Referencing and Validating User Attributes


Kumiko Ono and Henning Schulzrinne
{kumiko, hgs}@cs.columbia.edu
A Simple Mechanism for Trait-based Authorization[1]

- Helps recipients identify a “good” SIP request carrying a dubious originator’s AoR (= caller ID)
  - Unknown to the recipient or privacy-blocked
  - Unauthenticated SIP URI
  - tel-URI
    - Allows the originator choice of which AoR to use

- Easy and flexible deployment with moderate security
  - No need for binding user attributes to the user’s AoR
    - No need for an authenticated originator’s AoR, unlike SIP SAML assertions[2]
    - No support or prevention of delegation

- Privacy-aware
  - Supporting selective disclosure of user attributes
  - Limiting verifiers without needing to disclose their AoRs

[1] RFC4484
[2] draft-ietf-sip-saml-08.txt
Service Architecture

Attribute Validation Server (AVS): Issuer
e.g., members.ieee.org

ARID (Attribute Reference ID):
generated upon UAC's request and short-lived.
e.g., URL/Hash(username||expiry time||disclosure_mode||nonce||querier)
https://members.ieee.org/17750c5cbac9979171991d505d2e634e727d8d9b

HTTP over TLS
SIP over TLS

UAC
Alice
Member of IEEE
tel:+12345678

UAS: Relying Party
Bob
Accepts calls from IEEE members;
does not know Alice
sips:bob@example.com

1. Requests and obtains an ARID
2. Makes a call with the ARID
3. Queries the ARID's validity and receives user attributes
Using SAML Assertions for SIP

SAML or Attribute Authority: Issuer
e.g., members.ieee.org

Authentication Server
e.g., voip.cs.columbia.edu

1. Makes a call

Connected with alliance

2. Requests and obtains a reference to a SAML assertion

{Alice’s username, credentials, attributes}

3. Forwards the call request including the ref. to the SAML assertion

4. Dereferences the ref. to the SAML assertion and receives user attributes

Authentication Server

HTTP over TLS
SIP over TLS

UAC
Alice
Member of IEEE
tel: +12345678
and sips:alice@cs.columbia.edu

UAS: Relying Party
Bob
Accepts calls from IEEE members; does not know Alice
sips:bob@example.com
## Using ARID vs. SIP-SAML

<table>
<thead>
<tr>
<th></th>
<th><strong>Using ARID</strong></th>
<th><strong>SIP-SAML</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust model</td>
<td>Alice ↔ Issuer</td>
<td>Alice ↔ Issuer</td>
</tr>
<tr>
<td></td>
<td>Bob → Issuer</td>
<td>Bob → Issuer, Authentication server for Alice ↔ Issuer</td>
</tr>
<tr>
<td>Need for binding to</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>user’s AoR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How to protect</td>
<td>Sending over TLS</td>
<td>Sending over TLS</td>
</tr>
<tr>
<td>confidentiality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How to protect</td>
<td>Sending over TLS</td>
<td>Attaching a digital signature &amp; TLS</td>
</tr>
<tr>
<td>integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selective disclosure</td>
<td>Yes</td>
<td>Possible, but not defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricting verifiers</td>
<td>Yes, by hashing user’s AoR with a salt</td>
<td>Possible, but needs a minor modification in SAML for</td>
</tr>
<tr>
<td>with protecting user’s</td>
<td></td>
<td>privacy</td>
</tr>
<tr>
<td>privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How to convey in SIP</td>
<td>By reference: the Issuer’s URL in *a new Sender-</td>
<td>By reference: the Issuer’s URL in *a new token-info</td>
</tr>
<tr>
<td></td>
<td>References header* along with parameters for privacy</td>
<td><em>URL parameter of From header</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>By value: attached in the message body</td>
</tr>
</tbody>
</table>
Is Lack of Binding of User Attributes and the User Identity a Problem?

- **User attributes**
  - Issued to a person by one or more organizations
  - Can be authenticated by the issuer

- **A user’s identity in communication services (= user’s AoR)**
  - Issued to a person or to a device by a communication service provider
  - Usually different from the issuer of user attributes
  - Can be authenticated by the issuer and others by checking reachability

- **Both**
  - Each person has multiple AoRs and attributes
  - The value & trustworthiness depends on the issuer
  - Vary in lifetime
  - Often included in a user’s profile without authentication by the issuer
Is Lack of Binding of User Attributes and the User Identity a Problem? (cont’d)

- Validating user attributes NOT being bound to the user’s AoR
  
  **Pros:** Easier and flexible deployment, privacy-awareness
  
  - Any attribute issuers can provide validation services without alliance
  - Does not require the deployment of user’s AoR authentication services for recipients
  - Avoids unnecessary disclosure of the user’s AoR

- **Cons:** Weaker security?
  
  - Lack of individual accountability
    - Often care about affiliation, not caller identity (e.g., bank or government agency)
  - Threat of forwarding attacks using a received ARID
  - Threat of impersonation using a given or stolen ARID
Summary

- **We propose a simple mechanism for verifying user attributes:**
  - For trait-based authorization, especially for helping recipients identify a “good” SIP request regardless of the originator’s AoR
  - Focusing on easy and flexible deployability
    - No need for any alliances between a SIP authentication server and the issuer of user attributes
    - Trivially built using standard HTTPS LAMP setup, without special crypto setup
    - UAC: no multi-part SAML attachment, just an HTTPS query
- **The requirements and a solution using SAML assertions were discussed in the SIP community years ago**
  - But no apparent deployment
- **Does the community have interest in a more deployable solution?**