Home

MACE-paccman (Privilege and Access Management) Working Group

The MACE-paccman working group is dormant for now. Please contact Emily Eisbruch at i2mi-info@internet2.edu, with questions or comments.

The MACE-paccman Working Group provides a venue for discussion and development of access management material in the context of MACE and the Internet2 Middleware Initiative. It was co-chaired by Tom Dopirak, Carnegie Mellon University, and Keith Hazelton, University of Wisconsin - Madison.

For editing access to this wiki space, see the instructions at http://middleware.internet2.edu/docs/internet2-spaces-instructions-200703.html

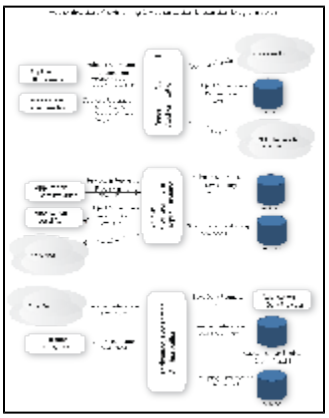
Also see the MACE-paccman website, which includes:

- minutes of conference calls
- instructions for subscribing to the mailing list
- finalized documents and other deliverables, as they become available
- links to related resources of interest

Projects

1. Federated Authorization Problems and Models
2. The Recipe for Privilege and Access Management
3. Looking at selected use cases with a policy service perspective approach, and modeling using XACML terminology (PAP, PIP, PEP, PDP)
4. Simple Cloud Identity Management (SCIM) protocol as candidate for (de)provisioning
    a. Namespaces for privileges and expressing them through URI and URNs
    b. When to use groups , roles, privileges
    c. Role Hierarchies
    d. Working examples of Access Management
5. Using the paccman glossary in other MACE Working Groups
6. Experiments with the Axiomatics Policy Engine
7. How can privileges be provisioned into an existing application?
8. A mace-wide access management glossary

AuthNZ Models



Use Cases

Glossary

Documents and Presentations

- Chris Phillips IAM Online presentation from August 2012 **(Slides .PDF)**
- MACE-paccman Working Group slides from Internet2 Member Meeting April 2012
- Session on "Where the Sidewalk Used to End: Privilege and Policy Management Strategies" at the 2011 Internet2 Fall Member Meeting
- Session on "Authorization and Intelligent Design" at 2011 Internet2 Spring Member Meeting (links to netcast and pdf files)
- MACE-paccman slides from Internet2 Member Meeting: April 2009 (pdf)
- MACE-paccman-glossary and comparative taxonomy
- MACE-paccman charter
- Mapping XACML and Signet Terms
- Kuali identity services summary (pdf)

- CMU Identity glossary
- Visual MACE-paccman charter
- Internet2 Privilege Management Survey Final Report - Fall 2008 (updated pdf ~4 MB)
- Categorizing Access Management Use Cases(Rob Carter and Scott Fullerton, June 2009 CAMP in Philadelphia)
- Surfnet Report on Collaboration Infrastructure
- APIs, Objects and Protocols for Access *Management*
- Oracle Entitlements Server Whitepaper ***NEW***

Links

- CIFER Project
- Classification of Authorization Use Cases addressed by XACML from Gartner, Inc. Author: Bob Blakely
- Policy Engine / PDP initiative
  At Advanced CAMP 2010, several middleware initiatives were launched. One of them, led by Leif Johansson and Keith Hazelton, is on policy engine evaluation using the featured MACE-paccman use cases.
- Grouper
  Anyone needing to manage group access to resources can use Grouper - from accountants to zoologists. A researcher might create a group and enable members to participate on an email list or view a web site. Students might use Grouper to set up and manage groups for similar applications as they work together on shared projects and class work. Your IT staff can delegate group management and enable those leading collaborations to set up and manage their own groups.
- Permis
  PERMIS provides you with the software that makes access control decisions, and also gives you the tools for managing your policies, your role assignments, and delegations between users
- Kuali Identity Management (KIM)
  KIM provides central identity and access management services. It also provides management features for Identity, Groups, Roles, Permissions, and their relationships with each other.
- perMIT Project (MIT)
  The perMIT project's purpose is to translate MIT's RolesDB, in production use for over 10 years, to an open source community project and finally deliver to the world a usable Permission Management System.
- spocp SPOCP (pronounced as SPOCP, for Simple Policy Control Protocol) is a very efficient rule-based authorization engine
- drools Drools is at its core a combination rules engine and process management package. Grouper's rule service is based on Drools. The rabbit hole entrance sign says: *Welcome*
- We believe there is a strong affinity between access management and provisioning. Some of the effort associated with the CIFER project may be of interest, especially the work underway in the Provisioning Subgroup.
- Simple Cloud Identity Management (SCIM)