Internet Authentication Protocols

Chapter 23

Mutual Authentication

Alice

$\tau_A$ (Alice’s challenge)

$\{\tau_A\}K_{AB}$ (Bob’s response)

$\tau_B$ (Bob’s challenge)

$\{\tau_B\}K_{AB}$ (Alice’s response)

Bob
Mutual Authentication

- **Problem** – How to share the key?
- **Solution** – Mediated Authentication
  - Secret key based protocols
    - Needham – Schroeder protocol & Kerberos
    - Trusted third party generates and distributes shared secret key
  - Public key based
    - X.509 Directory authentication service
    - Trusted third party certifies public key

Needham-Schroeder Protocol

<table>
<thead>
<tr>
<th>Message #</th>
<th>Direction</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Alice → S</td>
<td>A, B, N,A</td>
</tr>
<tr>
<td>02</td>
<td>S → Alice</td>
<td>{N,A, B, Ks, KNs, AKsNkA, Ks}</td>
</tr>
<tr>
<td>03</td>
<td>Alice → Bob</td>
<td>{Ks, AKs}</td>
</tr>
<tr>
<td>04</td>
<td>Bob → Alice</td>
<td>{N, Ks}</td>
</tr>
<tr>
<td>05</td>
<td>Alice → Bob</td>
<td>{N – 1}, Ks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symbols Used</th>
<th>What they mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>A, B, S</td>
<td>Publicly known identifiers of Alice and Bob and the trusted third party S</td>
</tr>
<tr>
<td>N_x</td>
<td>A random number unique to identity X</td>
</tr>
<tr>
<td>Ks, Kx</td>
<td>Secret key shared between Alice &amp; S, and between Bob &amp; S</td>
</tr>
<tr>
<td>Ks, Kx</td>
<td>Session key generated by S and distributed to Alice and Bob</td>
</tr>
<tr>
<td>{V}Kx</td>
<td>The item V encrypted with key Kx</td>
</tr>
</tbody>
</table>

Kerberos – Improved Needham-Schroeder Protocol

- Trusted key server system from MIT
- Provides centralised private-key third-party authentication in a distributed network
  - Allows users access to services distributed through network
  - Without needing to trust all workstations
  - Rather all trust a central authentication server
- Provides Single Sign-on
- Two versions in use: 4 & 5
Kerberos Overview

- Third-party authentication scheme involving
- Authentication Server (KDC / AS)
  - Users initially negotiate with AS to identify self
  - AS provides a non-corruptible authentication credential (ticket granting ticket TGT)
- Ticket Granting Server (TGS)
  - Users subsequently request access to other services from TGS using the TGT

Kerberos Version 5

- Kerberos v4 is most widely used version
- Also have v5, developed in mid 1990’s
  - Specified as Internet standard RFC 1510
- v5 provides improvements over v4
  - Addresses environmental shortcomings
    - Encryption alg, network protocol, byte order, ticket lifetime, authentication forwarding, inter-realm auth
  - And technical deficiencies
    - double encryption, non-std mode of use, session keys, password attacks
Kerberos Inter Realm Authentication

- A Kerberos “Realm” consists of:
  - A Kerberos server including TGS
  - A number of clients, all registered with server
  - Application servers, sharing keys with server
  - Typically a single administrative domain
- If multiple realms, their Kerberos servers must share keys and trust

Kerberos Inter Realm Authentication

X.509 Authentication Service

- Universally accepted standard for formatting public-key certificates
  - Widely used in network security applications, including IPSec, SSL, SET, and S/MIME
- Part of CCITT X.500 directory service standards
- Uses public-key crypto & digital signatures
  - Algorithms not standardised, but RSA recommended
Certificate Authorities

- Certificate consists of:
  - A public key plus a User ID of the key owner
  - Signed by a third party trusted by community
  - Often govt./bank **certificate authority** (CA)
- Users obtain certificates from CA
  - Create keys & unsigned cert, gives to CA, CA signs cert & attaches sig, returns to user
- Other users can verify cert
  - checking sig on cert using CA's public key

X.509 Certificates
Public Key Infrastructure

Identity Management

Federated Identity Management

- Use of common identity management scheme
  - Across multiple enterprises & numerous applications
  - Supporting many thousands, even millions of users
- Principal elements are:
  - Authentication, authorization, accounting, provisioning, workflow automation, delegated administration, password synchronization, self-service password reset, federation
- Kerberos contains many of these elements
Standards Used

- Extensible Markup Language (XML)
  - characterizes text elements in a document on appearance, function, meaning, or context
- Simple Object Access Protocol (SOAP)
  - for invoking code using XML over HTTP
- WS-Security
  - set of SOAP extensions for implementing message integrity and confidentiality in Web services
- Security Assertion Markup Language (SAML)
  - XML-based language for the exchange of security information between online business partners