Single Sign On: Are we there yet?

Work In Progress
Annual Computer Security Applications Conference
December 08, 2004

Rafae Bhatti, Elisa Bertino, Arif Ghafoor
Electrical and Computer Engineering, And CERIAS
Purdue University
Outline

- Single Sign On - An Overview
- Building Blocks and Challenges
  - Federated Identity
  - Privilege Management
- Integrated Approach
Why Single Sign On (SSO)?

- “Today’s collaborative and interconnected e-business landscape requires a secure and effective way to share trusted user identities”,
  RSA Security, Federated Identity whitepaper
Example from the RSA Security Whitepaper
SSO.. so where’s the challenge?

- An industry estimate puts identity theft as a $2 trillion criminal industry by year 2005.

Aren’t current SSO solutions enough?

- No, The problem definition is incomplete!!

- “Today’s collaborative and interconnected e-business landscape requires a secure and effective way to share trusted user identities” and entitlements.

- “We must further elaborate the interplay between authentication and authorization rather than following the classical approach and treating them as orthogonal issues. We must also refine existing access-control models to reflect the obligations on the provider and consumer of identities in multiparty transactions.”

Who’s concerned?

- Results from a recent industrial survey
- Integration of access management with identity federation solutions is crucial!
Outline

- Single Sign On - An Overview
- Building Blocks and Challenges
  - Federated Identity
  - Privilege Management
- Integrated Approach
Federated Identity

What are the issues …?

All implemented solutions are identity-based; has implications on scalability in open systems.

All known solutions (including the popular Passport) are centralized, an architecture that has been labeled by Rubin et.al. as antithetical to the distributed nature of the Internet.

Is that all …?

No, there remain other issues (Trust, Anonymity, Privacy, ..).
What is being done …?

- Emerging federated identity standard (SAML); adopted by Liberty Alliance
- SAML provides decentralized but identity based authentication
- Integration with privilege management still an open issue
What are the issues …?

Granting single sign on access to collection of resources with different (possibly contradictory) access protection rules

Trend for Web-migration requires revisiting the existing specifications for suitability to open Internet environment

Buell, Sandhu, Guest Editors Introduction, IEEE Internet Computing, Special Issue on Identity Management, November/December 2003
What is being done …?

- Recently proposed access management framework (X-GTRBAC) based on role based access control
- X-GTRBAC designed to provide decentralized access management in open systems; supports attribute based access control
- XML-based specification suitable to Web-based environments and integration with other XML-based specifications (such as SAML)
Outline

- Single Sign On - An Overview
- Building Blocks and Challenges
  - Federated Identity
  - Privilege Management
- Integrated Approach
Integrated Approach

Software architecture for an integrated federated identity and privilege management solution
Rafae Bhatti

- rafae@purdue.edu
- http://web.ics.purdue.edu/~bhattir/academics/