Managing and Assessing Risks in a PKI

MARK B. COOPER
PRESIDENT
MARK@PKISOLUTIONS.COM
WWW.PKISOLUTIONS.COM
Overview

- Overview of PKI
- PKI Authentication Solutions
- Risks Introduced by a PKI
  - Logical
  - Physical
  - Operational
What is PKI?

Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
Digital Certificates

A digital certificate:

• Represents the identity of a user, computer, or program
• Contains information about the issuer and the subject
• Signed by a CA which vouches for the identity of user/device/program
Certification Authority

A certification authority:

- Certifies the identity of a certificate requestor
  - The mode of identification depends on the type of CA, security policy and request handling requirements

- Issues certificates
  - The certificate template or requested certificate determines the information in the certificate

- Manages certificate revocation
  - The CRL ensures that invalid certificates are not used

- Extensible
  - Can install Policy and Exit modules to add workflow to certificate management
CA Hierarchy Tiers

Three Tier
- Root CA
- Policy CA
- Issuing CA

Two Tier
- Root CA
- Policy/Issuing CA
CA Hierarchy Tiers

Root Issuing CA

Single Tier
Common PKI Solutions

- User and Computer Identities
- Wireless Authentication - 802.11x
- VPN
- User Authentication/Encryption
  - Secure Email
  - Microsoft Rights Management Server
  - Logon Authentication / Smart Cards
User Authentication

- Based on User Knowledge Only
  - Authentication Name & Passphrase
- No Controls on this knowledge
- Easy to Share, Relatively Easy to Find
- No Non-Repudiation
- MITM, Pass-The-Hash, etc...
User Authentication – PKI Style

- Two-Factory Authentication
  - Have - Certificate
  - Know - Passphrase
- Single Instance/Location
- Non-Repudiation Available
- Protected against MITM, Pass-the-Hash, etc.
PKI Perception

- More Secure than Username/Password
- Provides Two-Factor
  - Dual Authentication
  - Strong Key Protection
- Difficult to Install
Risks Introduced by a PKI
Compromises

- Difficult to Detect Fraudulent Certificate
- Impersonation
  - Harder to Mitigate than Passwords
- Encryption Snooping
  - SSL
  - Files
  - Email
PKI Risks

- Certificate is Valid unless Revoked
  - No Issuance Verification
- Trust is at CA level and Implicitly includes all children
- Attacks are just as likely from internal as external forces
- Positive Control is Required at All Times
General Controls

- Follow the Keys
- Protection Cradle to Grave
- 2+ Administrators at All Times
- Protect Against Denial Of Service
Logical Control

- CA’s Signing Key is Most Critical Component
  - Soft Key vs Hard Key
  - Hardware Security Modules
- Harden for Local AND Network Attacks
  - CD-ROMs
  - USB
Physical Control

- Physical Isolation of CAs
  - All Required Elements Secured
    - Denial of Service & Compromise
  - Two-Man Locks - Silo Style
- Protection of Offline Material
  - Safes/Tamper-Proof Bags
- Remote Access Bypasses
  - Enforce Existing Physical Controls
Operational Control

- Key Management Quorums
  - All Personnel need expertise

- Audit Logs
  - MUST ACTUALLY AUDIT

- Separation of Duties - Common Criteria
Summary

- Key Management & Protection
- Operational & Security Controls
- Collusion
- Determine Your Organizational Threats
  - Mitigate
- Audit & Assess on Regular Basis
Questions?