Authentication and Authorization in the Internet

Torsten Braun
Rechnernetze und Verteilte Systeme
Institut für Informatik und Angewandte Mathematik
Universität Bern

www.iam.unibe.ch/~rvs

Overview

- Internet Security Fundamentals
  - Authentication
    - 3-Way Handshake Authentication
    - Authentication Server
    - Public Key Authentication
  - Certificates
    - Trust Chains
  - Authorization
- Authentication & Authorization Problem
  - Example: VITELS

- SWITCH AAI Initiative
  - AAI Overview and Terms
  - AAI Model
    - Registration
    - Resource Access
  - Shibboleth
  - AAI Implementation
    - AAI enabled Software
    - AAI Mediators
      - AAI Proxy
      - AAI Portal
  - Further AAI Issues
  - Outlook
Authentication

- Identities can be spoofed easily.
- Authentication is the process of proving one’s identity to someone else.
- Authentication protocols based on
  - shared secrets, e.g. passwords
  - authentication servers, e.g. Kerberos
  - public keys
Handshake Authentication

- Client and Server Handshake Key (CHK/SHK) calculated from shared secret (password).
- Problem: Client needs a password for each server.

\[
\begin{align*}
\text{Client} & \quad \text{Server} \\
\text{ClientID, } E(x, \text{CHK}) & \quad \text{E}(x+1, \text{SHK}, \text{E}(y, \text{SHK}) \\
& \quad \text{E}(y+1, \text{CHK}) \\
& \quad \text{E}(K, \text{SHK})
\end{align*}
\]

x, y: random
K: session key
- Shared secret keys between A and S, B and S
- Terminology
  - Timestamp T
  - Lifetime L
  - Session key K
  - Ticket
- Problem: A and B need shared secrets with same authentication server

Diagram:

- S
- Client A
- Server B

- $E((T,L,K,B), K_A)$
- $E((T,L,K,A), K_B)$
- $E((A,T), K)$
- $E((T,L,K,A), K_B)$
- $E(T+1,K)$
Problem:
A must be sure that the public key really belongs to B.

→ Certificate
   (Confirmation - issued by certification authority, CA - that public key belongs to a certain identity.)
October 17, 2003

Torsten Braun (U Bern): Authentication and Authorization in the Internet

Certificates

Client

- Client-ID
  - Public client key
  - Signature

Certification Authority (CA)

- Client-ID
  - Public client key
  - Signature

Communication Partner

- Client-ID
  - Public client key
  - Signature

Hash

secret CA key

public CA key
Trust Chains

- X provides certificate for Y.
- Y provides certificate for B.
- A knows public key of X and can verify certificate for Y from X.
- A knows then public key of Y and can verify certificate for B from Y.
- Organisation of trust chains in hierarchical trees
Authorization

- Authorization is the process to decide whether an authenticated user is allowed to access or perform operations on a resource.
- Authentication might be a basis for authorization, if that is based on user identities.
- Problems of authorization schemes
  - User accounts with high administration overhead
  - Credentials need to be delivered to servers
  - Fine-grained access control is often impractical
    - Examples: on-line libraries, distance learning courses
- Requirements for authorization
  - Scalability for resource administrators
  - Convenience for users, e.g. single login / password at home organization
**Problem:** Many users - many resources - many organizations
Virtual Internet and Telecommunications Laboratory of Switzerland (www.vitels.ch)

- Distributed resources
  - Network laboratories at several universities
  - Course server and web servers
- Distributed users from different organizations
SWITCH AAI Initiative

- **Authentication and Authorization Infrastructure**
- 2001/2002: study phase
- early 2003: selection of Shibboleth middleware (Internet 2) as basis for implementation
- currently: pilot implementation projects

[www.switch.ch/aai](http://www.switch.ch/aai)
AAI Overview and Terms

- Trust relationship between two organizations (home organization and resource owner) is extended to trust relationship between user and resource owner.
  - Users authenticate to home organization only!
  - Resource owners grant access to resource based on information about users (authorization attributes)

- Home Organization
  - Representative of a user community, e.g. universities, libraries, university hospitals etc.

- Resource
  - Application, web site, network, system, remote laboratory, etc.

- Resource Owner
  - Entity owning a resource and offering resource access to users
AAI Model: Registration

Legend:
- **data**
- **system**
- **Pre-processing**

1. Registration

User's Home Organization

User DB

Registration

Info (name, address, ....)

User

Resource Owner

Access Control Definition

Access Control Manager

Resource

Legend:
AAI Model: Resource Access

Legend:
- data
- system
- AAI-interaction
Shibboleth

- AAI solution of Internet2 / MACE
  (Middleware Architecture Committee for Education)
  - middleware.internet2.edu/MACE/
  - shibboleth.internet2.edu

- Components
  - SHIRE: Shibboleth Indexical Reference Establisher
    - Intercepts resource requests
  - SHAR: Shibboleth Attribute Requester
    - contacts AA to fetch authorization attributes of a user
  - WAYF: Where Are You From server
    - redirects user back to HS of home organization
  - HS: Handle Server
    - authenticates user locally and provides opaque handle identifying a user
  - AA: Attribute Authority
    - retrieves attributes (according to user's release policy) and passes them to SHAR
Shibboleth AA Process

1. Resource Owner
2. WAYF
3. Please tell me where you come from
4. I don’t know you. Not even which home org you are from. I redirect your request to the WAYF
5. I don’t know you. Please authenticate yourself
6. OK, I know you now. I redirect your request now to the Handle Service of your home org.
7. I don’t know you. Please authenticate yourself
8. OK, I redirect your request now to the Handle Service of your home org.
9. Let’s pass over the attributes the user has allowed me to release
10. OK, based on the attributes, I grant access to the resource
AAI enabled Software

Resource Owner

Application, e.g. Web Server, WebCT Vista
AAI Mediators

- Problem: Resources are not AAI aware
- Solutions: AAI Mediator
  - AAI Proxy
    - User is transparent for the resource
    - Resource access via proxy
    - Example: Access to on-line libraries are often based on IP addresses.
  - AAI Portal
    - provides user information in the form required by resource
    - Direct resource access
    - Examples: web and course servers
Torsten Braun (U Bern): Authentication and Authorization in the Internet

AAI Proxy

Resource Owner

Web Server “Black Box”

AAI Proxy (Web Proxy)
Torsten Braun (U Bern): Authentication and Authorization in the Internet

AAI Portal

AAI

Portal database

Resource Owner

Resource

sign on

data base

sign on

AAI Portal

portal

cloud.
AAI Portal Implementation

- SVC Mandate „SWITCH Pilot 1“
- Access to AAI portal by
  - Resource users
  - Resource administrators
    - Definition of resources and access rules
  - Portal administrators
- API allows to read/write user/resource data from/to AAI portal database.
- AAI portal with interfaces (adaptors) to AAI and resources, e.g.
  - Shibboleth adaptor
  - WebCT resource adaptor
    - Generation of WebCT user
    - Course subscription
    - Login on behalf of user
    - Redirection to course page
Demo

aaitest1.unibe.ch
Further AAI Issues

- Certification authorities
  - Root CA at SWITCH
- Definition of authorization attributes
- Non-technical issues
  - Legal
  - Financial
Acknowledgements

Thanks to

- Christoph Graf (SWITCHaai project leader)
- SWITCH and AAI working groups
- AAI portal design and implementation team at Universities of Basel, Bern and SWITCH
- Swiss Virtual Campus for supporting the AAI pilot mandate
- Audience for listening