Smart Grid Security
Key Management

Tony Metke

Distinguished Member of the Technical Staff

Motorola Solutions

Outline

- Key Management Challenges
- Proposed Solution
  - Certificates Everywhere
- Certificate Usage
- PKI Issues
- Solutions to PKI Issues

Key Management Challenges (1)

- Some key(s) need to be provisioned in every autonomous device.
  - Symmetric or Asymmetric
- The smart grid will have a lot of devices.
  - Whether AMI, DA, or other.
- Key provisioning is a sensitive operation.
  - Controls need to be put into place to ensure that it is performed securely.
  - This can be costly without the right technology.

Key Management Challenges (2)

- Customers write RFPs with requirements for things like;
  - ❑ AES Encryption
  - ❑ IPsec
  - ❑ TLS
  - ❑ SSH

  Often there is no mention of key provisioning or key rotation requirements.
- Vendors deliver systems that require <u>manual key provisioning</u>.
  - **For large systems the effort to securely provision keys manually can be enormous.**
- To save effort, customers sometimes take shortcuts, that can introduce significant vulnerabilities.
  - Using the same static key in many devices.
  - Using a default key built into the device
  - Accepting keys on first use
  - Turning security features off

Key Management Challenges (3)

- Inter-domain communications can complicate key management significantly.
  - Neighboring Utilities,
  - Home Owners
  - Public Safety,
  - Service Providers, etc.
- Group Communications complicates key management.
  - IEC 61850 - Generic Substation Events (GSE) uses Multicast.
  - Ad hoc/Mesh networks use multicast/broadcast.
- Often a key is not enough to authenticate an entity, or to determine the authorization status of an entity.
- User Name and Passwords don't work for highly distributed systems that need to be highly available.
  - Google has 57 data centers, the NAPG has 10,000 transmission substations, and 50 to 70K distributions substations. **Enterprise solutions for high availability aren't sufficient for the smart grid.**

Proposed Solution

Certificates Everywhere!

- Certificates can be used to prove identity and authorization status locally (without requiring AAA connectivity)
- In general, two types of certificates are required; Device Management Certs (issued by Manufacturer), and Operational IA Certs (issued by an operator or a service provider)

Certificate Usage

- Device Management (DM) certs.
  - Installed by the Manufacturer
    - Permanent certificates that never expire
  - Used to prove the identity of a device
    - The contain: Make, Model and Serial Number
  - Used to protect the platform
    - All downloaded software must be signed.
      - By Manufacturer? (YES)
      - By Regulatory Body? (For high assurance component ?) (Nevada Gaming Commission style software approval)
  - Can be used to authenticate the device for certain operations, including issuing a Operational IA cert.

Certificate Usage

- Operational IA (OIA) certs
  - Used to establish the operational identity of the device/user (e.g. the temperature sensor at Transformer 12, in Substation 34 belonging to utility x.)
  - Used to establish authorization status of an entity.
  - Operators leverage the DM certs to efficiently issue an operational cert with authorization attributes.
- Signed Policy Control Objects
  - Used to determine which certs can be accepted by a service provider.

PKI Pros and Cons

Pros

- Certificates can provide off-line authentication and authorization.
- Certificates can be used to provide cross organizational trust (securely and efficiently).
- PKI can provide comprehensive controls over the management of trust and authorization status.
- PKI can provide non-repudiation of cert management events, enabling detailed auditing.
- With the right tools, PKI can be automated to manage all system credential very efficiently.

Cons

- PKIs can be complex to set up and operate.
- PKIs require complex certificate policy documents and certificate practice statements.
- Cross-signing can be involve policy mapping which is often complex.
- Public key cryptography requires significant processor resources.
- PKI requires highly secure facilities for certificate authorities.

Addressing PKI Issues

- Standard PKI Policies and Procedures for SG
  - E.g. X9.79 Financial Services Industry
- Standard Certificate CP OID and naming conventions
- Smart Grid PKI Accreditation Service
- Tools build to those standards
  - Certificate Management Tools
    - Vetting, Issuance, Revocation & Status
  - RP Policy/Trust Anchor Management Tools
  - Auditing Tools
  - Software Signing and HAP tools.

Solution to PKI Issues

PKI Issue	Proposed Resolution
PKIs can be complex to set up and operate.	SG Standards reduce the burden on operator by certifying a finite set policies with know security characteristics.
PKIs require complex certificate policy documents and certificate practice statements.	SG PKI operators can use industry wide standard CP templates based on SG certificate policy standards
Cross-signing can be involve policy mapping which is often complex.	Two organizations with standards based policies should not need to perform policy mapping.
Public key cryptography requires significant processor resources.	ECC algorithms are efficient enough to run on 8 bit processors, and are being developed for RFID tag operations. These chips are low cost and low power.
PKI requires highly secure facilities for certificate authorities.	Yes, but it lowers risk and cost elsewhere. Another way to say this is that PKI enables trust and security to be provided by well protected off-line entities.

Take Always

SG PKI operators can reduce cost and complexity, while providing a system with a provable levels of security through;

- industry standardization of certificate usage and management, including naming conventions and standard policies,
- and tools developed around those standards.

For Additional Information

- NISTIR 7628 Volume 2 Chapter 6 “Cryptography and Key Management.
- IEEE Transactions on Smart Grid, Volume 1 Number 1, “Security Technology for Smart Grid Networks” 99-107.
- “Smart Grid Security Selected Principles and Components” Presentation at IEEE PES Conference on Innovative Smart Grid Technologies, Jan 2010 http://www.ieee-pes.org/images/pdf/isgt2010/january_19_2010/4-smart-grid-security/Smart-Grid-Security-Tony-Metke.pdf
- “Smart Grid Applications, Communications, and Security”, Berger et. al. Chapter 13 “Smart Grid Authentication and Key Management” http://www.amazon.com/Smart-Grid-Applications-Communications-Security/dp/1118004396