Secure Remote Substation Access Solutions

Supplemental Project - Introduction Webcast

October 16, 2013

Scott Sternfeld, Project Manager
Smart Grid Substation & Cyber Security Research Labs

ssternfeld@epri.com
(843) 619-0050
Agenda

• What is a Secure Remote Substation Access System?

• History of EPRI’s Remote Substation Access Research
  – 2012 project and workshop
  – Interest Group
  – Supplemental project

• Review of Top Challenges/Proposed Tasks
  - Penetration Testing
  - Device compatibility testing
  - Password Vault Integration

• How YOU can get involved!
What is a Remote Substation (IED) Access System?
Remote Substation Access System

• **What is it?**
  – Provides for remote “engineering” (manual) access to all substation (or field) devices (IEDs) in a secure fashion.
  – Optional: Integrated file extraction (automated) as part of an overall data integration solution.
  – Replaces a Terminal Server / “Jump Host” solution.
  – Can be used as a tool to aid in NERC CIP compliance.
    • Provides technical controls
    • Reporting capabilities
  – May also include:
    • Password management
    • Configuration (change) management for IEDs
    • Asset management
Cyber Security and Privacy 2012 Project: Assessment of Remote Access Solutions

Purpose:
Work with vendors and utilities to assess several products providing Interactive Remote Substation Access.

Approach:
- Develop comprehensive list of requirements
- Develop use cases/scenarios
- Vendor deployment in Smart Grid Substation Lab
  - Some configuration/development required
- Vendor demonstrations of scenarios

Presenting utility requirements with a ‘unified voice’
Cyber Security and Privacy 2012 Project: Assessment of Remote Access Solutions

• Requirements workshops:
  – May 23rd and June 13th, 2012

• Product demonstration:
  – Oct 24-25th, 2012 Knoxville, TN
  – Wide range of audience
    “Substation Security and Remote Access Implementation Strategies”

Utility Value:
  – Awareness of available products
  – Common demonstration platform
  – Vendor products improved

Vendors and utility collaboration for accelerated technology transfer
EPRI’s Cyber Security Research Lab
Knoxville, TN

Five vendors installed in the lab:

• EnterpriseSERVER.NET by Subnet Solutions

• CrossBow by Ruggedcom, a Siemens Business

• SEL-3620 by Schweitzer Engineering Labs

• ConsoleWorks by TDi Technologies

• IED Manager Suite (IMS) by Cooper Power Systems

• Potentially others…

Installation in a Common Demonstration Environment


Integrated file extraction (Relay, DFR, Meter, Transformer, other data)

Independent file extraction (DFR, Meter, Transformer, other data)

3rd Party Data Integration, Analysis and Presentation Tools/Applications
EnterpriseSERVER.NET - Subnet Solutions
CrossBow Secure Access Manager - Ruggedcom

The image shows the CrossBow Secure Access Manager interface with various devices and connectivity options displayed. It also includes a terminal emulator window with command output, indicating device connections and statuses.
ConsoleWorks – TDi Technologies

[Image of a computer interface for ConsoleWorks, showing various consoles and their status.]

© 2013 Electric Power Research Institute, Inc. All rights reserved.
IED Manager Suite - Cooper Power Systems
Remote Access Timeline

2012

2012 project:
Oct Workshop

2013

2014
Interest Group (Free!)
Secure Remote Substation Access Interest Group

Interest Group – open to all utilities!

– Webcasts to develop additional scenarios for testing
  • Identify top “challenging”, “unusual” or “difficult” IEDs, protocols or implementation challenges

– Can be discussion topics or working sessions
  • Ex. Mapping NERC CIP v5 requirements to Remote Access System capabilities or RFP requirements

– Discussions amongst peers

– Develop community of users
Secure Remote Substation Interest Group

Discussion topics with both EPRI and utility guest presenters:

• Implementation Challenges/Proposed Tasks

• Unique IED vendor integration challenges
  – *IED Compatibility Matrix*

• Password management issues and concepts
  – *Integration with Password Vault*

• NERC CIP v3 and v5 mapping

• Requirements review (one-on-one effort)

Identifying top Remote IED Access issues
Review of Top Challenges/Proposed Tasks
List of Remote Access Challenges/Tasks

1. Penetration Testing

2. Remote Access Vendor ↔ IED interoperability / compatibility tests

3. Integration with a “Password Vault”

Others:
• Password, Configuration, Change Management
• Alarm Correlation / Incident Management
• Coordination with Operations

These top items are planned to be addressed in our supplemental project, with additional items as time and funding permit.
Remote Substation Access Systems can manage our IED passwords, with role based access control and supporting CIP compliance…

...But are they SECURE?

Utilities have requested through the Interest Group for independent penetration tests to be performed on remote access systems.

We are now planning on including this task for 2014.
Scenario 1: Penetration Testing

Vulnerability Identification

• Databases
  – CVSS
  – CVE
• Configuration
  – CCE
  – CPE

NESCOR Testing Guides

• Guide to Penetration Testing
• Guide to Vulnerability Scanning

Tools

• Scanning
• Exploitation

A search on “SQL” and “passwords” in the NIST NVD CVSS produces 472 matches. These matches range from 1998 to 2013.
### Scenario 2: Remote Access Vendor ↔ IED interoperability / compatibility tests

<table>
<thead>
<tr>
<th>RA system / IEDs</th>
<th>SEL relay</th>
<th>GE UR relay</th>
<th>ABB Relay</th>
<th>Siemens Relay</th>
<th>PQ meter</th>
<th>DFR</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crossbow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESNET</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cooper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEL-3620</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TDI</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor X (example)</td>
<td>✔️</td>
<td>✗</td>
<td>✗</td>
<td>✔️</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Tests would be broken down into **specific** tasks such as:
  - Intelligent vs. Passive proxy
  - Ability to manage passwords
  - File/Event retrieval
  - Could include gateway products (RTAC, SMP, 2020, D20, SSNET)
Scenario 2: Specific Task function examples

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
</tbody>
</table>

### Advanced/ Automated Functions

**Login and Logout**
- **Automated login**
- **Automated logout**

**Passwords**
- **Change Device Password in gateway**
- **Change Password**

**Configurations**
- **Backup config**
- **Restore Config**
- **Get Config summary**

### Advanced/ Automated Functions

<table>
<thead>
<tr>
<th>Firmware</th>
<th>Events</th>
<th>SOE</th>
<th>Logs</th>
<th>Discover</th>
<th>Faceplate</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve firmware version</td>
<td>Compare firmware</td>
<td>Update firmware</td>
<td>Retrieve new event files</td>
<td>Retrieve SOE files</td>
<td>Retrieve device logs</td>
<td>Discover Connected devices</td>
</tr>
</tbody>
</table>
BYOD! (Bring your own device!!)
Scenario 3: Integration with a “Password Vault”
What is a “Password Vault”?

Benefits of a password management solution:
- Regular password changes improve security and compliance
- Control which users have access to passwords
- Allow detailed auditing of each use of these passwords

Some solutions offer advanced functionality including:
- Password Changes
- Password Verification
- Password Reconciliation

Automatic password management of service accounts either through ‘push’ or ‘pull’ approach
Scenario 3: Integration with a “Password Vault”

• Problem statement:
  – Multiple password vaults, different security or logging levels for various systems, makes difficult for auditing/compliance
  – Current IT Enterprise password vault products do not interact with substation IEDs

• Ideal end state:
  – Single integrated password vault to manage all shared/service account passwords.
  – Remote Access solution would connect to IEDs using passwords stored in Password Vault solution

• Potential solutions:
  – Integrate products via API
NERC CIP considerations:

“How do we be achieve remote access and remain compliant without being intrusive to the operational and maintenance activities??”
### Remote Access to CIP v5 mapping exercise:

#### Guide to Medium Substation Assets
- **Credit:** MidAmerican Energy and FirstEnergy
- **DRAFT standards as of November 2012 Recirculation ballot**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>007</td>
<td></td>
<td>5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.</td>
<td>-</td>
<td>Yes + PCA</td>
<td>n</td>
</tr>
<tr>
<td>007</td>
<td></td>
<td>5.2 Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).</td>
<td>Yes</td>
<td>Yes + PCA</td>
<td>y</td>
</tr>
<tr>
<td>007</td>
<td></td>
<td>5.3 Identify individuals who have authorized access to shared accounts.</td>
<td>-</td>
<td>Yes + PCA</td>
<td>y</td>
</tr>
<tr>
<td>007</td>
<td></td>
<td>5.4 Change known default passwords, per Cyber Asset capability</td>
<td>Yes</td>
<td>Yes + PCA</td>
<td>y</td>
</tr>
<tr>
<td>007</td>
<td></td>
<td>5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.</td>
<td>Yes</td>
<td>Yes + PCA</td>
<td>y</td>
</tr>
<tr>
<td>007</td>
<td></td>
<td>5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.</td>
<td>-</td>
<td>Yes + PCA</td>
<td>y</td>
</tr>
<tr>
<td>007</td>
<td></td>
<td>5.7 Limit unsuccessful attempts or generate alerts of unsuccessful authentication attempts</td>
<td></td>
<td>control centers only</td>
<td>y</td>
</tr>
</tbody>
</table>
Remote Access Timeline

2012

2012 project:
Oct Workshop

2013

June 2013

Secure Remote Access Interest Group

- Discussions
- Develop Test Scenarios

2014

Vendor product maturity
Exciting Supplemental Plans!
Secure Remote Substation Access Solutions Supplemental Project

This project will investigate and address implementation challenges for secure remote substation access security solutions, including:

- “Hands-on” workshop allows system familiarization and understanding of implementation challenges, best practices, and technology gaps

Areas of focus may include:

- Specific devices not easily integrated with existing solutions
  - Vendor proprietary IED tools/protocols
  - Use of multiple authentication devices/gateways

- Remote Access System Management of IEDs
  - Management and tracking of configurations
  - Patch management
  - Password management
Secure Remote Substation Access Solutions
Research Drivers

• Remote Access products are still maturing
  – Require support for legacy, current and future devices
  – Products must provide features to support changing cyber security and compliance requirements.

• Remote access to substations can provide new opportunities for data integration solutions such as fault location, asset optimization, and power quality monitoring.
  – Leads to improved asset monitoring

• Remote access can also reduce “windshield time” to reach field IEDs
  – Leads to improved restoration time

Value:
• This project is valuable to any utility that has or desires to implement secure remote access to substations, IEDs, and field equipment. The topics covered can be applied to both transmission and distribution substations.
Secure Remote Substation Access Solutions

Expected Key Results

Through participation in this supplemental, members will be able to:

• Learn about emerging technologies and solutions while gaining visibility into existing best practices

• Identify challenges unique to Remote Access systems

• Study implementation options, best practices and capabilities/limitations regarding the challenge.

• Share challenges, solutions and lessons learned with peers
Reasons to Participate

• Changes to NERC CIP may necessitate new features and new tests to be performed on remote access systems
  – Previous discussions with members highlighted NERC CIP as major focus with remote access systems.

• Side-by-side comparison of Remote Access Vendors in common environment
  – Unbiased visibility into vendor-based remote access solutions

• Demonstration and Workshop with individual presentations by remote substation access solution vendors.
Even More Reasons to Participate

EPRI’s Cyber Security Research Lab

• Take advantage of EPRI’s lab as **YOUR** resource!
  – Labs are difficult to maintain
  – Variety of multi-vendor substation equipment
    • Able to introduce other equipment as requested
    • OR… “Bring your own device”

  – Utility labs may not include “end-to-end” architecture
    • EPRI’s reconfigurable lab allows modeling and testing with **YOUR** substation architecture.

  – “Try before you buy”
    • Remote access to EPRI lab for “hands-on” testing from your office!
Remote Access Timeline

2012 project: Oct Workshop

2013

June 2013

Secure Remote Access Interest Group

- Discussions
- Develop Test Scenarios

Remote Access Solutions Supplemental

- Develop/Enhance Features
- Applying Test Scenarios
- Penetration Testing

Solving Implementation Issues!

Vendor product maturity
Key Take-Aways:

• Remote Substation Access products are still in their infancy.
  – You are not the first one to implement these products or run into challenges.

• We need to build and strengthen a community of users now!
  – Challenge: Users span multiple organizations
  – Work together to share technical approaches to NERC CIP

• Developing **unified** utility requirements and test scenarios can improve the market offerings.

• **Together, we can accelerate the maturation process!**
Secure Remote Substation Access Solutions

2014 plans

Interest Group
Free to participate, open to all utilities:
• Remote Access *Interest Group*:
  – Discussion of challenges
  – Presentations on related topics by peers
  – Utility only (no vendor) participation

Supplemental
• Webcasts
  – Presentation by vendors
• Development/Integration efforts
  – Translate Interest Group challenges into testing scenarios
• On-site workshop with vendors at EPRI labs. Knoxville, TN
  – Live demonstrations, interaction with vendors
  – Share challenges, solutions and lessons learned by peers
Secure Remote Substation Access Solutions

Objectives and Scope
• Address implementation challenges identified by the Secure Remote Access Interest Group such as:
  – Scalability
  – Management and tracking of IED configurations
  – Use of multiple authentication devices/gateways
• Provide implementation options and best practices
• Conduct a Secure Remote Access Workshop

Value
• Gain new knowledge and practical guidance on a variety remote access solutions and scenarios
• Coordinate with vendors to advance the capabilities of remote access solutions

Details and Contact
• Price: $40,000
• Qualifies for TC and SDF
Scott Sternfeld
• ssternfeld@epri.com
• 843-619-0050
SPN Number: 3002001767
Key meeting reminders and links

Secure Remote Substation Access Solutions – Introductory Webcast
October 16th Webcast - NOW
SPN Number: 3002001767

Remote Access Interest Group Calls
Quarterly: Nov 2013; Feb, May, Aug, Nov 2014

NERC CIP Tools and Techniques - Introductory Webcast
October 17th Webcast 11-12pm EST
Add to Calendar
SPN Number: 3002001768

For questions, please contact: Scott Sternfeld
• ssternfeld@epri.com
• 843-619-0050
NERC CIP Tools and Techniques

Objectives and Scope
• Provide guidance for transitioning to NERC CIP Version 5
• Project may focus on:
  – Configuration change management
  – Patch management
  – Identity access management
  – Determination of BES cyber assets and BES Cyber Systems

Value
• Identify gaps in current tools that have been deployed to address the CIP requirements
• Provide guidance and techniques for complying with CIP requirements

Details and Contact
• Qualifies for TC and SDF
  Scott Sternfeld
  • ssternfeld@epri.com
  • 843-619-0050
  SPN Number: 3002001768
Together…Shaping the Future of Electricity
Please observe these Antitrust Compliance Guidelines:

– Do not discuss pricing, production capacity, or cost information which is not publicly available; confidential market strategies or business plans; or other competitively sensitive information

– Be accurate, objective, and factual in any discussion of goods and services offered in the market by others.

– Do not agree with others to discriminate against or refuse to deal with a supplier; or to do business only on certain terms and conditions; or to divide markets, or allocate customers

– Do not try to influence or advise others on their business decisions and do not discuss yours except to the extent that they are already public
Architectures
Sample Network Environment

Corporate

Corporate User
R.A. Client s/w (option)

Corporate Router

DMZ

Modem

wCorp01T

Corp

Corporate services
-Active Directory, RSA
-Other Enterprise Applications

-Security Authentication Server
-Enterprise & Vendor Applications

Phone network (PSTN)

Example Smart Grid Substation

R.A. substation client (option 1)

Security appliance

R.A. substation client (option 2)

Gateway/Data Concentrator

Other IED

PQ Meter

Transformer Monitor

Comm link

RTU

Card reader

DFR

I/O

Relay

R.A. substation client (option 3)

Security video

Simplified model representation:

Corporate User

Corporate User = R.A. client s/w or PDP
(RSA token optional)

Firewall

DMZ Server

R.A. Server s/w

Modem

“Network Cloud”

Security appliance

R.A. substation client (option 1)

Gateway/Data Concentrator/Comm Processor/RTU

IED

Security enabled phone switch

Substation Router

Transformer monitors

-Transformer monitors
-Card readers
-Video monitoring
-Distribution Automation (D/A)
-Historian Node

© 2013 Electric Power Research Institute, Inc. All rights reserved.
Engineering Access and File Extraction

Integrated file extraction
(Relay, DFR, Meter, Transformer, other data)

Independent file extraction
(DFR, Meter, Transformer, other data)

3rd Party Data Integration, Analysis and Presentation Tools/Applications

Asset Management
Power Quality Applications
Fault Location Applications
Data Presentation/Dashboard

Utility Office Environment

Substation Environment


Secure Remote Access Server
Secure Remote Access Client (Token optional)
File Repository

FMS
Operational Data
"Non-Operational Data"

Manager
Router
Legacy Comm Processor
Modern Data Concentrator
DFR
Transformer Monitor
PQ meter

Ethernet connection
Serial connection

Secure Remote Substation Access Interest Group

A Technology Transfer Outreach Effort of the EPRI Cyber Security Program

Purpose of the SRSA Interest Group

The SRSA Interest Group is a forum for utilities to share experiences and best practices, discuss the tools and techniques, and exploring research topics for the advancement of secure remote substation access.

There is an established need for remote substation access solutions that provide support for a wide range of IEDs including current, legacy, and future devices, and also deliver the required level of cyber security and compliance support. Remote communications access to substations can provide new opportunities for data integration solutions such as fault location, asset optimization, and power quality monitoring. It may also reduce the number of times field personnel are required to visit substations to retrieve IED configuration or event files for analysis. However, balancing this level of access with cyber security and potential regulatory compliance requirements can be very difficult. This balance can be achieved through proper preparation, procedure implementation, and organizational support.

The objectives of this interest group are to identify implementation challenges for secure remote access functionality, advance the state-of-the-art of secure remote access systems for the power delivery domain, and build a community of end users to socialize secure remote substation access concepts and best practices.

Key activities for the interest group include:

Additional Resources

July 18th, 2013
Secure Remote Access Interest Group Webcast
Recording (17.7 MB)
Presentation (2 MB)

June 6th, 2013
Secure Remote Access Interest Group-kickoff Webcast
Recording (12 MB)
Presentation (3 MB)

EPRI Secure Remote Substation Access Interest Group Charter - May 2013 (71 KB)

For more information, contact Scott Sternfeld at EPRI.
EPRI’s Smart Grid Substation Lab
Knoxville, TN

Product testing and demonstration site:
Common environment for all vendors