Referencing and Validating User Attributes

http://www.ietf.org/internet-drafts/draft-ono-dispatch-attribute-validation-00.txt

Kumiko Ono and Henning Schulzrinne
{kumiko, hgs}@cs.columbia.edu

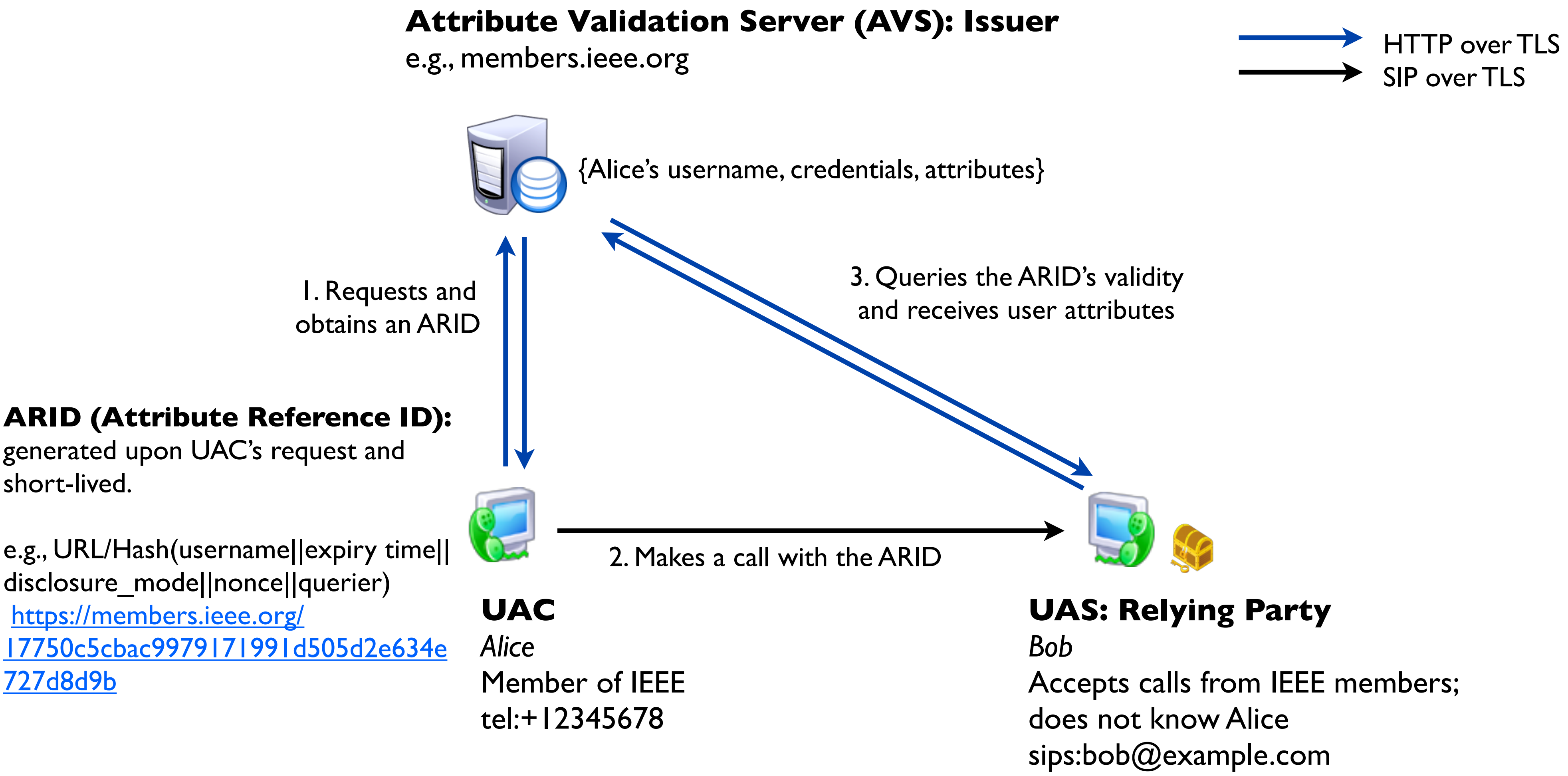
A Simple Mechanism for Trait-based Authorization[1]

- **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

→ HTTP over TLS
→ SIP over TLS

{Alice's username, credentials, attributes}

1. Requests and obtains an ARID

3. Queries the ARID's validity and receives user attributes

ARID (Attribute Reference ID):
generated upon UAC's request and short-lived.

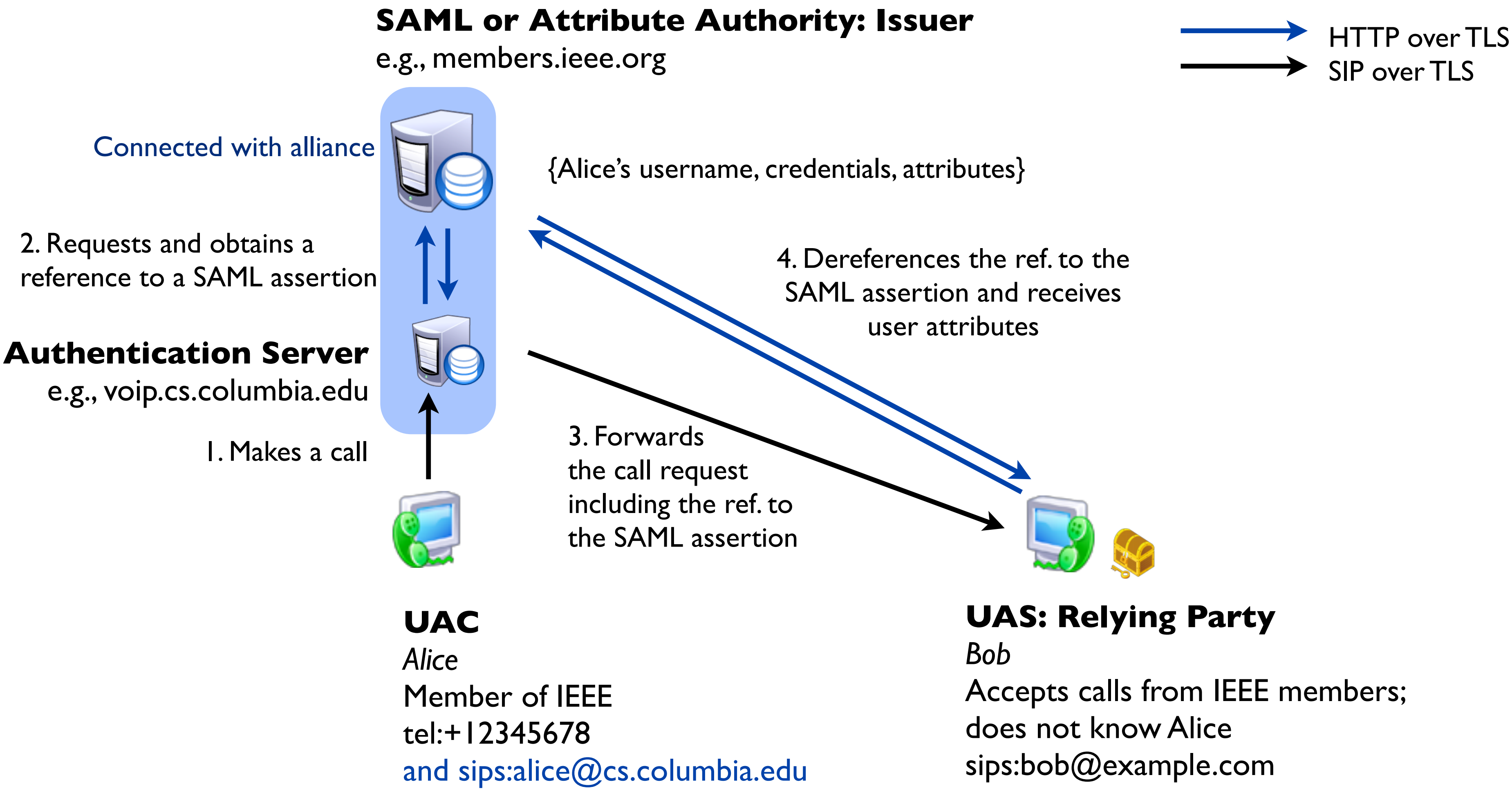
e.g., URL/Hash(username||expiry time||disclosure_mode||nonce||querier)
https://members.ieee.org/17750c5cbac9979171991d505d2e634e727d8d9b

2. Makes a call with the ARID

UAC
Alice
Member of IEEE
tel:+12345678

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

[Ref.]
Using SAML Assertions for SIP



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

HTTP over TLS
SIP over TLS

Connected with alliance

{Alice's username, credentials, attributes}

2. Requests and obtains a reference to a SAML assertion

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

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

1. Makes a call

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

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

	Using ARID	**SIP-SAML**
Trust model	Alice ⇔ Issuer Bob ⇒ Issuer	Alice ⇔ Issuer Bob ⇒ Issuer Authentication server for Alice ⇔ Issuer
Need for binding to user's AoR	No	Yes
How to protect confidentiality	Sending over TLS	
How to protect integrity	Sending over TLS	Attaching a digital signature & TLS
Selective disclosure	Yes	Possible, but not defined
Restricting verifiers with protecting user's privacy	Yes, by hashing user's AoR with a salt	Possible, but needs a minor modification in SAML for privacy
How to convey in SIP	By reference: the Issuer's URL in *a new Sender-References header* along with parameters for privacy	By reference: the Issuer's URL in *a new token-info URI parameter of From header* By value: attached in the message body

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?**