Chapter 23
Internet Authentication Applications

Kerberos Overview

• Initially developed at MIT
• Software utility available in both the public domain and in commercially supported versions
• Issued as an Internet standard and is the defacto standard for remote authentication
• Overall scheme is that of a trusted third party authentication service
• Requires that a user prove his or her identity for each service invoked and requires servers to prove their identity to clients
Kerberos Protocol

- Designed to counter a variety of threats to the security of a client/server dialogue
- Obvious security risk is impersonation
- Servers must be able to confirm the identities of clients who request service

Use an Authentication Server (AS)

- User initially negotiates with AS for identity verification
- AS verifies identity and then passes information on to an application server which will then accept service requests from the client

Authentication server (AS)
Ticket-granting server (TGS)

Host/application server

If client sends user's password to the AS over the network an opponent could observe the password

An opponent could impersonate the AS and send a false validation

Kerberos Realms

- A Kerberos environment consists of:
  - A Kerberos server
  - A number of clients, all registered with server
  - A number of application servers, sharing keys with server
- This is referred to as a realm
  - Networks of clients and servers under different administrative organizations generally constitute different realms
- If multiple realms:
  - Their Kerberos servers must share a secret key and trust the Kerberos server in the other realm to authenticate users
  - Participating servers in the second realm must also be willing to trust the Kerberos server in the first realm

Figure 23.1 Overview of Kerberos
Kerberos Versions 4 and 5

- Kerberos v4 is most widely used version
- Improvements found in version 5:
  - An encrypted message is tagged with an encryption algorithm identifier
    - This enables users to configure Kerberos to use an algorithm other than DES
  - Supports authentication forwarding
    - Enables a client to access a server and have that server access another server on behalf of the client
    - Supports a method for interrealm authentication that requires fewer secure key exchanges than in version 4

Kerberos Performance Issues

- Larger client-server installations
- Very little performance impact in a large-scale environment if the system is properly configured
- Kerberos security is best assured by placing the Kerberos server on a separate, isolated machine
- Motivation for multiple realms is administrative, not performance related
Certificate Authority (CA)

Certificate consists of:

• A public key with the identity of the key’s owner
• Signed by a trusted third party
• Typically the third party is a CA that is trusted by the user community
  (such as a government agency, telecommunications company, financial institution, or other trusted peak organization)

User can present his or her public key to the authority in a secure manner and obtain a certificate

• User can then publish the certificate or send it to others
• Anyone needing this user’s public key can obtain the certificate and verify that it is valid by way of the attached trusted signature

X.509

• Specified in RFC 5280
• The most widely accepted format for public-key certificates
• Certificates are used in most network security applications, including:
  o IP security (IPSEC)
  o Secure sockets layer (SSL)
  o Secure electronic transactions (SET)
  o S/MIME
  o eBusiness applications

A number of specialized variants also exist, distinguished by particular element values or the presence of certain extensions:

• Conventional (long-lived) certificates
  o CA and “end user” certificates
  o Valid for extended periods of months to years

• Short-lived certificates
  o Used to provide authentication for applications such as grid computing, while avoiding some of the overheads associated with conventional certificates
  o Typically valid for periods of hours to days, which limits the period of abuse if compromised
  o Because they are usually not issued by recognized CAs, there are issues with verifying them outside the issuing jurisdiction

• Proxy certificates
  o Widely used to provide authentication for applications such as grid computing, while addressing some of the drawbacks of short-lived certificates
  o Identified by the presence of the “proxy certificate” extension
  o May be used in conjunction with other certificate types
  o Allow a user to easily create a credential to access resources in some environment, without needing to provide their full certificate information

• Attribute certificates
  o Defined in RFC 5280
  o Use a different certificate format to link a user’s identity to a set of attributes that are typically used for administrative and system purposes
  o A user may have a number of different attribute certificates, with different sets of attributes for different purposes
  o Defined in the “Attribute” extension
Public-Key Infrastructure (PKI)

- The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography
- Developed to enable secure, convenient, and efficient acquisition of public keys
- “Trust store”
  - A list of CA’s and their public keys

![PKIX Architectural Model](Figure 23.4 PKIX Architectural Model)

![X.509 Formats](Figure 23.3 X.509 Formats)
Summary

- **Kerberos**
  - The Kerberos Protocol
  - Kerberos realms and multiple Kerberi
  - Version 4 and Version 5
  - Performance issues

- **X.509**

- **Public Key infrastructure**
  - Public Key infrastructure (PKIX)