Key Management

Gary Lee
CS996
Information Security Management
Overview

KMI/PKI - Infrastructure

♦ Services
  – Certificate Management
  – Symmetric Key Management

♦ Processes

Case Study

♦ Federal PKI
KMI/PKI

- Key Management Infrastructure/Public Key Infrastructure

- Strategy based on multiple levels of assurance
  - High level assurance: protection of national security information
  - Medium level assurance: good enough for other services
KMI/PKI Operational Services

- Symmetric key generation and distribution
- Support for asymmetric cryptography and its associated certificate management
- Directory service
- Management of the infrastructure
Security Applications

Table 8.1-2. Security Applications Supported By Cryptographic Type

<table>
<thead>
<tr>
<th>Security Application</th>
<th>Symmetric Cryptography</th>
<th>Asymmetric Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>*</td>
<td>X</td>
</tr>
<tr>
<td>Nonrepudiation</td>
<td>*</td>
<td>X</td>
</tr>
<tr>
<td>Transmission Confidentiality</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>File Encryption</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>*</td>
<td>X</td>
</tr>
<tr>
<td>Availability (e.g., Spread Spectrum)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Key Agreement</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

*These services can be enabled by symmetric cryptography when provided in conjunction with other mechanisms (e.g., a cyclic redundancy check [CRC] encrypted with the message).*
KMI/PKI Processes

- **Registration** — enrolling individuals who are authorized to use the KMI/PKI.
- **Ordering** — requesting the KMI/PKI to provide a subscriber a key or a certificate
- **Key Generation** — generating the symmetric or asymmetric key into a certificate
- **Certificate Generation** — binding the subscriber information and the asymmetric key into a certificate
KMI/PKI Processes

- **Distribution** – providing the keys and certificates to the subscriber in secure and authenticated manner
- **Accounting** – tracking the location and status of keys and certificates
- **Compromise recovery** – removing compromised keys and invalid certificates from the system in an authentication manner
- **Rekey** – replacing the keys and certificates periodically
KMI/PKI Processes

- **Destruction** – destroying the secret key when it is no longer valid
- **Key Recovery** – recovering subscriber’s private encryption key
- **Policy Creation** – defining the requirements for the employment of previous processes
- **Administration** – running the infrastructure
- **Value-Added PKI Processes** – supporting optional processes, including archive, timestamp, and notary services
Certificate Management
Primary Components

♦ Certificate Authority (CA)
  – A trusted authority to create and assign certificates

♦ Registration Authority (RA)
  – A trusted entity that authenticates the identity of subscribers requesting certificates

♦ Certificate Repository
  – The location where a CA posts certificates and CRLs
Primary Products

♦ Asymmetric key material
  – A public/private key pair

♦ Certificates
  – A record binding a subscriber’s identity with his or her public key

♦ Certificate Revocation List (CRL)
  – A list containing certificates that no longer contains a valid binding between a public key and an identity
PKI Design Approaches

♦ Hierarchical
♦ Hierarchical with Trust lists
♦ Mesh
♦ Hierarchical with Bilateral Cross-Certification
♦ Bridge Certificate Authority
♦ Online Status Checking
Hierarchical PKI

♦ Root certificate is the “trust anchor”
♦ Verifying a certificate occurs in a certificate chain.
♦ May not be suitable for non-hierarchical organizations
Hierarchical with Trust Lists

- A trust list is maintained
- Any certificate signed by a CA within the trust list is accepted
- Very flexible
- Compatible with hierarchical PKIs
Mesh PKI

- Certificate signed by most local CA is accepted
- Appropriate for non-hierarchical organizations
- No need to maintain trust lists
- Can have negative performance impact
Hierarchical with Bilateral Cross-Certification

♦ Root CAs issue cross-certificates to each other
♦ Verifying a certificate chain starts with own root
♦ Can be a mechanism to provide interoperability among alliances
Bridge Certification Authority

- Allows hierarchical and mesh PKI to interoperate
- A bridge is not a root; it is a trust anchor
Online Status Checking

- Relying party authenticates with an online status responder
- Requires reliable network connections between status responder and relying parties
Security Services

♦ Confidentiality
  – Private keys are encrypted and distributed by the PKI

♦ Integrity
  – Digital signatures bind subscriber information to their public keys
Policy Creation

♦ No KMI/PKI can guarantee 100% security
♦ A KMI/PKI security policy will reflect on a subscriber’s requirements
  – Policy can be strict or loose
♦ Some issues a policy should address
  – Key generation
  – Computer security requirements
  – Interoperability requirements
  – Rekey Mechanism
  – Certificate profile
  – Key and certificate distribution
Registration

- Certificate Management Authority (CMA) is responsible for making decisions
- A CMA can be a
  - CA if it signs certificates
  - RA if it provides registration information
- CMA reviews certificates and verifies the information within them
- CMA ensures that the proper identity is bound to the public key in the certificate
Ordering

- A request for a certificate may lead to the generation of a public/private key pair
- Key/Certificate Generation
- RA must verify requester information
- Generated certificate is stored until the RA or CA operator approves it
- Subscriber is notified by the CA via email or posting on web front-end
Generation

♦ Key Generation

- Local key generation
  - Private keys are maintained by subscriber
  - Only public key needs to be conveyed to the CA
  - Preferred way of generating key material for digital signatures
- Centralized key generation
  - CA generates key material on behalf of the subscriber
  - Used in environments with high security requirements
  - CA has the responsibility to distribute the private key to the subscribers (via secure protocols)
  - Preferred way of generating key material for encryption
- Hybrid methods are available
- Two key system can also be used (one for encryption, the other for signatures)
Generation

♦ Hardware or software key generation
♦ Keys and “key material” (e.g., hardware tokens) have a classification level (S, TS, SBU, etc.)
  – Key classification level must be greater than or equal to the information classification
  – Keys are handled the same as any other information at that level
  – When a secure communication link is set up, endpoints make sure that the other end is using a key of the right classification level.
Generation

♦ Key material
  - Paper (not used any more)
  - Physical data storage:
    • DS 101 Fill Device
    • CIK--Crypto ignition Key
    • FORTEZZA PCMCIA card
    • DoD CAC (Common Access Card) smart card (PKI)

♦ Key length
  - Strong asymmetric keys are usually 1,024 bits, and 2,048 bits or longer for sensitive applications
Generation

♦ Certificate Generation
  – All information in the request is verified
  – Subscriber must be authenticated by the RA
  – Certificate may be generated automatically or with the intervention of the CA operator
  – A copy of the certificate is stored in the CA database
  – The certificate that is created is posted on the web front-end of the CA or is emailed to the subscriber
  – The infrastructure must generate the initial root key in a unique way
    • Root certificate is self-signed
Distribution

♦ Many ways to distribute certificates
  – Emailing
  – Posting on the Web front-end of the CA
  – Certificate repository or directory

♦ Dependent on application
  – Web browser
    • CAs send emails containing URL for the certificate
    • Subscriber connects to web front-end of CA and downloads the certificate (example: my.poly.edu)
  – Web server
    • Usually distributed via email from the CA
Compromise Recovery

- **Security compromise revocation**
  - Associated private key is compromised
  - Subscriber is fired from an organization

- **Routine revocation**
  - Information within certificate is no longer valid

- **CA must be notified**
  - Certificate revocation notice is sent to CA

- **CA places the certificate in a CRL**
  - Periodically generated and posted
  - Emergency CRLs can be distributed more frequently
  - Can use online validation to consolidate CRLs
Key Recovery

- Normally provided for asymmetric key material used for data encryption
- Key backup and key escrow
  - Provided by the CA if the CA was involved in the key generation for a subscriber
  - CA can store a copy of the private key in a secure database
  - It is possible for another infrastructure to support key recovery
Rekey

- Performed when certificates need renewal
  - A certificate naturally reaches expiration
    - A new key pair and certificate is created
    - Only the certificate needs to be renewed, the keys are retained
  - A certificate is revoked and a new certificate needs to be created

- Renewing a key depends on the recommended key life span

- Transition to a new key should not detriment availability

- OTAR (Over the Air Rekeying)
  - Sending new keys to a remote device over the communications link (keys are encrypted) & automatically loading the crypto devices
Accounting

- Keeping track of the location and status of certificates
- Archiving of accounting material
- Accounting information should include
  - Task
  - Time
  - Status
  - Operator involved
- All accounting material must be protected from accidental deletion, modification, or malicious attacks
- Provides the following task
  - Damage assessment of operator if operator is proven untrustworthy
  - Recording certificate information from the ordering process
  - Archiving of key and token history
  - Proving to auditors that policies and procedures were followed
Administration

♦ Administrative functions should be distributed among a large number of people
♦ Different administrative roles
♦ A few tasks performed by administration
  – Enforcing the policy
  – Performing key and certificate accounting
  – Managing technical security mechanisms
  – Training operators
  – Maintaining availability
Destruction

- Asymmetric key material may be destroyed when they expire or when they are compromised
- The subscriber would manually remove the keys and certificates from database
- Sometimes retaining expired key material is necessary
  - Accessing encrypted data
Symmetric Key Management
Overview

♦ Many legacy systems still use symmetric cryptography
♦ Encryption and decryption keys are usually the same
♦ Sender and receiver needs to agree on a key
♦ Several advantages and disadvantages
♦ Critical Elements include: generation, ordering, distribution, storage and destruction
Overview

♦ Advantages
  – Local generation of session keys minimizes problems of distribution
  – Key structures are very simple
    • random numbers provided by truly random number generation
  – Keys do not require extensive validation

♦ Disadvantages
  – One lost key may compromise the entire system
  – Difficulty scaling to larger communities
  – Keys must be kept secret
  – As more people know the symmetric, the risk of key compromise increased.
Critical Elements

Figure 8.1-9. Critical Elements of Symmetric Key Management Activities
Critical Elements

♦ Ordering
  – Only authorized individuals should be allowed to order a key
  – Symmetric networks are predefined
    • Need to know who needs the key and when it is needed
    • Keys should be delivered prior to using it

♦ Generation
  – Key generation must be performed in a secure environment
  – Weak keys should be deleted
Critical Elements

♦ Distribution
  – Two-person control for higher assurance
  – Electronically
  – Can be distributed physically

♦ Storage
  – Electronic keys should be stored in encrypted form

♦ Loading keys into cryptographic applications
  – Require protected interface
  – Physical protection of the key at the interface
Critical Elements

♦ Destruction
  – Keys should not be stored any longer than needed
  – Be aware of the media that the key is stored on (ex. paper, RAM, PROM, etc.)

♦ Compromise
  – A compromise may expose all encrypted traffic (present and past)
  – Recovery is critical, each user must be given a new key.

♦ Accounting
  – Track individuals who have access to a key
  – When and where the key was delivered
  – When a key is destroyed
Case Study: Federal Key Management

♦ Federal PKI is headed by the Federal PKI Steering Committee (SC)
♦ Will provide secure communications and commerce among federal agencies
♦ Consists of CAs, RAs, certificate status responders and management authorities
♦ Uses a Bridge CA to provide interoperability among federal agencies
  – Federal Bridge Certificate Authority
♦ [www.cio.gov/fpkisc/](http://www.cio.gov/fpkisc/)
Federal PKI Architecture
Certificate Assurance Levels

♦ Class 3
  – Protect some mission critical information
  – Mission support and administration
  – Software token
Certificate Assurance Levels

♦ Class 4
  – Protected Sensitive But Unclassified (SBU), mission critical information over unencrypted networks
  – Crossing boundaries
  – Hardware token

♦ Class 5
  – Protected Classified information over unencrypted networks
KMI/PKI Recent

- NSA
  - KMI PRSN Pilot
  - EKMS
  - Physical Systems
- DISA
  - Current Class 4 PKI (DMS)
  - Current DoD Class 3 PKI
  - Operations
- Commercial
  - Class 3 and below PKI
- Manual Systems
- High Grade Electronic Applications
- X.509 Certificate Based Applications

4/26/2004
KMI Vision Architecture

Manual Systems

CF, Tier 0

KMI Management Servers

Networks/Web

BASE/POST ACCOUNT (Client Workstation)

REGIONAL SITES (Servers)

Tier

High Assurance ROOT

Certification Authorities

High Assurance Certification Authorities

Commercial Certification Authorities

Medium Assurance ROOT

Certification Authorities

NSA

KMI Managers

UNCLASSIFIED
KEY MANAGEMENT

4/26/2004
Secure Terminal Equipment (STE)

- Key materials on FORTEZZA Smart Card/Crypto Engine
- Approved for Classified use
- Phone not classified when card is removed
Present/Future Trends

♦ Public awareness of PKI must be heightened
♦ Compatibility among vendors
  – Standardization of protocols
  – Standardization for certificate and cryptographic token storage format
♦ Smart Cards
  – Private keys are stored in a microchip on a card
♦ Biometrics
♦ Certificate Revocation
♦ Certificate Recovery
Reference

♦ Key Management Infrastructure/Public Key Infrastructure, Information Assurance Technical Framework, Section 8.1. http://www.iatf.net/framework_docs/version-3_1/index.cfm