Web Services Security and Federated Identity Management

Birgit Pfitzmann, bpf@zurich.ibm.com
with Thomas Gross

March 8, 2005

www.zurich.ibm.com
Federated Identity Management (FIM)

Roles

Collection, recognition
- Allowed?
- Efficient?
- Verified?

Exchange
- Possible?
- Allowed?
- Efficient?
What’s New?

Scientifically
Standards
Management

Federated single sign-on

Nothing.
(Event-based directory integration)

XML-based.
(DSML, SPML, WS-Provisioning)

More liability and privacy issues

Pure browser case.
(Else 3-party authentication)

• Also WS versions
• Also more attributes

• More liability and privacy issues
• Metadata exchange
Literature

- Korman/Rubin 00: Passport problems
- Pfitzmann/Waidner 02 etc.: Privacy
- Pfitzmann/Waidner 02, Gross 03: Liberty and SAML problems
- Gordon et al: WS protocols, but not FIM
- Gross/Pfitzmann 04: Positive analysis of WSFPI
Attack Example: SAML Artifact Profile

0. Browse, redirect

1a. Authenticate user

2. Redirect to D & artifact

3. GET ... & artifact

4. SAML Request w/ artifact

5. SAML Response: assertion

6. Result page
A Multi-Layer Vulnerability

1a. Authenticate user

2. Redirect to D & artifact

3. GET ... & artifact

6. Error page with non-SSL link

7. GET non-SSL page

HTTP Referer: URL w/ artifact

Interrupts channel $D \leftrightarrow S$

Gets artifact

Impersonates $U$ at $D$
What Can We Hope to Prove?

- Vulnerable operational environment
  - Based on passwords
  - Fake-screen attacks easy
  - Browser security assumed
  - OS security assumed
- Identity provider can impersonate user
- Privacy can be good except
  - Not anonymity AND certified attributes
  - Id supplier learns trail of id consumer URIs

Here: Secure channel establishment under appropriate operational assumptions
Privacy Overview

Attributes about a person P are only given to an organization O, used there, or forwarded with P’s consent.

- **“Standard” implication**
  - Explicit privacy policy for attributes (exceptions by law)

- **Special cases:**
  - Attribute = ID  \(\Rightarrow\)  Multiple roles
  - Attribute = URL  \(\Rightarrow\)  Traffic privacy
  - O = wallet holder  \(\Rightarrow\)  Allow multiple wallets, in particular local wallets
The WSFPI Protocol – Basis for a Proof

WSFPI ≈ Interop Profile

WS-Fed Passive  WS-Fed Active

WS-Federation

Other WS-Sec*  HTTPS  Tokens
Proof Challenges

- Browsers and users
  - Browser as protocol party – restricted abilities
  - User also a protocol party – zero-footprint browser contains no identity
  - Browser and user might leak “protocol-internal” secrets

- Modularity, e.g., use of secure channels and SAML tokens

- Standard-style presentations
  - We prove rigorous instantiation
WSFPI: Correct Message Flow

0. Browse
4. Redirect(URIₘ, (wa, wtrealm, [wreply, wctx, wct])

5. Authenticate user
   a' := wreply or wtrealm;
   wresult := sign(nameₘ, (URIₘ, URIₙ, idₜ))

6. POSTForm(a', (wresult, [wctx]))

7. POST

Verify ...

10. Response

Secure channel
Structure of the Proof

Proof of Secure Channel Establishment

Precise Protocol Definition

Submodules

Security Assumptions

Trust Scenario
Summary and Outlook

- **FIM**: 3-party authentication, often with attribute exchange
- First protocol proof exists
- Next steps:
  - Relate assumptions to more detailed browser and user models
  - Use such models as criteria for browser evaluation
- **Privacy**:  
  - Protocols *can* achieve privacy with 2 exceptions  
  - For private use, GUI and policies equally important