Demystifying Privilege and Access Management
Strategies for Local, Federated, and Cloud Environments

Wednesday, August 8, 2012 – 3 p.m. ET

Chris Phillips, Technical Architect, Canadian Access Federation (CANARIE)

Tom Barton, Sr. Director for Architecture, Integration and CISO, University of Chicago

Thank you to InCommon Affiliates for helping to make IAM Online possible. 
We’re all building a global identity services network

• Campus IAM
• Identity federations
• Tools & practices development
• Standards
• International coordination
• Community support & development

➢ For today’s IAM Online, focus is on campus IAM
Layers of campus IAM

• Identities
  – Registries of who/what, identifiers, attributes, systems integration

• Credentials & authentication
  – Internal, external
  – Linked to Identity

• Access management
  – Roles, rules, entitlement, affiliation, groups, privileges, policy, authority, delegation, …

NB: Terminology is tricky! For balance of this hour, Chris gets to choose the terms of this conversation. Ok?
Our Speaker – Chris Phillips

• Canadian Access Federation
• SCIM (Simple Cloud Identity Management)
• Former campus IAM lead

• Member, MACE-Paccman Working Group
• Paccman = Prilivege & ACCess MANagement
Demystifying Privilege and Access Management

Strategies for Local, Federated and Cloud Environments

Chris Phillips | August 8th, 2012 | InCommon IAMOnline
The Speaker – Chris Phillips

- Technical Architect, Canadian Access Federation (CAF)
- Prior ~10yrs: Queen’s University in Kingston
  - Enterprise directories & Sun SSO, Shibboleth infrastructure
  - IDM: homegrown operation & transition to Sun IDM 8.x
  - PeopleSoft ERP deployment w/real time IDM connection
  - Participated in early CAF efforts
- Involved in MACE WG’s since 2005
  - (MACE-DIR, SocialIdentity, MACE-Paccman & others)
- Contributor to IETF provisioning specification SCIM
  - System for Cross-Domain Identity Management
  - aka Simple Cloud Identity Management

- Today: presenting on behalf of MACE-paccman WG members.
About CANARIE

Operates Canada’s ultra-high-bandwidth research network
• Connects one million users at 1,100 institutions, “big science” facilities like TRIUMF, NEPTUNE, CLS, SNOLAB, and to Compute Canada HPC consortia
• 19,000km of fibre with a 40 Gbps backbone
• Funds programs that enable greater access to research data, tools and peers and to stimulate the ICT sector

Operator of the Canadian Access Federation
• SAML federation based on Shibboleth
• Canadian Eduroam 802.1x wireless roaming operator
• eduGAIN participant

Primary investment from Government of Canada - $480 M since 1993

Map date: 29 May 2012
Agenda

- Intro & context about MACE-Paccman
- Describing the challenges & factors to consider
- Glossary & concepts
- Building your privilege and access management model
- Contrast and Comparison with use cases
What is MACE-Paccman

List is 110 strong...
Shoutout to Rob Carter, Emily Eisbruch Chris Hyzer, Steve Olshansky, Michael Pelikan, Mark Scheible, Bill Thompson, Heather Flanagan, Jim Leous, Boyd Wilson, Benn Oshrin, Mark Rank, Keith Hazelton, Tom Dopirak
MACE-paccman in Context
Who you are is not as important as what you are and what you are entitled to do.
Factors To Consider
Factors: ‘Distance’ From Your Data

- **Variable distance from the data**
  - **Local** - Systems of Record (SOR), home grown, Commercial Off The Shelf (COTS)
    - Internally apps enjoy tightly coupled access to fresh data
    - Usually ‘behind the wall’
  - **Federated** – apps aware of more than local & remote SOR’s
    - accept other identities underpinned by a trust decision
    - Foot in both worlds at times -- inside & outside the wall.
    - Data ‘distance’ further out
      - Upon sign in of user or provisioning task
  - **Cloud (aka SAAS, PAAS)** – apps abstracted away lower level details, could be furthest away from your fresh data
    - Similar challenges as federated
    - SLAs may or may not be under your control
    - Outside the wall
    - Deployment profile & app sophistication guide data mngmt
Factors: Design & Intent

• Different design patterns
  – Rigid data structures vs elastic ones
  – Sometimes flexibility to a fault – not prescriptive enough

• Philosophical design differences
  – Intentionally designed to support externalized AuthN/Z vs bolt on

• Implementer intentions
  – Walled garden product may cause challenges…

• Effort to keep current
  – Balance between get it done now vs perfect design
Factors: Governance & Process

• Governance
  – Clarity around:
    • Who says who says
    • Authorization model:
      – Centralized or distributed?
      – Application or data centric?

• Process and Practices
  – Are change control practices in place & recognize the implications of local, federated, and cloud use styles?
  – System Of Record (SOR) steward may not realize:
    • Dependencies on their data and change turnaround
    • How far flung SOR data may be
Terminology
# GLOSSARY – THE SIMPLE ONE

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Describes the access to a resource e.g. &quot;delete&quot;,&quot;add&quot;, &quot;reserve&quot;. Often used interchangeably with function and verb.</td>
</tr>
<tr>
<td>Group</td>
<td>A set of subjects</td>
</tr>
<tr>
<td>Limit</td>
<td>A constraint on a privilege that must be calculated at time of access</td>
</tr>
<tr>
<td>Privilege/Permission</td>
<td>An expression of access to a resource</td>
</tr>
<tr>
<td>Resource</td>
<td>A service, datum, or any other object for which access is controlled</td>
</tr>
<tr>
<td>Role</td>
<td>A set of subjects and the set of privileges they all possess</td>
</tr>
<tr>
<td>Subject</td>
<td>A person, or a service acting on behalf of a person, or a set of subjects.</td>
</tr>
<tr>
<td>Attribute</td>
<td>A name-value pair of data associated with a person, may be multivalued</td>
</tr>
<tr>
<td>Entitlement</td>
<td>A specific attribute that is used as a container for a list of privileges associated with that person.</td>
</tr>
</tbody>
</table>
Useful Concepts

- MACE-Paccman WG:
  - no need to re-invent the wheel on concepts and terminology, XACML[1] has been here before
  - neutral to technology and vendor -- helps describe key areas across platforms and vendors
  - See MACE-Paccman wiki for:
    - Term mappings for Shibboleth & Grouper
    - Sample user stories/use cases

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Administration Point (PAP)</td>
<td>The location which administrates the policies</td>
</tr>
<tr>
<td>Policy Decision Point (PDP)</td>
<td>The location which evaluates and issues authorization decisions</td>
</tr>
<tr>
<td>Policy Enforcement Point (PEP)</td>
<td>The location which intercepts the user’s access request to a resource and</td>
</tr>
<tr>
<td></td>
<td>enforces the PDP decision</td>
</tr>
<tr>
<td>Policy Information Point (PIP)</td>
<td>The location which provides information the PDP (database, ldap directory,</td>
</tr>
<tr>
<td></td>
<td>etc)</td>
</tr>
</tbody>
</table>

## The Evolution of Access Management

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None - most physical controls</td>
<td>If you can authenticate you get everything</td>
</tr>
<tr>
<td>Control by contract</td>
<td>Same as above with a ‘no abuse’ policy</td>
</tr>
<tr>
<td>Hard coded privilege tables at the resource</td>
<td>What most applications still do</td>
</tr>
<tr>
<td>The above + ldap calls for intrinsic attributes</td>
<td>Mostly Affiliation but other eduPerson attributes apply</td>
</tr>
<tr>
<td>An attribute authority</td>
<td>The resource can get any attribute that policy permits</td>
</tr>
<tr>
<td>An external yes/no authorization service</td>
<td>An external service calculates whether access is permitted</td>
</tr>
</tbody>
</table>
The Recipe

Building your Privilege and Access Management Model
Building Your Model

- **Assess**
  - Create an inventory
    - scope of access, span of control, magnitude
- **Recognize & Generalize**
  - Classify by known types or bespoke effort
- **Craft the Vision**
  - ‘now’ vs ‘what it should or could be’
    - Opportunity to write the self-fulfilling prophecy
    - Have both short and long term goals
    - Demonstrating value at each step better than ‘big bang’
  - Baseline for vision & values
    - How else will people know the context?
    - How else to know if you are in alignment?
Available Ingredients

• Staples of Access Control
  – Groups
  – Roles
  – Entitlements
  – Attributes

• Needed but not always easy to get
  – Governance & accountability
  – Key processes identified & defined
  – Naming conventions
## Contrasting the Styles

<table>
<thead>
<tr>
<th>Technique</th>
<th>Strengths</th>
<th>Weaknesses</th>
<th>Opportunity</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>• Ubiquitous</td>
<td>• One size does not fit all</td>
<td>• Prevalence of Existing tools: Grouper, AD native admin</td>
<td>• Privacy, hard to lock endpoints from editing.</td>
</tr>
<tr>
<td>Role</td>
<td>• Good Aggregator of entitlements</td>
<td>• Not as ubiquitous as groups therefore less UI &amp; tools</td>
<td>• Common vocabulary available</td>
<td>• Hard to maintain unless dynamically calculated on the fly</td>
</tr>
<tr>
<td>Entitlement</td>
<td>• Very Fine Grained, Ability to subscope</td>
<td>• Information leakage in single form</td>
<td>• Large, can go down to as fine as one needs (e.g. see field X)</td>
<td>• Delegated admin will be desirable but hard to come by</td>
</tr>
<tr>
<td>Attribute</td>
<td>• All about existing data • Fed’n Friendly</td>
<td>• One full schema does not exist</td>
<td>• Powerful when using XACML and attributes as input.</td>
<td>• Attribute by attribute authenticity &amp; trust by whom &amp; for whom needs work</td>
</tr>
</tbody>
</table>
An Example: Groups Only or Hybrid Approach

Institution X has a central IT department with a manager and sys admins of which some have root.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Implementation</th>
<th>Benefits</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>• 2 groups:</td>
<td>• Out of the box</td>
<td>• No relationships can be inferred</td>
</tr>
<tr>
<td></td>
<td>• Dept-IT,</td>
<td>• Existing (group) tools</td>
<td>• Scaling challenge groups map 1:1 to permissions</td>
</tr>
<tr>
<td></td>
<td>• hasRoot</td>
<td>• Downstream systems could digest easier</td>
<td>• Diverges from org structure to mish mash.</td>
</tr>
<tr>
<td></td>
<td>• Set members as needed</td>
<td></td>
<td>• Not intuitive to decode meaning of groups</td>
</tr>
<tr>
<td>Hybrid of Groups</td>
<td>• 1 group ‘Dept-IT’</td>
<td>• Discrete separation of org membership, role and job function</td>
<td>• Not all systems have visibility to all elements</td>
</tr>
<tr>
<td>Roles Attributes</td>
<td>• 1 role ‘sysadmin’</td>
<td>• Partitions span of control decisions to that which is relevant</td>
<td>• Administration of environment (what should be a group? What should be an entitlement?) is challenging</td>
</tr>
<tr>
<td></td>
<td>• 1 entitlement ‘hasRoot’</td>
<td>• Minimal elements</td>
<td>• Privacy</td>
</tr>
<tr>
<td></td>
<td>• Role has set of entitlements w/ ‘hasRoot’</td>
<td>• Role acts as container for entitlement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Entitlements can stand alone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Entitlements can be subscoped</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Services & Privilege and Access Mgt

- **Same ingredients (groups, entitlements, etc)**
  - Not always the same level of detail
  - may require ‘dumbing the data down’
    - E.g. May need to translate course membership to ‘ is Student’ or ‘user’
- **Same Factors to consider, but highlights different areas:**
  - Identity Management elements jump to forefront:
    - Do I have enough data at the right time and the right place?
      - If not, how do I get it there & at what frequency?
    - Ability to sign on good enough for access?
    - What about account (de-)provisioning conditions?
  - Data exchange rarely bi-directional
    - A group created local to the application will not propagate back to the center
      - Mitigation option: master group information centrally & propagate on change using Grouper.
Emergent SSO Cloud Models

- **SAML SSO, Just In Time (JIT) provision user & update on sign on**
  - Examples: Confluence wiki, box.net
  - Ability to sign in equates to permission to access service
  - Box goes a bit further with JIT and creates groups on demand as well.
    - Permissions linked to group membership need to be managed in the service via the GUI however.
  - Benefit: real time provision on sign on, group creation
  - Drawback: data ages out since last sign on, changes not sent until user logs in

- **SAML SSO, Account Pre-provisioned in advance, Just In Case (JIC)**
  - Examples: Office365 with SAML SSO (not the only one implementation method)
    - Accounts are pre-provisioned in advance via powershell.
    - Pre-provisioning step is point of evaluation for service access.
    - Service access = SSO succeeds + account exists in service, otherwise service not allowed
Technique Ubiquity vs Technique Granularity

- Ubiquity
  - Groups
  - Roles
  - Entitlements
  - Attributes

- Granularity
Dynamicism vs Complexity

Why Care? It’s all about the age of the data
Takeaways

- **It’s about techniques and inputs**
  - Outcome of recipe will be what you can digest and support
  - Common techniques provide a yardstick of what are common themes
  - Helps identify outliers that do not conform to your vision

- **Expect a blend of approaches**
  - Groups good starting point, but likely not sophisticated enough.
  - Sophisticated needs will drive sophistication in delivery
  - Expect drive to attribute based decisions & near real time data updates

- **Tailor the Strength & Weakness analysis to your situation**
  - Adjust based on your perspective, abilities, and portfolio of apps

- **‘Cloud’ services access not much different from federated access.**
  - Standard allow/disallow service access via IdP policy application,
  - Challenge is discrete service changes within a single Service Provider (e.g. how does users AuthZ change features on user transition from student to alum?)
  - As many ways to manage access as there are Service Providers.
    - Why? Lack of standards, hard problem, needs to be ‘right-sized’
Call for Continued Participation

• Cataloguing common use cases benefits us all
  – Have a problem or solution you would like to share?
    – Add it to the wiki of use cases
    – Discuss/share on the MACE-paccman working group calls
  – MACE-paccman Working Group Calls:
    • Alternate Thursdays 1PM Eastern
    • MACE-paccman Working Group Co-Chairs
      – Tom Dopirak, Carnegie Mellon University
      – Keith Hazelton, University of Wisconsin - Madison

• Mailing List:
  – Subscribe to the mailing-list to get Agendas and Call-in information
    • http://middleware.internet2.edu/paccman/

• Wiki:
  – http://spaces.internet2.edu/display/macepaccman

• Thank you!
Evaluation
Please complete the evaluation of today’s IAM Online:
http://www.surveymonkey.com/s/IAMOnline_August_2012

CIFER Topic of November IAM Online

IAM Online Announcement List
Email sympa@incommon.org with the subject: subscribe iamonline

Next IAM Online – September 12, 2012 (3 pm EDT)
www.incommon.org/iamonline
Thank you to InCommon Affiliates for helping to make IAM Online possible.

Brought to you by InCommon, in cooperation with Internet2 and the EDUCAUSE Identity and Access Management Working Group