Access Management 2.0: UMA for the Enterprise

@UMAWG
#UMAam20 for questions
20 March 2014
tinyurl.com/umawg for slides, recording, and more
Agenda

- The realities and challenges of modern access control (CA)
- “UMA for the Enterprise 101”
- Enterprise UMA case study and demo (Gluu)
- What vendors are saying and doing about UMA
- Q&A
The realities and challenges of modern access control
UMA Continues The Shift In Identity Management That Began With OAuth

The Traditional Enterprise

Identity Management is centralized and internal

The 21st Century Enterprise

Identity Management is decentralized and external

This is the secret to achieving scale and agile federation
“UMA for the Enterprise 101”
OAuth is a three-entity protocol for securing API calls in a user context.

Figure 1: Abstract Protocol Flow

- **(A)** Authorization Request → **Resource Owner**
- **(B)** Authorization Grant → **Resource Owner**
- **(C)** Authorization Grant → **Authorization Server**
- **(D)** Access Token → **Authorization Server**
- **(E)** Access Token → **Resource Server**
- **(F)** Protected Resource → **Resource Server**

End-user resource owner gets redirected to AS to log in and consent to access token issuance.

AS and RS are typically in the same domain and communicate in a proprietary way.

UMA’s original goal: apply privacy-by-design to OAuth data sharing

Outsources protection to a centralized “digital footprint control console”

The “user” in User-Managed Access (UMA)

Standardized APIs for privacy and “selective sharing”

Some guy not accounted for in OAuth…

Further reading: tinyurl.com/umapbd
Emergent UMA properties: flexible, modern, claims-based authorization

The RS exposes whatever value-add API it wants, protected by an AS
The AS exposes an UMA-standardized protection API to the RS.
The AS exposes an UMA-standardized authorization API to the client.

UMA, SAML, and OpenID Connect can coexist nicely.
Key use cases

- Managing personal data store access
- E-transcript sharing
- Patient-centric health data access
- ...and enterprise access management 2.0

Source: MIT Consortium for Kerberos and Internet Trust, https://kit.mit.edu
AM1.0 vs AM2.0

- Complex and feature-rich
- Usually proprietary
- Mobile/API-unfriendly
- Brittle deployment architecture
- Not agnostic to authn method
- Hard to source distributed policies
- Usually coarse-grained

- RESTful and simpler
- Standard interop baseline
- Mobile/API-friendly
- Just call authz endpoints vs. deploying an agent
- Agnostic to authn method and federation usage
- Flexible in policy expression and sourcing
- Leverages API’s “scope-grained authorization”
Enterprise UMA case study
What vendors are saying and doing about UMA

Further reading: tinyurl.com/uma1iop
NuveAM by Cloud Identity

• UMA-compliant AS:
  – Access control to Web data
  – API security and management
  – Real-time monitoring and audit

• Use cases: Securing Personal Data Services (PDS) and access management 2.0 (API security)

• Uses open standards, including UMA, OAuth 2.0, OpenID Connect, and SAML 2.0

• Open source frameworks: Java and Python
• Support for mobile (Android)
• Integrates with Identity Management and Identity Federation

http://www.cloudidentity.co.uk/products/nuveam
NuveAM by Cloud Identity

Open Standards
- REST
- OAuth 2.0
- OpenID Connect
- UMA

Protected Applications
- Cloud APIs
- Data Repositories
- Enterprise APIs

Client Applications
- Mobile Applications
- Corporate Systems
- Cloud Applications

LOGIN
LDAP / Active Directory

IDM

nuve

nuve

nuve

Manage Access Control

Audit

Authorize Access to Data and APIs

Protect Data / APIs and Verify Access Requests

Users
NuveAM for the enterprises

- Management of resources, APIs, permissions, and access control policies
- Access control on demand
- Detailed audit information
- Application management: resource servers and clients (with NuveLogin)
- Integration with identity management
- Integration with identity federation and SSO
NuveAM for the enterprises

Home » History
Filter events: All / Authorizations / Resources / Policies

- You added James Martin (Minor Injuries Unit) to sharing settings of Chest X-Ray Images with comments
  18:45:40 19.03.2014 (show details)

- 🔄 John Smith accessed one of your resources using Minor Injuries Unit application.
  14:14:45 17.01.2014 (show details)

- 🔄 John Smith accessed one of your resources using Minor Injuries Unit application.
  14:14:45 17.01.2014 (show details)

- You accessed Chest X-Ray Images with comments using Health Analysis App application.
  Resource name: Chest X-Ray Images with comments
  Resource server: eHealth Vault
  Requester: Health Analysis App
  Access date: 14:14:45 17.01.2014
  14:14:45 17.01.2014 (hide details)
NuveAM for the enterprises
Next steps
Next steps for the WG…and you

• Get involved!
  – Become an “UMAnitarian” (it’s free)
  – Participate in the interop and our implementation discussions
  – Follow and engage with @UMAWG on Twitter

• Current work:
  – Technical: claim profiling to allow claim-gathering using SAML, OpenID Connect, LDAP…
  – Business: Binding Obligations spec to tie “terms of authorization” to multi-party state changes

• Stay tuned for another webinar in Q2
Questions? Thank you!

@UMAWG
#UMAam20 for questions
20 March 2014
tinyurl.com/umawg for slides, recording, and more