Protection and Security: Shibboleth

- Federated Authentication system using SAML for secure conversation
- Enables Single-Sign On to Web Pages and Portals
- Authentication is done by the user's home institution
  - Identity Provider (Origin)
- Authorisation (and access) is done by the resource

Outline

- What is the problem Shibboleth is trying to solve?
- What are the key concepts?
- How does the Shibboleth protocol work?
- What is the high-level Shibboleth architecture?
- How are attributes managed?
- Summary and references

Some philosophies of Shibboleth

- Federated Administration
  - A trust fabric exists between campuses, allowing each site to identify the other speaker, and assign a trust level
  - Provider sites are responsible for authenticating their users, but can use any reliable means to do this
- Access Control Based On Attributes
- Active Management of Privacy.
  - The Identity Provider (origin) site, and the browser user, control what information is released to the Service Provider (target)

Example problems that Shibboleth is intended to solve

- Campus A wants to share an on-line service (e.g., an on-line course, computing resource, …) to authorized users on Campus B
- Campus C wants to provide access to restricted digital content to members of a collaborative research group from many locations
- User X wants to access restricted digital content on AIDS research at a remote site for research purposes, but does not want to reveal his identity to the remote site for personal reasons.

5

More Example Problems

- Students use licensed library materials regardless of their location
- Want to allow users to access many types of resources but to maintain fewer accounts and passwords per user and between institutions
- Access based on roles instead of hard-coding of user names

6

Key Concepts

- Security
  - A goal is to protect servers, communications, networks, hosts, personal information
  - Each of these may have distinct authentication and authorization needs
    - networks (denial of service, physical infrastructure)
    - hosts (OS bugs, miss-settings, etc.)
    - personal information and communication (signed and encrypted email, directory protection, etc,)
  - some technologies (PKI, firewalls, etc.) can serve several areas

7

Key Concepts

- Authentication and Authorization
  - A user is **authenticated** when you are sure that the user is who he/she claims to be (e.g., that user logs in to an account with a password).
  - A user is **authorized** to use a resource if he/she is allowed to have access to it. Authorization always implies authentication.

⇒ Shibboleth separates the step of authentication and the step of authorization to use a resource.

8

Key Concepts

⇒ Authentication in the real world is hard because you have to *trust* the authenticator

- Trust
  - A goal of Shibboleth is to develop a continuum of trusted entities and community infrastructure trust models

9

Key Concepts

- Privacy
  - Passive privacy - The current approach
    - A user passes identity to a service, and then worries about the service's privacy policy. To comply with privacy, services have significant regulatory requirements.
  - Active privacy - A new approach.
    - A user (through their security domain) can pass attributes to the service that are not necessarily personally identifiable. If they are personally identifiable, the user decides whether to release them

A goal of Shibboleth is to move to active privacy

10

Key Concepts

- Continuum of Trust
  - Collaborative trust at one end
    - You can look at my calendar; students in Physics 201 at Brown can access this on-line sensor; members of the UWash community can access this licensed resource
    - Consequences are political or social; shorter term; structures tend to clubs and federations
  - Legal trust at the other end
    - Sign this document and guarantee that what was signed was what I saw; identity access to a high security area
    - Consequences include financial liabilities, legal process; structures tend to hierarchies and bridges

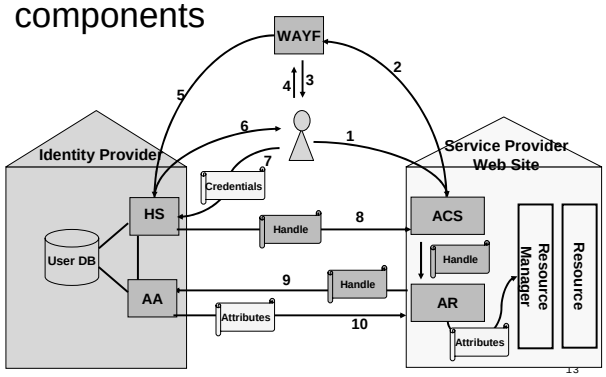
11

Interrealm Trust Structures

- Federated administrations
  - Basic bilateral (e.g., origin and target)
  - Complex bilateral; multilateral
  - Virtual organizations and Grids
- Trust hierarchies
  - Certificate Authorities are trusted by users and service providers
  - May assert formal or stronger trust than federations
  - Bridges and policy mappings are required to connect hierarchies
  - Appear larger scale than federations

12

Simple view of Shibboleth components



13

Key Concepts

- Brokering authorization and authentication
  - The Identity Provider is a broker of authentication and authorization between the user and the service provider, respecting security and privacy, in an appropriate trust fabric
  - Authenticate a user using a local (campus) authentication mechanism, and send a handle to a service provider

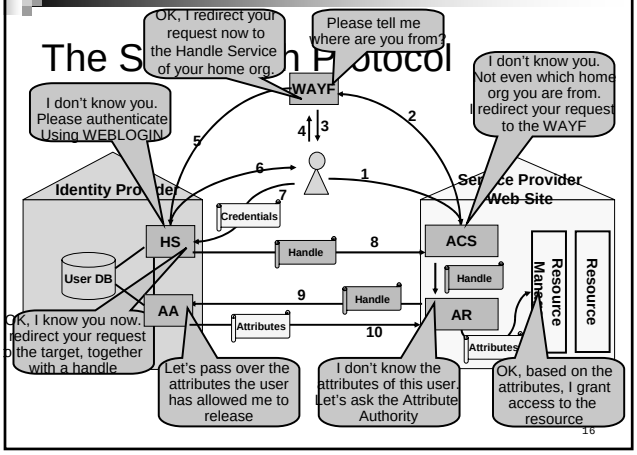
14

Key Concepts

- Trust in transactions
  - The user trusts the Identity Provider (origin) to faithfully represent its attributes to targets and obey privacy rules
  - The Identity Provide trusts the user to obey its authentication and authorization rules
  - The Service Provider (target) trusts the origin to accurately manage and communicate user attributes and respect the user's privacy settings
  - The Identity Provider trusts the target to take the appropriate transaction actions and to not misuse the user's information.

15

The Shibboleth Protocol



16

High Level Architecture

- Federations provide common Policy and Trust
- Service and Identity Provider site collaborate to provide a privacy-preserving "context" for Shibboleth users
- Identity Provider site authenticates user, asserts Attributes
- Service Provider site requests attributes about user directly from Identity Provider site
- Service Provider site makes an Access Control Decision
- Users (and Identity Provider organizations) can control what attributes are released

17

Trust, and Identifying Speakers

- Federations distribute files defining the trust fabric
- Individual sites can create bilateral trust
- When a Service Provider receives a request to create a session, the Authorization Assertion must be signed by the Identity Provider (using PKI validation), and must be a member of a common Federation.
- When an Identity Provider receives a request for attributes, it must be transported across SSL.
- The name of the Requestor (from the certificate) and the name of the user (mapped from the Handle) are used to locate the appropriate ARP.

18

Technical Components

- Identity Provider Site – Required Enterprise Infrastructure
  - Authentication
  - Attribute Repository
- Identity Provider Site – Shibboleth Components
  - Handle Server
  - Attribute Authority
- Service Provider Site - Required Enterprise Infrastructure
  - Web Server (Apache or IIS)
- Service Provider Site – Shibboleth Components
  - Assertion Consumer Service - SHIRE
  - Attribute Requester - SHAR
  - Resource Manager
- Where Are You From Service - WAYF

19

Managing Attribute Release Policies

- **The Attribute Authority provides ARP management tools/interfaces.**
  - Different ARPs for different targets
  - Each ARP Specifies which attributes and which values to release
  - Institutional ARPs (default)
    - administrative default policies and default attributes
    - Site can force include and exclude
  - User ARPs managed via "MyAA" web interface
  - Release set determined by "combining" Default and User ARP for the specified resource

20

Typical Attributes in the Higher Ed Community

Affiliation	"active member of community"	member@washington.edu
EPPN	Identity	gettes@duke.edu
Entitlement	An agreed upon opaque URI	urn:mace:vendor:contract1234
OrgUnit	Department	Economics Department
EnrolledCourse	Opaque course identifier	urn:mace:osu.edu:Physics201

21

The Target Manages Attribute Acceptance

Rules that define who can assert what…..

- MIT can assert student@mit.edu
- Chicago can assert staff@argonne.gov
- Brown CANNOT assert student@mit.edu

22

Summary

- Shibboleth is a tool for enabling users at diverse sites to have secure, protected, and private access to remote services
- It brokers authentication and authorization through the use of local enterprise services
- It relies on a trusted fabric of federations and trust hierarchies
- It provides tools for managing the release and acceptance of attributes

23

References

- Ken Klingenstein (Internet2), Concepts & Scenarios, Shibboleth, Certs, and PKI Workshop Presentations
  http://www.stonesoup.org/Meetings/0201/shib.pres/kling.htm
- Michael Gettes (Georgetown, Duke), Introduction to Shibboleth
  http://www.educause.edu/asp/doclib/abstract.asp?ID=EAF0429
- http://shibboleth.internet2.edu

24