

YarCom[®] Inc.

SCADA Key Management Infrastructure (SKMI): Can Be Done Today

Dr. Gus Lott

YarCom[®] Inc

Reno, NV



- Generate, exchange, store, use, and destroy credentials and cryptographic keying materials within a cryptographic boundary that complies with FIPS PUBs 140-1 or 140-2 Level 2 or higher standard.

AGA 12-1 § 4.2.1

KMI requirement

- Scale
- Generation
- Distribution
- Use
- Re-key/Destroy
- Missed issues
- Conclusion

- Pedernales Electrical Coop – US largest
 - 8,100 square miles
 - 191,264 members
 - 14,898 miles of distribution line
 - 320 miles of transmission line
 - 69 substations
- 200 distribution breakers
- 12,000 remotely devices in control database (What is a device?)

- Austin Electric
 - 400,000 customers
 - 9,000 miles of distribution line
 - 48 substations
- 2744 SCADA transmission devices in database
- “Not many distribution control devices”

YarCom[®] Inc. **Electric Reliability Council of Texas**

- 80% of Texas transmission
- 37,000 miles of transmission lines
- > 100,000 transmission control devices on “5000 busses”
- Historian receives > 1 Mbps 24/7 continuous data input rate

**Reasonable SCADA KMI should support
 10^3 to 10^5 keyed devices.**

- Scale similar to other deployments
 - PKI X.509v3 - > 5,000,000 in one medium assurance infrastructure
 - RFID EPC Class 1 Generation 2 - EPCglobal Certificate Profile – millions!
 - Available sensor KMI models
 - SCADA Key Management Architecture (SKMA)
 - Sandia Key Management (SKE)
 - Localized Combinatorial Keying (LOCK)/Exclusion Based Systems (EBS)

- Who is the cryptographic keying material authority/provider for the system operator?
 - Employee
 - Third party
 - Risk/cost based decision
- Must include a continuity, restoration, and archival escrow authority/provider
- Directory & inventory service closely coupled – make it one service

- Initial deployment – new devices vs. bolt on
 - Internal serial or other device specific ID – *something it is*
 - Hardware or well-isolated software key pair - *something it has*
 - Tamper resistant
- Logically combined management functions
 - Inventory
 - Address/channel/number – *something it knows*
 - Key material

- ***Just do it !***
- Versioning is a huge use issue
 - 5 to 10 year roll-out – NMCI example
 - Threats change
 - Security standards change
- Lack of commitment – “Utility owners say they realize cyberattacks pose a risk but don’t see it as a huge problem.”
 - William Rush, Gas Technology Institute, *SCADA on thin ice*, *FCW* May 8, 2006

- AGA 12 series address most other use issues
- **Communications overhead** from this info exchange
- Validation
- SCADA – nearly static population
 - Don't rely on human-user PKI lessons learned
 - Long life-cycle and additions rather than constant turn over

- Re-key – what is the periodicity?
- Maintenance personnel or KM specific personnel
- Equipment replacement & versioning
- Validation
 - Essential portion of re-key
 - Anti-tamper check included
 - Physical vs. cyber
- Set a schedule and commit to it

- To minimize, consistent with security policy, the burden imposed by key management on SCADA operations.
- To minimize the inconvenience and complexity imposed on the user.

AGA 12-1 § 4.4.1

This is the great BUT...!

- Turn it off attack - most any attack will drive the user off the cryptographic system to something that “works”.
- Communications overhead - >1Mbps to historian – it’s own denial of service
- Insider threat
- TRANSEC
 - Layer-1 denial of service
 - Link intrusion
 - APCO model for secure communications

- It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:
- (d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- (e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or

Homeland Security Presidential Directive 7
Dec 17, 2003

- “...private sector owners and operators should be encouraged to provide **maximum feasible security** for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.”

PRESIDENTIAL DECISION DIRECTIVE/NSC-63
May 22, 1998

- Existing, scalable, proven KMI in place today – not a one vendor solution
- Including KMI hardware tokens, readers, and API's within the PLC, RTU, IRTU, IEPC, CM devices – done today in other devices
- ASA 12-1 calls for FIPS 140-2 validation – enforcement? Done today if serious.
- Mandated use – not a burden excuse – yet to be done
- Vendors with new devices – when?
- ***JUST DO IT !***

Questions ?

Dr. Gus Lott

775-742-6804

gklott@yarcom.com