**Identification and Authentication**

- Identification?
  
  **WHO ARE YOU?**

- Authentication?

- Authorization

**On-Line Identity**

*On the Internet, nobody knows you’re a dog.*

Copyright © 1993 The New Yorker

**Internet Authentication Applications**

- Application-level authentication and digital signatures

- Implementations:
  - Kerberos symmetric 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 secret-key third-party authentication in a distributed network
  - Allows users access to services distributed through network…
  - …without needing to trust all workstations
  - Instead all trust a central authentication server

- Two versions in use: 4 and 5

**Kerberos Overview**

- A basic third-party authentication scheme

- Two servers (possibly one one machine)

- Authentication Server (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 on basis of users TGT
Kerberos Overview

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 called a realm
  - typically a single administrative domain
- For 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 algorithm, network protocol, byte order, ticket lifetime, authentication forwarding, inter-realm authentication
  - and technical deficiencies
    - double encryption, non-std mode of use, session keys, password attacks

Kerberos Performance Issues
- Works with larger client-server installations
- Kerberos performance impact is very little if system is properly configured, since tickets are reusable
- Kerberos security is best assured if the server is a separate, isolated machine
- Motivation for multiple realms is administrative, not performance

Certificate Authorities
- A digital certificate consists of:
  - a public key plus ID of the key owner
  - signed by a third party trusted by community
  - often government/bank certificate authority (CA)
  - Goal: bind an identity to a public key
- Users obtain certificates from CA
  - User creates keys and unsigned certificate, gives to CA
  - CA signs certificate, returns to user
- Other users can verify certificate by checking signature on certificate 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 cryptography and 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

- Definition: use of a common identity management scheme:
  - Across multiple enterprises and 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
Federated Identity Management

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

Questions