Lecture VII: Public Key Infrastructure (PKI)

Internet Security: Principles & Practices

John K. Zao, PhD (Harvard) SMIEEE
Computer Science Department, National Chiao Tung University
Spring 2012
Problems with Public Key Cryptosystems

- Where & how can the public key for an entity be found?
- How to determine if a public key really belongs to whom it is supposed to?
- What is the legitimate use for a given public key? (e.g., signing checks, signing contracts)
- When is a public key no longer valid?
- How can you protect the corresponding private keys?
- What happens if a private key is lost?

Solution

- Use Public Key Certificates and Public Key Infrastructure (PKI)
Public Key Certificates

- Binds a *public key* to a *subject* (e.g., person, employee, officer, company, institution, authority)
- Signed by an *authority* that vouches for the integrity of the binding and the identity of the subject
- Includes a *serial number* to help detect unauthorized or forged certificates
- Specifies when certificate will *expire*
- Indicates under what *policies* the certificate was granted and what policies it is used
- Provides *other useful information* regarding the subject or use of the certificate
X.509 Public Key Certificate

Version: 1
Serial #: 0x0273000007
Signature Algorithm: RSA with MD5
Issuer: /C=US/O=BBN, Inc./OU=BBN PKI Services/
Not Valid Before: Sep 3 1995 20:00:00
Not Valid After: Sep 14 1996 20:00:00
Subject: /C=US/O=BBN, Inc./CN=Steve Cohn/
Public Key Algorithm: RSA
Public Key:

bb226db7496397756b 2e9e2cc2efalb7155c 5181f8f6db60d35f08d
cafda48c40c9f7873a 281040b1feaa073a502 d22337c517234 175a4a9b4984f88618
627de4a4533adcf18b 1a6d194f33d517234 4a3bd6a4ced748e3d5
b768877f0552ff8a20 567f8302e062848eee 44deb265ba832aadbe 7517
2f3c064e406e49d1f2

Signature Algorithm: RSA with MD5
Signature:

42ab3847920c0b3418 5181f8f6db60d35f08d dc4a9b02034184cb01
cafda48c40c9f7873a 281040b1feaa073a502 d9bc76435e7c94f5cc
627de4a4533adcf18b 2e9e2cc2efalb7155c 175a4a9b4984f88618
b768877f0552ff8a20 567f8302e062848eee 4a3bd6a4ced748e3d5
9023bcd84572ca1234 44deb265ba832aadbe bc06


**Uses for Certificates**

- **Establish Identity**
  - Used to identify subject (authenticated identity)

- **Assign Authority**
  - Often referred to as “attribute certificates”
  - Spells out rights & privileges granted to holder of corresponding private key

- **Secure Confidential Information**
  - Used only to encrypt symmetric keys
  - Certificate needs to be readily accessible so other parties can retrieve public key of subjects
Public Key Infrastructure (PKI)

Major Components

- Certificate Authorities (CAs & RAs)
- Trust Relationships
- Distribution Mechanisms
- Management Protocols
Certificate Authorities (CAs)

- Abstraction of traditional sources of authority (e.g., manager, official, bureaucrat)
- Responsible for issuing certificates and renewing expired certificates
- Sets policies for certificate issuing and their use
- Revokes certificates for cause
- Establishes operational policies and procedures for issuing, renewing, and revoking certificates
Who Will Serve as a CA?

- Government Agents
- Post Office
- Employers
- Hospitals, HMOs
- Financial Institutions
- Retailers
- Publishers, Entertainment Providers
- Internet Service Providers
Trust Relationships

- Schemes by which CAs authorize each other
- Enable users certified by a particular CA to verify certificates issued by other CAs
- Enable CAs to issue certs for end users or other CAs
- Basic trust relationship scheme is a hierarchy
  - The “root” CA in a hierarchy is trusted by all parties
  - Validating a certificate involves creating a path back to root CA
  - Simplifies managing relationships
- Management of trust relationships depends on an organization’s operational requirements
Trust Hierarchy

Root CA

CA Certificate

CA Certificates

Leaf Certificates

Alice

Bob

CA

Certificate

Certificate
On-line and Off-line CA Architecture

Off-Line CA

On-Line CA

Web-based RA

User

Certificate Request

Web Server

Firewall

Tooltalk

Certificates and CRLs

(O)RA
Certificate Management

- Certificate Registration
- Certificate Renewal
- Certificate Revocation
- Certificate Distribution
- Certificate Archiving
- Process Auditing
Potential CA System Attack Points
Potential CA Attacks

- Passive/Active Wire-tapping
  - User-RA Path
  - RA-CA Path
- CA/RA personnel compromise
- Computer system attacks
  - OS Penetration
  - Firewall & Front-end Penetration
  - CA Software / Database Manipulation
- Crypto module attacks
  - Simple Physical Tampering
  - Module Theft / Swapping
  - Close-in Attacks (TEMPEST, Temperature, Timing Analysis, Differential Fault Analysis, …)
CA Security Requirements

- Protection of CA Private Keys
  - Confidentiality against wide range of attacks
  - Support for CA multiple instantiation
  - Support for CA key recovery

- Validation of certificate issuance requests
  - User / Organization Identification
  - Verification of certificate syntax against rules for a specific CA or RA (basic certificate fields and extensions)

- Validated certification revocation requests*

- Timely distribution of revocation data (CRLs/OCSP)*

* Not enforceable via CA technology
CA Protection: Services

- Physical Security
- Operational Security
  - Personnel Security
  - Procedural Security
- Operating System and Application Security
- Network Security
- Cryptographic Module Security
CA Protection: Mechanisms

- Locks, Sensors, Guards, ...
- Personnel Background Checks
- Audit Trails
- Multi-party Authorization
- Certificate Syntax Filtering (Rule Based)
- Secure Operating System
- Software Configuration Management
- Encrypted/Authenticated RA-CA Communication
- Firewall Protection of On-line CA
- Hardware Cryptographic Modules