privileges are defined in understandable business terminology, leading to clear delineations within systems and services
- Maintenance of privileges are distributed to departments, labs, and centers, keeping the maintenance activities close to the people who understand the business needs, and feel personal responsibility for the activity.
- A single authorization can feed more than one system, e.g., financial reporting authorizations control access to reporting both in SAP financial system and in data Warehouse
perMIT’s data model

- ASPEC = subject + function + qualifier (aka scope)
  - Joe
    - Can Access: Oxford English Dictionary Online
  - Jane
    - Can Download: MS Office 2007
  - John
    - Can Modify Voice Mail Forwarding: 6172589850
  - Jim
    - Can Create Functions: in category HR
  - Juan
    - Can spend and commit: on cost object Q678543
  - Attila
    - can approve: on cost object Q678543
Usage at MIT

• In use by over 30 applications, including:
  – Financials, payroll, student system, admissions, registrar, telephony, libraries, graduate aide, HR, environmental health and safety, data warehouse, MIT ID system, help desk, master department hierarchy, accounts management

• 6258 people have the ability to grant privileges (10/2/2009)
  – Institutional size is roughly 23,000
  – Only 601 can grant privileges if you exclude 5637 people who have the GRANT flag turned on for their privileges in the Telephony and Network category (for maintaining VoIP preferences).

• Growing interest from a number of business areas:
  – Physical security / door access / parking
  – Backup system
  – Certificate authority
  – Travel / reservations
Newest customers on campus, in progress

- Travel arrangements (feeds to Concur)
- Gift reporting / Gift acknowledgement (Resource Development)
- Role management within WordPress blogs (Math Dept)
- Streaming media / course lectures (AMPS)
- Grade submissions
• Add replication for high availability
• Improved auditing (function maintenance and qualifier maintenance)
• Stronger data typing / generalization of some of the business logic
• Broaden the allowable subjects:
  – Scoped identifiers for federated use cases
  – Attribute / value pairs
  – Groups
• Release the code as open source
Scoped Identifiers as Subjects

- UI provides look up services allowing the person doing data entry to search by name, or various identifiers.
- The value added to the Subject of the ASPEC will not necessarily be canonicalized.
- For example, if your application uses a Targeted-Id, you can’t enter the EPPN and expect it to work properly.
- Limited canonicalization for local users
  - pbh == pbh@mit.edu
  - We require this for legacy issues within MIT
Attributes as Subjects

- Subjects will be able to be a single attribute value pair.
  - `eduPersonEntitlement= urn:mace:dir:entitlement:common-lib-terms`
  - `scopedAffiliation=student@*.*.edu`

- Subjects will NOT be a combination of attributes allowing rich grammar for arbitrary use cases.
  - `eduPersonEntitlement= urn:mace:dir:entitlement:common-lib-terms AND scopedAffiliation=student@*.*.edu`

- In a federated environment, the “foreign” IdP should have enough information about the user to determine what value, if any, it should release for `eduPersonEntitlement`. The sites negotiate the requirements out of band.
• This will introduce an LDAP dependency.
• Scenario:
  – Group:Orange + blog administrator + mathlets blog
  – Web service asks, what functions (roles) does JoeUser@nyu.edu have for the mathlets blog?
  – perMIT will have to notice that one of the subjects is a group and then check LDAP to see if JoeUser@nyu.edu is a member of the group Orange.
• Note this functionality may upset the auditors greatly, unless you also have a good audit record for your group management system and can easily correlate that data to audit logs from other systems.
perMIT’s roadmap for MIT deployment

- Deploy perMIT as a slave to Roles DB
  - perMIT will receive the same nightly feeds from the Data Warehouse that Roles already receives
  - Validate data consistency
  - Interactive updates are made to the Roles DB, which acts as the master
  - Replication of interactive updates are propagated to perMIT in soft-realtime
- Migrate applications to read from perMIT
- Reverse Master / Slave relationship
Where are we on the roadmap?

- Nightly feeds to perMIT partially working
- Web service to pertMIT ~80% complete
- Replication 50% complete
- Primary Roles DB developer (since 1996) retired as of March 31, 2010
How is PACMAN like Java?

- In 1997 as soon as a programmer in higher-ed became fluent in Java they left for a dotCom startup.
- In April of 2010 we lost our primary perMIT developer to a large financial services company.
- Interested in talking to contractors with appropriate skill sets.