Chapter 22 – Internet Authentication Applications

First Edition
by William Stallings and Lawrie Brown

Lecture slides by Lawrie Brown
Internet Authentication Applications

- will consider authentication functions
- developed to support application-level authentication & digital signatures
- will consider
  - Kerberos private-key authentication service
  - X.509 public-key directory authentication
  - public-key infrastructure (PKI)
  - federated identity management
Kerberos

- 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
- two versions in use: 4 & 5
Kerberos Overview

- a basic third-party authentication scheme
- have an Authentication Server (AS)
  - users initially negotiate with AS to identify self
  - AS provides a non-corruptible authentication credential (ticket granting ticket TGT)
- have a Ticket Granting server (TGS)
  - users subsequently request access to other services from TGS on basis of users TGT
Kerberos Overview

1. User logs on to workstation and requests service on host.
2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.
Kerberos Realms

- a Kerberos environment consists of:
  - a Kerberos server
  - a number of clients, all registered with server
  - application servers, sharing keys with server
- this is termed a realm
  - typically a single administrative domain
- if have multiple realms, their Kerberos servers must share keys and trust
Kerberos Realms
Kerberos Version 5

- Kerberos v4 is most widely used version
- also have v5, developed in mid 1990’s
  - specified as Internet standard RFC 1510
- 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 Performance Issues

- see larger client-server installations
- query Kerberos performance impact
  - very little if system is properly configured
  - since tickets are reusable
- Kerberos security best assured if place its server on a separate, isolated machine
- administrative motivation for multi realms
  - not a performance issue
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 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
X.509 Certificates
Public Key Infrastructure
PKIX Management

- **functions:**
  - registration
  - initialization
  - certification
  - key pair recovery
  - key pair update
  - revocation request
  - cross certification

- **protocols:** CMP, CMC
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
Identity Management
Federated Identity Management

(a) Federation based on account linking

(b) Federation based on roles

(b) Chained Web Services
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
Summary

- reviewed network authentication using:
  - Kerberos private-key authentication service
  - X.509 public-key directory authentication
  - public-key infrastructure (PKI)
  - federated identity management