Where the sidewalk used to end, privilege management

Chris Hyzer
University of Pennsylvania
Agenda

• Introduction to privileges
• VPD use case and demo with Grouper
Anonymous user accesses on-line directory application

- User goes to application, looks up public data
Institution users can see private data

- Use authentication
- If you are authenticated, you are an institution user, right?
Yet another story about…

• Yet another story about how authentication does not equal authorization…
Is anyone who can authenticate an institution user?

• Prospective students?
• Parents of students?
• Ex-employees?
• Alumni
• Anyone in the federation?
• … probably not…
Institution users can see private data

- Use course-grained authorization (SAML assertion, LDAP lookup, Group lookup, etc)
Course-grained authorization still has (implicit) privileges

- The privilege objects do not exist in a system
- Code in the application implicitly converts the course attributes into privileges to allow the user to do stuff

```java
21  <c:if test="user.institutionUser">
22     <a href="institutionUser.jsp">Institution user query</a>
23  </c:if>

461 /**
462  * institution query
463  * @param request
464  * @param response
465 */
466 public void institutionQuery(HttpServletRequest request, HttpServletResponse response) {
467     Subject loggedInSubject = GrouperUiFilter.retrieveSubjectLoggedIn();
468     if (loggedInSubject.getAttributeValue("institutionUser") != "true") {
469         throw new RuntimeException("User is not allowed!");
470     }
471 }
```
Fine-grained local privileges

- The online directory contains privilege objects
- These privileges objects are mapped to the “institution user role” or to the individual logged-in user
Fine-grained centralized privileges

- The privilege management system has privilege objects
- These privileges objects are mapped to the “directory application institution user role” or to the individual user
- Note: application might not need to know if institution user
- Centralized privilege assignments could be cached locally
Fine-grained centralized privileges cached locally

- Centralized permissions cached locally
- Can improve performance
- E.g. for row level security
Fine-grained centralized privileges

- Standard protocol (FIFER?) between application and Centralized Privilege Management System

![Diagram]

- Browser
- Authentication
- Application
- Centralized Privilege Management System

- Can user run institution user queries?
- Can user edit own data?
- Can user change data for other users?
Why use centralized permissions?

• Can see what resources a user has access to
  • Better deprovisioning
• Enterprise point in time
• Applications can share permissions (e.g. several payroll applications)
• Cross application separation of duties
• Admins need fewer Uis/systems
• Fewer UIs to build
• Advanced features: rules, limits, allow/disallow, etc
• … especially if it is easy for application developers to use or packages to integrate with
Policies

• Rules that specify parts of access management decisions
• E.g. Employees with at least one active job can access the Paid-time-off application
Grouper-loader approach

Browser → Authentication

Application:
- Can user run institution user queries?
- Can user edit own data?
- Can user change data for other users?

Data warehouse:
- Load a group “activeEmployees” based on SQL query

Grouper:
- Paid time-off user role
  - “activeEmployees” group is assigned to the role
  - “canLogin”, “canCreatePtoRequest”, “canViewOwnBalances” is assigned to the role

Can user run institution user queries?
Can user edit own data?
Can user change data for other users?
Grouper loader “policy” approach

• Need the information available in SQL/LDAP
• Currently cron’ed, could use real-time (wouldn’t be hard but you need an SQL/LDAP change log notification)
• Can take advantage of Grouper features:
  • Does user have access to resource?
  • Which resources does a user have access to?
  • Which users have access to resource?
  • Point in time:
    • Who had access to the resource last week?
    • Which resources did the user have access to over the last month?
  • Permission limits
Questions?