Control System Security: A Case Study in Collaboration

Stephen Hilt – TVA
Sharon Xia – AREVA
Mike Assante - NERC
Dale Peterson – Digital Bond
Clint Kreitner – Center for Internet Security (CIS)

The collaborators

- The asset owner/operator – TVA
- The control system vendor – AREVA
- The consultant (with DOE funding) – Digital Bond
- The configuration standards – CIS
- The cybersecurity standards – NERC

The Asset Owner/Operator View

- The motivation to improve Control System security
  - NERC CIP compliance
  - NIST/FISMA compliance
  - Risk Management
- Security Configuration standard
  - The use of COTS software platforms
  - Change Management
  - Industry standard settings over in-house developed standards.

Goal of the NERC CIP Program

- Encourage voluntary collaboration to develop benchmarks to be used by BPS entities
- Motivate the supply chain via the procurement process
- Encourage collaborations among asset owners, security researchers, and vendors
- Mandatory reliability standards are necessary, but are not sufficient as they tell you “what to do” and not “how to do it” & standards are more static in nature
- Compliance does not necessarily achieve a significantly improved security posture, unless entities adhere to proven and expert developed practices

Building on the Standards

- Advanced collaborations can take the best knowledge from the right people/organizations and apply it in a time sensitive manner
  - Keeps up with technology (new system versions/upgrades)
  - Keeps up with the ever changing threatscape
  - Harnesses expertise and interest of:
    - Cyber security researchers
    - Security professionals and facilitators
    - Security administrators

Electric Infrastructure Protection

- A real community effort!
  - Provides a channel to apply information developed from government funded research efforts
  - Develops sound practices in the form of configurations that brings security value to CIP compliance
  - Gives asset owners the ability to proactively integrate and verify security of critical cyber assets before deploying them
  - Helps the vendors support their customers, design winning products, and improve their product development process

The CIS Benchmarks

- Produced via expert consensus (>1,500 SME's)
- Current portfolio of 50 IT benchmarks
  - Recommended values for configurable settings
    - Desktop
    - Mobile
    - Network
    - OS
    - Printers
    - Servers
  - Multiple hardening levels
- CIS-CAT - CIS Configuration Audit Tool
  - Scores a system against the benchmark values

1.3.10Audit Policy: Privilege Use: Sensitive Privilege Use

Description:
This control defines whether the audit is activated when a user account or service uses a sensitive privilege. It is recommended that this setting be configured as described below:

- For the Enterprise Member Server and Enterprise Domain Controller profile(s), the recommended value is `No auditing`.
- For the SSLF Member Server and SSLF Domain Controller profile(s), the recommended value is `Success and Failure`.

Rationale:
Enforcing audit settings allows for security incidents to be detected and enough evidence to be available for analysis of those incidents. Certain regulated industries require the logging of certain events and activities.

Remediation:
To establish the recommended configuration via GPO, set the following to the value prescribed above:

```
Computer Configuration\Windows Settings\Security Settings\Advanced Audit
Policy Configuration\System Audit Policies - Local Group Policy
Object\Privilege Use\Audit Sensitive Privilege Use\Audit Policy: Privilege
Use: Sensitive Privilege Use
```

Perform the following to establish recommended configuration state via auditpol.exe.

```
auditpol /set /subcategory:"Sensitive Privilege Use"
[/success:<enable|disable>  /failure:<enable|disable>]
```

Audit:
Navigate to the GPO articulated in the Remediation section and confirm it is set as prescribed. To audit the system using auditpol.exe, perform the following:

```
auditpol /get /subcategory:"Sensitive Privilege Use"
```

Default Value:
`No auditing`

References:
CCE-2205-3
CCE-2349-9

Digital Bond's Bandolier

- Dept. of Energy Research Contract
- Identify Optimal Security Config Settings
  - Start with industry guidelines on OS, IT apps
  - Test with vendor to insure they don't break it
  - Identify SCADA/DCS specific security settings
- Create Bandolier Security Audit File
  - Automate testing of thousands of parameters
  - Works with Nessus Compliance Plugin / Low Impact
  - Available from Digital Bond or ICS Vendor

AREVA e-terra Numbers

- Linux System: 1337 Security Settings
  - Client, App Server and Web Server
  - 110 e-terra application checks
- Windows System: 676 Security Settings
  - Client, App Server and Web Server
  - 63 e-terra application checks
- Application Check Example
  - Are trace files configured to record operator actions?

Bandolier Security Audit Files

- ABB 800xA [dev]
- ABB Ranger
- AREVA e-terra
- Emerson Ovation
- Matrikon OPC
- OSIsoft PI Server

- Siemens Spectrum Power TG
- SISCO ICCP [dev]
- SNC GENe
- Telvent OASyS DNA
- Toshiba TOSMAP [dev]

- More to come

Meet Customers' Needs

- Security baked into the products
  - Provided security guides for the AREVA products
    - **e-terra***platform* Network Security Guides
    - **e-terra***platform* System Security Guide – Windows
    - **e-terra***platform* System Security Guide – Linux
- Cost effective ongoing monitoring by asset owners
  - The 10 AREVA Bandolier templates
- Auditable reports for compliance
  - NERC CIP-002 through CIP-009
  - NIST/FISMA

Adopt Industry Best Practices

- The AREVA System Security Guides and Bandolier templates
  - Based on the CIS Benchmarks
  - Customized to fit the AREVA Systems
- Collaboration with Digital Bond
  - Provided automated audit tool
  - Customized Bandolier OS templates for AREVA systems
  - Produced templates for application checks
  - Tested the AREVA Bandolier templates in the R&D lab

Deliver Secured Systems

- Harden the systems in FAT
- Customize the AREVA Bandolier Templates to conform to customers' security policies
- Audit the systems using Nessus and the Bandolier templates in FAT and SAT
- Deliver the customized templates with the systems to customers
- Provide trainings

Benefits to the Owner/Operator

- Deployment of new systems
  - Documented and audited secure configurations
    - Assure only necessary services are enabled
      - Disable FTP, telnet, etc..
    - Set appropriate file and registry permissions
- Maintaining secure configurations over time
  - Use of industry recognized configuration standards
    - Reduction in configuration errors
    - Vendor product updates

Benefits to the Owner/Operator

- Scan results provide documented evidence for compliance audits
  - NIST/FISMA
  - NERC

Ongoing …

- Generic CS benchmarks for W7, Server 2008
  - Benchmark teams now forming
    - Call for participation

- Vendor application product specific benchmarks

- Collaboration…
  - The power of many working toward a common goal
    - TVA, NERC, AREVA, Digital Bond, DOE, CIS