Introduction to Public Key Infrastructure

Tim Polk

January 13, 2005
Overview

• Why PKI?
• PKI Components
• PKI Architectures
• Path Validation
Why PKI?

- PKI is not the goal
- Scalable security services are the goal
- PKI supports scalable security services using public key cryptography
Security Services That Can Be Supported By PKI

• Authentication - Ability to verify the identity of an entity
• Confidentiality - Protection of information from unauthorized disclosure
• Data Integrity - Protection of information from undetected modification
• Technical Nonrepudiation - Prevention of an entity from denying previous actions
Secret Key Cryptography

- Classical form of cryptography - Caesar Cipher
- Single key used to encrypt and decrypt data
- Strengths
  - Very fast relative to public key cryptography
  - Relatively short keys
- Weakness: Key must be shared among interested parties
Public Key Cryptography

• Each entity has a PAIR of mathematically related keys
  – Private Key - known by ONE
  – Public Key - known by Many
• Not feasible to determine Private Key from Public Key
• Strength – no shared private keys
• Weakness
  – Relatively slow
  – Requires longer keys for same level of security
Choosing Cryptographic Tools

• Secret key is best
  – Bulk encryption

• Public key is best suited to
  – Digital signatures (e.g., RSA and DSA)
  – Key Management
    • Key transfer (e.g., RSA)
    • Key agreement (e.g., Diffie-Hellman)
Why Do We Need Certificates?

• Whose public key is this, anyway?
• What is this key good for?
  – Signatures or encryption?
  – < $100 or up to $10,000,000?
  – Secure mail, secure web, or document signing?
  – How much can I trust it?
Credit Card

• Features
  – Magnetic Stripe
  – Issued by trusted 3rd party (TTP)
    • issuer verifies user info
    • Issuer knows if information is current
  – Fixed expiration

• Drawbacks
  – Easy to forge
  – Partial identification

Pleasantville National Bank

9999 9999 9999 9999

VALID FROM 04/97  EXPIRATION DATE 11/30/99

Bob Smith
MEMBER SINCE 95

Trusty Cards
Digital Public Key Certificates

• Features
  – Digital object (no typing!)
  – Tamper-evident
  – Issued by a TTP
  – Complete user identification
  – Fixed expiration

• Drawbacks
  – Must trust issuer

Serial Number: 206
Certificate for: Bob Smith
Company: Fox Consulting
Issued By: Awfully Big Certificate Co.
Email Address: bsmith@home.net
Activation: Jan. 10, 2000
Expiration: Jan. 10, 2002
Public Key: 24219743597430832a2187b6219a75430d843e432f21e09bc080da43509843

ABC’s digital signature
0a213fe67de49ac8e9602046fa7de2239316ab233dec70095762121ace6f4fg66854392ab02e4
Using Public Key certificates

Serial Number: 206
Certificate for: Bob Smith
Company: Fox Consulting
Issued By: Awfully Big Certificate Co.
Email Address: bsmith@home.net
Activation: Jan. 10, 2000
Expiration: Jan. 10, 2002
Public Key:
024219743597430832a2187b6219a
75430d843e432f21e09bc080da43
509843

ABC’s digital signature
0a213fe67de49ac8e9602
046fa7de2239316ab323dc
ec70095762121ae94f666
854392ab02c4

Alice’s copy of ABC’s public key
0a213fe67de49ac8e9602
046fa7de2239316ab323dc
ec70095762121ae94f666
854392ab02c4

Alice - please ship 100 widgets to
Joe’s Warehouse
100 Industrial Park Dr.
Pleasantville, CA
Thanks, Bob!

Bob’s digital signature
12fa45cde67ab890034ab6739912acc4
587362600ff1e27849300b6cdff0034
Why Do We Need CRLs or Status Checking?

• Credit cards are revoked if the card holder
  – Dies
  – Loses the card
  – Cancels the card
  – Doesn’t pay

• Certificates may be revoked if the subject
  – Dies
  – Loses their crypto module
  – Leaves the company
Credit Card Verification

• Two mechanisms for handling credit card revocation
  – The “hot list”
    • Paper booklet listing hot cards
  – Calling the issuer
    • Providing the card number AND the $ amount
    • Received an authorization number OR a denial
CRLs & Status Checking

• CRLs are analogous to the “hot list”

• Status checking is analogous to calling the issuer to obtain information on a credit card

Issued By: Awfully Big Certificate Co.
Activation: June 10, 2001
Expiration: July 10, 2001

Revoked Certificate List:
84, 103, 111, 132, 159, 160, 206, 228, 232, 245, 287, 311, 312, 313

ABC’s digital signature
ab45c677899223134089076ab7d7eff2336a7569316a
f1288399a7445abc4dd67980121234726389ac
Certification Authority (CA)

- An entity that is trusted by PKI users to issue and revoke public key certificates
- A CA is a collection of personnel and computer systems
  - Highly secured (e.g., a guarded facility, with firewalls on the network) against external threats
  - Strong management controls (separation of duties, n of m control) to protect against internal threats
Registration Authority (RA)

• An entity that is trusted by the CA to vouch for the identity of users to a CA
  – This entity is only trusted by the CA
  – Generally relies on operational controls and cryptographic security rather than physical security
Repository

• An electronic site that holds certificates and certificate status information
  – Need not be a trusted system since all information is tamper-evident
  – Most commonly accessed via LDAP
  – Theoretically could be accessed using HTTP, FTP, or even electronic mail
PKI Architectures

- Single CA
- Hierarchical PKI
- Mesh PKI
- Trust lists (Browser model)
- Bridge CAs
Single CA

• A CA that issues certificates to users and systems, but not other CAs
  – Easy to build
  – Easy to maintain
  – All users trust this CA
  – Paths have one certificate and one CRL
  – Doesn’t scale particularly well
Hierarchical PKI

• CAs have superior-subordinate relationships

• Users trust the root CA
Mesh PKI

- CAs have peer-to-peer relationships
- Users trust the CA that issued their certificates
Trust lists (Browser model)

- User trusts more than one CA
- Each CA could be a single CA or part of a PKI
  - For hierarchies, should be the root
  - For mesh PKIs, could be any CA
Trust List Example

Alice’s Trust List

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-1</td>
<td>Alice</td>
</tr>
<tr>
<td>CA-2</td>
<td>Bob</td>
</tr>
<tr>
<td>CA-3</td>
<td></td>
</tr>
</tbody>
</table>

CA-1

CA-4

Alice

CA-5

Bob

CA-2

Carol

CA-3

CA-6

CA-7

David
Bridge CAs

• Designed to unify many PKIs into a single PKI
• Designed to translate trust information into a single entity
Bridge CA Example

- There may be dead-ends and cycles
The Path Development Problem
Path Validation

- Also need to check the status of each certificate!