Identity and Access Management

Prof. dr. ir. André Mariën
There is a problem with IAM

• IAM projects are high-risk projects and at the same time critical improvement projects
  – High failure rates → management confidence ▼
  – IT business relationship ▼
  – Organizations that do not fail?
    • Often: expected benefits have not materialized
• What are the root causes of the difficulties?
  – Lack the right tools?
  – Inherent complexity?
  – Incompetent people?
Security lingo for objectives

• Ensure confidentiality
  – Confidentiality ≠ encryption
  – But access control is key for confidentiality
    • Encryption, key management: support for access control
• Ensure accountability
  – Link between the physical world (people of flesh and blood) with technical world
    (userID/password, certificate, token, claim, ...): crucial relationship
  – Manage privileges, but also manage privilege management
  – Accurate and comprehensive reporting
• Avoid conflict of interest
  – Identifying conflict of interest situations and defining duties with segregation constraints
  – Identity management must be enterprise wide:
    • link all logical instances to the actual, physical principal
• Ensure least-privilege
  – Only privileges that are needed, but when needed
  – Organizational agility: acquiring and dropping privileges follows business changes immediately
Business objectives

• Know you users
  – Manage their identities

• Ensure compliance
  – Accountability, data protection, duty segregation

• Prevent unauthorized access
  – Authenticated, Authorized, access control

• Affordable
  – Fit with business and IT reality
  – Maintainable and mostly automated
Your first decisions may put the whole program at risk

• Classify it as an IT project
  – All will go well in the development and implementation phase
  – Nothing but trouble near roll-out and production
• Decide on a company wide model, example: RBAC
  – Proof-of-concept test succeed
  – Roll-out and maintenance slowly turn into nightmare
• Pick a product, configure, do some role mining, done
  – Great plan
  – Try outs seem to work
  – Role mining produces on larger scale are less convincing
  – No underpinning of roles, so how to maintain?
Observations

• Identity space
  – multiple systems for managing identity information exist and are here to stay
    • spread across the organization
    • different vendors
    • different purposes
  – Fundamental to “identity” is its uniqueness, but many views coexist

• Business view
  – business must controlling access, but not all in the same way:
    • based on functions, tasks, organizational structure, ...
    • Force one way: sure to meet resistance
  – Business needs drive authorization and access control: the business need leads to authorizations and access granting

• Technology space
  – N+1 problem:
    • Every application, service, package: +1 for account repositories
    • New & enhanced authorization and access control model(s)
  – Ease of integration:
    • Some systems: immutable, really inert
    • others come and go, or are replace by new ones with a different vision
Mickey mouse model

• Divide and conquer: Four domains
  – Identity management
  – Business privilege management
  – Technical authentication and access control
  – Enterprise privilege management: the domain linking it all together

• Core activities
  – Entity registration and correlation
  – Business privilege modeling and model population
  – Access control solutions and provisioning
  – Privilege management and privilege use
Four domains

• The three satellite domains must be able to evolve independently
  – Keep the center very stable
  – Maintain interfaces as much as possible
  – Absorb changes in the mapping on the borders (hinges)

• Minimize impact on other domains from
  – Changes in identity management solutions
  – Business unit reorganization, model for privilege management changes
  – Technology changes: new solutions, other provisioning, other repositories
Identity management

• Approaches
  – Registration authority, with local registration agents
  – Correlation extensions in the various solutions
  – “Master data management” approach

• Principle: Identity as root
  – Identity-rooted data modeling
  – Specific extensions
    • Technical identities, and link with accountable identity
    • Third party stub identities, and link with accountable identity
Privileges/rights: Phases

• Define
  – Vocabulary
  – Model

• Assign
  – Authorization

• Provision
  – Feed provisioning system with translated privilege data

• Control
  – Access control
Business privilege management

• Rooted in business
  – The privileges of an entity are a consequence of the business context

• Business units have multiple privilege models
  – Organizational Roles, Organizational structure, Task based
  – Professional certification or authorizations
  – Unstructured subsets (for instance workload driven)

• High level differences between
  – Unit type: HR, finance, sales, IT
  – Business: bank, insurance, trading

• Primary schemes:
  – Direct: assign privileges to identities
  – Chain: example: Role to tasks to privileges

• Approach:
  – Map business model to a limited subset of concepts
    • Example: functions, tasks, organizational units, accreditations
  – Map this subset to privileges: pre-authorization step
Technical authentication and access control

• Account management
  – Accounts as a consequence of privilege assignments
• Authorization often hidden inside applications
  – Model per application, no model at all
• Technical privilege modeling
  – Permissions: abstract specific implementation
  – Example: Three distinctions to make: user, supervisor, manager; implementations can vary:
    • Three classes of userIDs (Uxxx, Sxxx, Mxxx)
    • userID must be member of the right group
    • ACL contains userID
• Access control models
  – OASIS model provides solid base: policy (enforcement, decision, information, administration) points: PDP, PEP, PIP, PAP
  – More details later
• Provisioning, SSO, federation, exceptions, credential management
The four-world model
Process: business drives

• Processes and process design matter, a lot
• Move away from “request access”
  – Access granting is based on business decisions
    • No need to ask for an account
    • No need to check business reason for a request
  – Revert thinking: business decision implies granting access
    • Not: ask for access as a separate process
    • Changes in business imply granting the necessary access
• Task assignment, work unit assignment, … are business events at the basis of privilege changes
  – Should lead to privilege changes
  – Privilege changes should lead to account requests or removal
  – No need to “request” new or delete old privilege
Privilege processes

Administration

Privilege Definition

Privilege Assignment

Information Model

Privilege Control

Privilege Provisioning

Operation

11/3/2014

(C) A. Mariën
## Sub problems and Aspects

<table>
<thead>
<tr>
<th></th>
<th>Definition</th>
<th>Assignment</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Identity</strong></td>
<td>What is it? Where is it? Kind of identity</td>
<td>How to introduce? When to assign? When to end?</td>
<td>Crosslink Existance Identity reference</td>
</tr>
<tr>
<td><strong>Account</strong></td>
<td>Realms Systems Types</td>
<td>Account management</td>
<td>Authentication</td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>Model Model instances</td>
<td>Authorization</td>
<td>Access control</td>
</tr>
</tbody>
</table>
Automation

- Process: Three steps
  - Legitimate request for access?
    - Implied by business decision.
    - Derive situation from business data
  - Authorize access
    - Principle-based authorization, not case-based.
    - Modeling exercise: define privileges and mapping onto business attributes
  - Enable access
    - (Provisioning)
      - Update access control repositories to allow access.
      - Update account repositories
      - Update access control component database (PIP, PDP implementation)

- Business privilege assignment
  - Based on principles
    - “All employees are authorized to access email”
    - “Only personnel in HR has access to personnel records”
    - “Only managers have access to evaluation reports”
  - Based on business information sources
    - “is an employee”
    - “works in HR”
    - “is a manager”
    - “is a certified accountant”
  - Automatic:
    - No approval delays for automated privilege assignment
    - Privilege removal: as soon as business context changes
  - Responsibility:
    - Direct impact on operational rights
    - Change throttling/buffering
Additional complexity

- **Constraints**
  - Incompatible privileges cannot be combined
  - Important objective for business
  - Issues: where to check? When to check? Override?

- **Contexts (mobile workforce, different commercial contexts)**
  - Privileges assigned in context require context verification (acting for, from, ...)

- **Delegation (illness, holiday)**
  - Delegation as normal business practice
    - Not exceptional
    - Not via credential passing

- **Transitions (function change, role change, in/out)**
  - Transitions as normal business practice
    - Start working, move to different unit, move to different function
  - Change takes time
    - Coexistence of two situations
    - Controlled move

- **Parameterization**
  - Opaque parameters for specific business information transfer to access control components
  - Context information
Master data management

• One master
• Clearly determine which is the master
• Various set-ups possible
Management master with provisioning to slaves
Distributed repositories and management, with consolidation
Access control

• Parameters for access control
  – Requesting entity
    • Privileges
    • Account
  – Resource, target
    • Target
    • Action
    • Parameters
      – Owner, restrictions
  – Request
    • Context: time, channel, location
• Actual access control: how? XACML model
XACML Data Flow Model
OASIS XACML based view

- Differentiation: location of the Access Control Enforcement Point (PEP), Decision Point (PDP), Administration Point (PAP) and Information Point (PIP):
  - Provisioning Model (PAP[, PIP]):
    - privileges are translated into realm permissions and provisioned towards the different realm masters.
    - PDP, PEP: in the applications
  - Privilege Information Retrieval Model (PAP,PIP):
    - PDP, PEP: in the applications
    - But: PIP consulted to take decision
  - Centralized Privilege Control (PAP,PDP[,PIP]):
    - PEP: in the applications
    - PDP is externalized
    - possibly PIP consulted to take decision
Application interaction patterns

Unmodified/legacy application

Provisioning

Application

Authentication

Access control

Provisioning Driver

Provisioning Engine

privileges

permissions

EPM

11/3/2014

(C) A. Mariën
Application interaction patterns

• EPM
  – Maps account to permissions
  – Provides permissions to the application

• Application
  – Request permissions for an account
  – Interprets the permissions, and possibly other elements, to check if access is granted

Privilege information consumer
internal access control

11/3/2014
(C) A. Mariën
Application interaction patterns

- **EPM**
  - Maps account to permissions
- **Access control component**
  - Gets access request information (account, parameters)
  - Obtains permissions (with parameters) from EPM
  - Takes access control decision
- **Application**
  - Uses the access control component to get a decision
Application interaction patterns

Target: Externalized access control
High level security architecture

- Users
  - Registration
    - Request
    - Account management
    - Authorization
    - Requestors
  - Approvers
- Check: interception
- Check: enforcement
- Workflow
- Master Repositories
- Provisioning
- Audit Trail
- Auditor
- Application
- Local repositories
- Privilege control
- Authentication