Key Management

Dr. Arjan Durresi
Louisiana State University
Baton Rouge, LA 70810
Durresi@csc.lsu.edu

These slides are available at:
http://www.csc.lsu.edu/~durresi/csc4601-07/

Overview

- Distributions of Public Keys
- Public Key Authority
- Public Key Certificates
- Public-Key Distribution of Secret Keys

Key Management

- Public-key encryption helps address key distribution problems
- Have two aspects of this:
  - distribution of public keys
  - use of public-key encryption to distribute secret keys

Distribution of Public Keys

- Can be considered as using one of:
  - Public announcement
  - Publicly available directory
  - Public-key authority
  - Public-key certificates

Public Announcement

- Users distribute public keys to recipients or broadcast to community at large
  - eg. append PGP keys to email messages or post to news groups or email list
- Major weakness is forgery
  - anyone can create a key claiming to be someone else and broadcast it
  - until forgery is discovered can masquerade as claimed user

Uncontrolled Key Distribution
Publicly Available Directory

- Can obtain greater security by registering keys with a public directory
- Directory must be trusted with properties:
  - contains \{name,public-key\} entries
  - participants register securely with directory
  - participants can replace key at any time
  - directory is periodically published
  - directory can be accessed electronically
- Still vulnerable to tampering or forgery

Public Key Publication

Public-Key Authority

- Improve security by tightening control over distribution of keys from directory
- Has properties of directory
- And requires users to know public key for the directory
- Then users interact with directory to obtain any desired public key securely
  - does require real-time access to directory when keys are needed

Public-Key Certificates

- Certificates allow key exchange without real-time access to public-key authority
- A certificate binds identity to public key
  - usually with other info such as period of validity, rights of use etc
- With all contents signed by a trusted Public-Key or Certificate Authority (CA)
- Can be verified by anyone who knows the certificate authorities public-key

Public-Key Authority

Public-Key Certificates
**Public-Key Distribution of Secret Keys**

- Use previous methods to obtain public-key
- Can use for secrecy or authentication
- But public-key algorithms are slow
- So usually want to use private-key encryption to protect message contents
- Hence need a session key
- Have several alternatives for negotiating a suitable session

**Simple Use of Public Key Encryption to Establish a Session Key**

**Simple Secret Key Distribution**

- Proposed by Merkle in 1979
  - A generates a new temporary public key pair
  - A sends B the public key and their identity
  - B generates a session key K sends it to A encrypted using the supplied public key
  - A decrypts the session key and both use
- Problem is that an opponent can intercept and impersonate both halves of protocol

**Public-Key Distribution of Secret Keys with Confidentiality and Authentication**

- If have securely exchanged public-keys:

**Hybrid Scheme**

- KDC uses a public key scheme to distribute a secret master key
- KDC uses the secret master key to distribute session secret keys
- Performance: Distribution of session keys by public key encryption could degrade overall system. With a hybrid scheme public key is used only occasionally to update the master key
- When a single KDC serves a widely distributes set of users
- Used in IBM mainframes

**Summary**

- Distributions of Public Keys
- Public Key Authority
- Public Key Certificates
- Public-Key Distribution of Secret Keys
- Hybrid Schemes