FAME-PERMIS Project

Flexible Authentication Middleware Extension to PERMIS

Alexandra Nenadic
School of Computer Science, University of Manchester
What it FAME-PERMIS about?

• FAME-PERMIS is a collaboration between University of Manchester and University of Kent

• FAME stands for:
  – Flexible
  – Authentication
  – Middleware
  – Extension (to)

• PERMIS
  – Policy-based decision engine for user authorisation
  – Currently, PERMIS authorisation decisions are made based upon:
    {Subject, Target, Action}
FAME-PERMIS Objectives

- Currently, there is no linkage with user’s authentication level (i.e. whether user used PIN, password, certificate, smart card, biometric device etc. to authenticate)

- Link the strength of authentication method with access control decision making provided by PERMIS

- Extend PERMIS:
  - {Subject, Target, Action, LoA}
  - LoA – Level of Assurance in authentication
FAME-PERMIS Objectives – cont’d

• Support multi-factor authentication
  – Freedom to choose from several authentication methods
  – When user is away or does not have all the technology required for authentication (e.g. card reader or biometric device), he/she may choose different authentication method
  – Combine several authentication methods to gain higher LoA

• Not inventing authentication methods, but combining the existing, as “one-method-fits-all” may not be suitable for dynamic e-environments and fine-grained access-control

• Use JISC-adopted Shibboleth infrastructure to implement FAME-PEMIS
Why FAME-PERMIS?

- Why do we need LoA (Level of Assurance)?
- Users can get different access privileges to the same resource based on the authentication method used
- To access some resources, such as e-library, IP address can be sufficient if inside campus
- Other resources, such as exam papers, may require stronger form of authentication, e.g. username and password
- Medical doctors accessing confidential patients’ data should use even stronger authentication methods, such as public-key certificates
Shibboleth Infrastructure

1. Give me access to RESOURCE
2. Authenticate with your ORIGIN
3. Who are you?
4. I am joe, my credential
5. Authenticate joe, OK
6. Here is your handle, go to TARGET
7. Here’s the handle, what can you tell me about the user?
8. Selected joe’s attributes
9. Here are attributes is user allowed access RESOURCE?, OK
10. RESOURCE
How FAME-PERMIS fits into Shibboleth

1. Give me access to RESOURCE

3. Who are you?

6. Here is your handle, go to TARGET

4. I am joe, my credential

10. RESOURCE

7. Here’s the handle, what can you tell me about the user?

8. Selected joe’s attributes

+ LoA

+ min. LoA

 RESOURCE, e.g. a web page, protected by Shibboleth

Authorization engine, e.g. PERMIS

TARGET

USER, joe

Local Authentication System #n – LoA #n

ORIGIN

Shibboleth- ORIGIN

5. Authenticate joe, OK

TARGET

Shibboleth-TARGET

Local Authentication System #n – LoA

ORIGIN

Local Authentication System
How We Define LoA for Authentication?

• Based on NIST (National Institute of Science and Technology) draft from January 2004: “Recommendation for Electronic Authentication”

• NIST defines 4 Levels of Assurance (LoAs):
  – Level 1 (lowest) to Level 4 (highest)
  – Defined in terms of
    • Strength of cryptographic techniques used, and
    • Strength of authentication tokens used
  – Authentication token is a credential presented by user and used in authentication – PIN, password, certificate, etc.
## Authentication tokens and Their LoAs

<table>
<thead>
<tr>
<th>Authentication token</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard token</td>
<td>✓</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Soft token</td>
<td>✓</td>
<td>✓</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Zero-knowledge password</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>One-time password</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Strong password</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summary

- FAME-PERMIS
  - Flexible Authentication Middleware Extension to PERMIS
- Link the strength of authentication method with access control decision making provided by PERMIS
- Support multi-factor authentication with multiple LoAs
- Use existing authentication systems
- Build on top of JISC-adopted Shibboleth infrastructure
Contacts and Further Information

• School of Computer Science, University Of Manchester
  – Dr. Ning Zhang
  – E-mail: nzhang@cs.man.ac.uk

• Department of Computer Science, University of Kent
  – Prof. David Chadwick
  – E-mail: d.w.chadwick@kent.ac.uk

• www.fame-permis.org