TMT10 - Top 20 Mistakes in Microsoft Public Key Infrastructure (PKI)

Mark B. Cooper
President & Founder
PKI Solutions Inc.

Level: Intermediate
About PKI Solutions Inc.

- 10 years as “The PKI Guy” @ Microsoft
- Charter – Microsoft Certified Master DS
- Numerous books and whitepapers
- Services include:
  - ADCS Architecture, Deployment and Consulting
  - Assessment and Remediation Services
  - In-Depth PKI Training
  - Retainer and Support Services

SFO January 2015, NYC February 2015
Genesis of The List

- Compiled Over 10 Years @ Microsoft
- Consulting, Engineering and “RedZone”
- Private and Public Sectors Around the World
  - Hundreds of Customer Environments
- Lead to PKI Best Practice Review
  - Evolved over the years to ADCS Assessment
Benefits of ADCS Assessments

• Problems Can Lay-in-Wait
• Many Manifest After First CA Renewal
• Testing and Validation Often Insufficient
• Fresh Perspective to Spot Deficiencies
#1 - CRL Management

- **Validity & Publishing Intervals**
  - Intervals Balanced with Need To Know
    - Identification versus Authorization
    - Highly Affected by Caching Behavior on Clients
    - Windows Caches for Lifetime of CRL
      - `Certutil.exe -setreg chain\ChainCacheResyncFiletime @now`
      - Less Effective: `Certutil.exe -URLcache delete`

- **Validity versus Publishing**
  - Next Update versus Next CRL Publish
  - Leverage Over-Laps to Provide Redundancy
    - `CRLOverlapPeriod/Units & CRLDeltaOverlapPeriod/Units`
#1 - CRL Management

- Availability
  - CRL Availability versus Issuance Availability
  - Organizational Requirements
  - Options
    - Active Directory Redundancy
    - HTTP Redundancies

- Distribution Mechanisms
  - Active Directory versus HTTP
  - Driven by Accessibility and Client Majorities

- Delta CRL
  - Generally Un-Needed in Most Environments.
#2 - CDP/AIA DNS Alias

- **HTTP Defaults to Local Host Name**
  - No FQDN Compliant
  - Sticky to Specific Server
  - **Difficult to Migrate, Upgrade or Modify**
  - Inaccessibility

- **Alias Provides Portability**
  - Migrate As Infrastructure and Deployment Requires
  - Migrations & Upgrades are Non-Issue
  - Easy to Add Fault Tolerance
#3 – CRL/AIA Extension Errors

- **File/URI Location Built by Variables**
  - UI Manipulation Has Challenges
  - Configurable in Registry – Often with a Script

- **Errors Introduced**
  - OCSP Set as AIA Location
    - Include in the AIA extension of issued certificates
  - Copy and Paste Between CDP and AIA
  - Lack of CRL Suffix
    - The Pseudo-Hidden Achilles Heel
  - Modifying AIA to Remove Server Name
    - Extension Largely Ignored in Code
    - Requires Manual Manipulation
    - Results in Published Path and File Mismatch
#3 – CRL/AIA Extension Errors

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish CRLs to this location</td>
<td>1</td>
</tr>
<tr>
<td>Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually</td>
<td>8</td>
</tr>
<tr>
<td>Include in CRLs. Client use this to find Delta CRL locations</td>
<td>4</td>
</tr>
<tr>
<td>Include in the CDP extension of issued certificates</td>
<td>2</td>
</tr>
<tr>
<td>Publish Delta CRLs to this location</td>
<td>64</td>
</tr>
<tr>
<td>Include in the IDP extension of issued CRLs</td>
<td>128</td>
</tr>
</tbody>
</table>
#3 – CRL/AIA Extension Errors

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include in the AIA extension of issued certificates</td>
<td>2</td>
</tr>
<tr>
<td>Include in the online certificate status protocol (OCSP) extension</td>
<td>32</td>
</tr>
</tbody>
</table>
#4 - Misuse of OCSP

- **Designed for Efficient CRL Distribution**
  - Overcomes Large CRL File Transfers (Multi-MB+)
  - Certificate Specific Enquiries from Responder
  - Dependent on CRLs
  - CRL Interval Dependent

- **Not Real-Time Information**

- **Deterministic Results**
  - CAB Forum
  - Available in 2012 R2 & 2008 R2 w/HotFix 2960124
#5 – OCSP Renewal

- OCSP Signing Certificate
  - Required from EACH CA Serviced
  - Signed by CA

- CA Signs with Current Keypair

- Services older Keypairs/CRL
  - Default Config will Break OCSP on CA Renewal

- OCSP Requests Specify Correct CA
  - CA Needs to be Configured Properly

  certutil -setreg ca\UseDefinedCACertInRequest 1
#6 – ADCS Hotfixes

- **Distinct from Updates**
  - Not Distributed by Windows Update

- **Product/Issue Specific Fix**
  - Previously Reported Issue with Remediation
  - Test and Apply Only if Needed Philosophy

- **Preventative Use**
  - If Possible In the Environment, Consider the Hotfix
  
  Don’t Need to Wait For Problem

- **Time Consuming to Find**
  - Comprehensive List Available
#7 – Network Device Enrollment Service Security

- **Microsoft’s SCEP Implementation**
  - Cisco Designed for Non-Authentication Integrated Devices
    - **Routers & Switches**
    - Available Since Server 2000 in Resource Kit
    - Integrated with Server 2008

- **Leveraged for many BYOD Scenarios**
  - VoIP, Tablets, Phones, Internet of Things

- **Security and Architecture**
  - Authentication and Enrollment Disjointed
  - BYOD Often Necessitates DMZ Exposure Risks
#7 – Network Device Enrollment Service Security

- **Manage URI Access To Server**
  - Does Solution Require Exposure of Admin Page?
  - Firewall & SSL Protection

- **NDES Key Protection**
  - Hardware Security Module (Think Heartbleed Protection)

- **NEW* Server 2012 R2 NDES Policy Module**
  - Offloaded Authentication and Enrollment Management
  - Authorization Tied to Enrollment Request

- **New Whitepaper From Microsoft**
#8 - ADCS & Domain Controllers

- Don’t Do It
- Seriously – Don’t Do It!
- Interaction Issues Largely Resolved
  - DCOM Group
  - LDAP/S Certificate Selection Process
- Known Issues
  - Can’t Change Domain Membership (DCPromo Anyone?)
  - **DC Upgrades, Re-Hosting, DC Retirement**
  - Domain Admins versus CA Admins
#9 - Logical Security Controls

- **Remote Desktop Services**
  - Scourge of Physical and Logical Security
  - Most Common Mistake

- **USB/CD Attack Vectors**
  - Easy To Load/Attack/Log/Compromise
  - Disable USB in BIOS (with Password)
  - Disable CDROM AutoPlay

- **Firewalls & Anti-Virus**
  - Microsoft or Other – ENABLE IT!

- **Password Policies**
  - At Least Match Your Organizational Standards
  - Especially Offline Roots!
#10 - Root Certificate Extensions

- **Properties of Root Certificate – Not CA**
  - Driven by Install Options and CAPolicy.inf

- **CDP & AIA Extensions**
  - Best Practice is a blank CDP/AIA Extension for Root
  - ADCS Behaviors since 2003
    
    Old Habits are hard to break

    [certsrv_server]
    renewalkeylength=4096
    RenewalValidityPeriodUnits=20
    RenewalValidityPeriod=years

- **Issuance Policies in Server 2012**
  - Explicit Hierarchy
  - Impact on OCSP
#11 - SMTP Exit Module

- **Free Monitoring**
  - Built into Service
  - No UI, Use Script or Registry

- **Eliminate Queues of Pending Requests**

  - EXITEVENT_CRLISSUED
  - EXITEVENT_CERTDENIED
  - EXITEVENT_CERTISSUED
  - EXITEVENT_CERTPENDING
  - EXITEVENT_CERTUNREVOKE
  - EXITEVENT_CERTRETRIEVEPENDING
  - EXITEVENT_CERTREVOKE
  - EXITEVENT_SHUTDOWN
  - EXITEVENT_STARTUP


- **Pseudo Transactional Tracking and Recovery**
  - Use CRLIssued for “Real-time” Database Recovery
#12 – Certificate Validity Periods

- **Hierarchy Lifetimes Truncate Children**
  - Plan from The Client and Up
  - 2x Child Lifetime

- **Balance with Cryptographic Usefulness**
  - Longer Validity with More Complex Crypto

![Certificate Validity Periods Diagram]

- **Root CA**: 10 Years
- **Enterprise CA**: 5 Years
- **Device Cert**: 2 Years
#12 – Certificate Validity Periods

- **Half-life Renewals with Same Key**
  - Harder to Track but Fewer Keys

<table>
<thead>
<tr>
<th>Level</th>
<th>Certificate Type</th>
<th>Root CA</th>
<th>Enterprise CA</th>
<th>Device Cert</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>10 Years</td>
<td>5 Years</td>
<td>2 Years</td>
</tr>
<tr>
<td>Root CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise CA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Cert</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Same Key Renewal**
  - 2.5 Years

- **New Key Renewal**
  - 5 Years
  - 2.5 Years

### Notes
- **Root CA**
  - 10 Years validity
- **Enterprise CA**
  - 5 Years validity
- **Device Cert**
  - 2 Years validity
#13 - Certificate Key Lengths

- **Design for Expiration Before Compromise**
  - Balance Key Length, Validity Period and Value
  - Expires before Brute Force Compromise
  - Theoretical Timeline – Could be Lucky #2 Guess

- **Determine Compatibility Matrix**
  - Applications are the Biggest Unknown
  - Deploy Highest Crypto Option Where Able
  
  *Carve out those legacy crypto needs*

- **RSA 2048 & SHA1**
  - Minimal Commercially Viable Crypto
#13 – Certificate Key Lengths

NIST Recommendations 2010

<table>
<thead>
<tr>
<th>Date</th>
<th>Minimum of Strength</th>
<th>Symmetric Algorithms</th>
<th>Asymmetric</th>
<th>Discrete Logarithm Group</th>
<th>Elliptic Curve</th>
<th>Hash (A)</th>
<th>Hash (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010 (Legacy)</td>
<td>80</td>
<td>2TDEA*</td>
<td>1024</td>
<td>160</td>
<td>1024</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>2011 - 2030</td>
<td>112</td>
<td>3TDEA</td>
<td>2048</td>
<td>224</td>
<td>2048</td>
<td>224</td>
<td></td>
</tr>
<tr>
<td>&gt; 2030</td>
<td>128</td>
<td>AES-128</td>
<td>3072</td>
<td>256</td>
<td>3072</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>&gt;&gt; 2030</td>
<td>192</td>
<td>AES-192</td>
<td>7680</td>
<td>384</td>
<td>7680</td>
<td>384</td>
<td></td>
</tr>
<tr>
<td>&gt;&gt;&gt; 2030</td>
<td>256</td>
<td>AES-256</td>
<td>15360</td>
<td>512</td>
<td>15360</td>
<td>512</td>
<td></td>
</tr>
</tbody>
</table>

- Http://www.keylength.com
#13 – Certificate Key Lengths

You can enter the year until when your system should be protected and see the corresponding key sizes or you can enter a key/hash/group size and see until when you would be protected.

<table>
<thead>
<tr>
<th>Method</th>
<th>Date</th>
<th>Symmetric</th>
<th>Asymmetric</th>
<th>Discrete Logarithm Key</th>
<th>Elliptic Curve</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Lenstra / Verheul</td>
<td>2034</td>
<td>96</td>
<td>2788</td>
<td>2272</td>
<td>171</td>
<td>2788</td>
</tr>
<tr>
<td>2 Lenstra Updated</td>
<td>2034</td>
<td>91</td>
<td>1834</td>
<td>2285</td>
<td>182</td>
<td>1834</td>
</tr>
<tr>
<td>3 ECRYPT II</td>
<td>2031 - 2040</td>
<td>128</td>
<td>3248</td>
<td>256</td>
<td>3248</td>
<td>256</td>
</tr>
<tr>
<td>4 NIST</td>
<td>&gt;2030</td>
<td>128</td>
<td>3072</td>
<td>256</td>
<td>3072</td>
<td>256</td>
</tr>
<tr>
<td>5 ANSI</td>
<td>&gt;2020</td>
<td>128</td>
<td>4096</td>
<td>200</td>
<td>4096</td>
<td>256</td>
</tr>
<tr>
<td>6 NSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 RFC3766</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 BSI (signature only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Http://www.keylength.com
#14 - CA Key Protection

- Paramount to Integrity of PKI
  - Exposure Negates Cryptographic Strength

- Soft versus Hard Keys
  - Heartbleed Exploit

- Easier & Cheaper to Protect Key then Remediate Key Compromise

- Hardware Security Modules
  - CA and NDES Roles
  - Thales e-Security & Gemalto/SafeNet

- TPM-Based CA – Word of Caution
#15 - CRL Publishing to File Share

- Default Publishing to Local CertEnroll
  - Works out of the Box
  - No Resilience or Fault Tolerance
  - No External Access
    - At least there SHOULDN’T be
- Scripting CRL & Publishing
  - No Monitoring or Reporting
  - Disconnected from Manual Revocation
#15 - CRL Publishing to File Share

- **Use CA To Publish For You**
  - Requires SMB Support Between Computers
  - Create FileShare on Target
  - Add CA Computer Object to Share Permissions
  - Add CA Computer Object to NTFS Permissions
  - Define CRL Extension
    - `FILE://\servername.contoso.com\sharename\%3\%8\%9.crl`

- **AIA Hardcoded – UGH!**
  - Infrequently Updated
  - Include in Procedural Documentation
#16 - Patch Management

- ADCS is Not Set and Forget
  - Vulnerable
  - Prime Target

- Offline CAs
  - Physical and Logical Isolation Offer SOME Protection
  - Maintain Supported Service Pack Level
  - ADCS Specific Updates
  - Time/Clock Related Updates

- Online CAs
  - Above Plus Microsoft Updates/Patches
#17 - Architecture

- **PKI Hierarchy Deployment Mismatch**
  - Not Designed to Security/Operational Needs
  - Designed on Labs/Books/Whitepapers Blindly

- **Single and Three-Tier Most Often Incorrect**

- **Policy/Intermediate CA**
  - Is there a CAPolicy.Inf?
    - **If Not, Most Likely Server is Superfluous**

- **Single Tier/Enterprise Root CA**
  - Using Smart cards, S/MIME, Code Signing, File Encryption, Large Number of Non-AD Clients?
    - **If So, PKI Should be Multi-Tier**
#17 - Architecture

- “Today, I Just Need a …… Certificate”
- **Design for Next 12-18 Months Minimum**
  - What Else is Approved?
  - What Does Organization need?
  - Easy to Under-Engineer, Hard to Over Do It
- **Security and Architecture Key Aspects**
  - Security Can Be Improved, But Integrity Can’t
  - Architecture is Generally Inflexible
#18 – “Offline” Root

- **Physical Isolation of Root**
  - Reduces Attack Surfaces
  - Requires Physical Access
  - Eliminates Remote Attacks

- **“Sometimes” Offline**
  - Turned Off When Unused, Brought On Network for Maintenance

  *You are asking for trouble!*

- **Offline Means OFFLINE!**
  - Define & Use USB Flash/Virtual Floppy Procedures
#19 - Collusion Requirements

- **Design— No Single Person Access, EVER**
  - Collusion Procedures Define Multi-Person Access
  - Cradle to Grave Operational Control
- **Enforce Procedures**
  - Easily Broken Without Accountability/Controls/Auditing
  - HSMs Enforce Controls
  - Locks and Card keys, Never the Same Person
- **A Moment Alone Can Never Be Undone**
#20 - Documentation

- **Bane of Every Organization**
  - Challenging Like any other Project
  - Documentation Could Save the Environment Some Day
  - (Almost) Never too Late to Document!

- **Primary Areas to Document**
  - Offline CA Retrieval and Standup
  - Server Rebuild
  - CA Key Renewals
  - Disaster Recovery/Continuity Plan
  - Emergency CRL Signing
Questions?

pkisolutions.com
mark@pkisolutions.com
@pkisolutions

Wednesday Sessions
Managing and Deploying BYOD Identity Solutions with a Microsoft PKI
Securing Cloud Servers and Services with PKI Certificates