Safeguarding Substations Against Electronic Intrusion

Making Electric Power Safer, More Reliable, and More Economical™

Presented to the
APPA Engineering & Operations Technical Conference Program
San Antonio, Texas
Tuesday, March 9th, 2004
By
David Costello
Presentation Outline

- What is Electronic Intrusion?
- Review of Substation Communications
- Review Increasing Threats
- Suggest Mitigating Technologies
- Provide References
What is Electronic Intrusion?

“There is entry into the substation via telephone lines or other electronic media for the manipulation of electronic devices including digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, PLC, and communication interfaces.”

Substation Communications Benefits

- Faster Fault Clearing
- Faster and Automated Sectionalizing and Service Restoration
- Real Time Monitoring and Diagnostics
- Wear-Based / JIT Maintenance
- Fault Location, SER and Event Reports for Rapid Troubleshooting and Root Cause Analysis
Substation Communications Benefits

- Concurrent Access to Valuable Information by Multiple Users
- Remote Control and Configuration
- Instant Notification of Events and Alarms by SCADA, Local HMI, E-mail, Pager, and Phone
Who Says There is an Increasing Risk?

- White House
- FBI’s National Infrastructure Protection Center
- DOD Defense Information Systems Agency
- Critical Infrastructure Assurance Office
- IEEE Standard 1402 - 2000
- North American Electric Reliability Council
- National Security Telecommunications Advisory Committee
- Electric Power Research Institute
- National Security Agency
- National Institute of Standards and Technology
What is Causing the Increased Risk?

- Industry Pressure to Downsize, Automate, and Cut Costs
- Instability in Electric Utility Job Market
- Instability in Electric Power Service
- Shift from Proprietary I&A Systems to Networked Solutions With Open Protocols
- Increased Dial-in and Network Access
- FERC 888 / 889 Open Access Requirements
What’s Causing the Increased Risk?

- Increased State Espionage and Terrorism
- Increased Industrial Espionage
- Increase in Nationally-Sponsored Information Warfare Efforts (At Least 13 Countries per CIA)
- Increase Use of Hacktivism
- Blunders, Errors, Omissions
- Fraud, Theft, Criminal Activity
What is Causing the Increased Risk?

- Rapid Growth of Computer Literacy
- Increased Recreational and Nuisance Hacking
- Widespread Availability of Hacker Tools
  - 20-40,000 Viruses in McAfee / Symantec Databases
  - 3 New Viruses per Day (DOD)
  - 30-40 New Attack Scripts per Month (NIST)
### Quick Research Results

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population of the US</td>
<td>292M</td>
</tr>
<tr>
<td>Number of Households in US</td>
<td>110M</td>
</tr>
<tr>
<td>% of Households with PC</td>
<td>60%</td>
</tr>
<tr>
<td>Average People per Household</td>
<td>2.6</td>
</tr>
<tr>
<td># of People with Access to a PC</td>
<td>183M</td>
</tr>
<tr>
<td>Population of the World</td>
<td>6.3B</td>
</tr>
<tr>
<td>% of World Internet Population in US</td>
<td>30%</td>
</tr>
<tr>
<td>World Internet Population</td>
<td>610M</td>
</tr>
</tbody>
</table>

Unscrupulous (Bad People with Criminal Intent) + Competent (People with Knowledge of a System) = ?
Worst Case Consequences

Note – August 14th 2003 NE Blackout Not Caused by Electronic Intrusion
But We Need to Put This in Perspective

Causes of Damage to the North American Electric Infrastructure

1. Natural Disasters
2. Deliberate Physical Attacks
3. Accidental Damage
   ...
4. Electronic Intrusions
Importance of “Strong” Passwords

- Strong Passwords are the Easiest and Best Defense
- Strong Passwords Contain
  - 6 or more characters
  - Mixed case sensitivity
  - At least one special character
  - No names, dates, acronyms, or pronounceable words
- Example – The Palouse has four beautiful seasons!
  - TPh4bs!
  - >5,100 years to “crack” at 10Mbs (DOD)
More Password Recommendations

- No Equipment “Backdoor” Passwords
- Replace Manufacturer’s Defaults
- Devices Should Allow:
  - 6 or more characters
  - 90 character alphabet
  - Obfuscation of password length
  - @@@@@@ Echo During Entry
Password Policies

- Passwords Should be Known Only to Individuals with Authorized Access
- Teach Password Security and Monitor Compliance
- Keep Passwords in a Secure Location
- Change Passwords:
  - Periodically (NSA recommends quarterly)
  - Whenever Security is Compromised
Access Restrictions and Control

- Use Port Inactivity Timeouts
- Use “Three Strikes – You’re Out” Denials

Which Initiate:
- Timed lock-out
- Physical alarm
- Disconnection of physical modem or telnet session
- Warning banner
  
  Access Denied.
  WARNING! Access by unauthorized persons strictly prohibited.
Access Restrictions and Control (2)

- Physical or Software Access Control
  - SCADA-Supervises Dial-Up Modem
    - Modem Port Setting $\text{NOCONN} = \text{RB1}$
  - Physical Permissive Supervises Remote Access
    - Control Switch for Local or Remote Control

- Monitor Alarms for Intrusion and Device Health

- Store Access Logs in Non-Volatile Memory and Review Frequently
Access Restrictions and Control (3)

- Use Two or More Levels of Password Protection
  - One for viewing data
  - Second for settings and controls
    - Alarm on access to Level 2
    - Do not allow feature to be disabled
  - In integrated systems, partition real-time protection from SCADA components

- Star Topology Increases Survivability and Security
Secure Modem Connections

- Open Auto-Answer Modems Susceptible to Auto-Dialers and Provide Backdoor to Utility Network
- Modem Key – Lock Pairs
  - Point-to-point connection
  - Can be applied between phone line and operation equipment
- Encrypting Modems
  - Restrict access and encrypt data
Secure Modem Connections (2)

- Dial-Back Modems Must be Secure to Prevent Hang-Up Spoofing
- Can be Used At One End of Existing Connection
- Dial-Back Modem Recommendations:
  - Force at least a five ring auto-answer
  - Use predefined dial-back numbers only
  - Force a one-minute dial-back delay
  - Force a password time-out disconnect
  - Disconnect after three bad passwords
Secure Modem Connections (3)

- Dial-Back Modem Recommendations:
  - Force a five-minute inactivity time-out after disconnect
  - Use only direct access local settings
  - If possible, implement a separate password management account responsible only by direct connection to the modem

- Reference 12 Lists Options Under $1000
- Use War Dialers within your Own Domain to Locate Unauthorized or Forgotten Modems
Low-Cost Secure Modem Devices

Modem
Key / Lock

Matched
Crypto-Modems

Programmable Password-Controlled Modem
Authentication Technologies

- Access Restriction and Authentication are Cornerstones of Secure Networks
- Provides One-to-One Mapping Between a User and a Key
- Keys Can be:
  - Physical – e.g. Electronic Access Badge
  - Knowledge-Based – e.g. PIN or Password
  - Biological – e.g. Fingerprint, etc.
Authentication Technologies (2)

- Convenient in that they can be applied to a Computer Port
- Match the Strength of Authentication to the Criticality of the Data and Equipment Being Protected
  - Two- and three-factor authentication may be needed in safety-critical operations
- Reference 12 Lists Options Under $1000
Low-Cost Authentication Devices

- Proximity Reader and Badge
- Token Key Generators
- Programmable Buttons
- Fingerprint Scanner
Network Security

- **Firewalls**
  - Protected gateway to defend perimeter against external intrusions
  - Hardware and/or software means of segmenting networks with restricted access into and between segments
  - Be sure to secure “back doors”, e.g. modem connections
Network Security (2)

- Virtual Private Networks
  - Internet Protocol Security (IPSec) encryption and authentication combined with Firewalls
  - Forms a point-to-point, secure, encrypted connection over a public network
  - Often referred to as “tunneling”
Low-Cost VPN Devices
Network Security (3)

● Intrusion Detection Systems
  ♦ Employed to detect misuse and external intrusion
  ♦ Two methods
    ▪ Signature detection matches known, observable intrusion characteristics against a database of profiles
    ▪ Anomaly detection compares ongoing system behavior against a profile of normal behavior
Network Security (4)

- Eliminate Unused Accounts and Unnecessary Ports and Services
- Enable All Web-Browser Security Options and Site Restrictions (e.g. disable anonymous logins)
- Separate Insecure Activities (e.g. web surfing, e-mail) from Critical Systems
- Update Security Patches and Virus Scanners Diligently
- Keep Communication Configuration, System Details, and Network Access Private
Network Security (5)

- Use Star Topologies and Network Switches, Not Hubs
- Use IDSs, Virus Scanners, and Firewalls to Protect Your Perimeters
- Segregate Systems (e.g. Enterprise-level IT from SCADA from Protection)
- Review Alarms and Logs Daily
Wireless and Telecommunications Security

- Assume Your Wireless Network is Public, and Follow All Recommended Practices for Public Network Security
- Be Aware that Telecommunications Providers are Insiders with Access to Your Data; Assume it is Visible Unless Encrypted
- Implement Alarm Conditions to Monitor Abnormal Use
Encryption Technologies

- Unencrypted Data are Susceptible to Eavesdropping
- Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules
Encryption Technologies (2)

- Cryptographic Concepts
  - Confidentiality, or sending messages over an insecure medium without exposing the concepts
  - Data Integrity, or ensuring that the message alterations or substitutions are evident and can be reconstructed
  - Authentication, or unambiguously determining the origin of a message
Scrambling Basics

- Goal of an encryption algorithm is to transform the data in a manner that is reversible for anyone with knowledge of a shared digital key.

Concerns for Utility Applications
- Additional Latency
- Increased Bandwidth
- System Reliability in Presence of Noise
Utility Applications for Encryption

Point-to-Point Real-Time Protection or Dial-Up Connections

Point-to-Multi Point SCADA Connections
Develop Company Policies

● At a Minimum, Policies Should Contain Company Positions Regarding:
  ♦ Access Rights, Passwords, Antivirus Software, Perimeter Security
  ♦ Remote and Wireless Access Concerns
  ♦ New and Departing Employee Policy
  ♦ Administration Rights
  ♦ Backups and Recovery Strategy
  ♦ Vendor and Visitor Policies
  ♦ Audits
NERC Cyber-Security Standard

- Effective Password Management, Including Periodic Password Changes
- Disabling Expired or Unused Computer Accounts
- Disabling Unused Network Services and Ports
- Identification of Vulnerabilities and Responses
NERC Cyber-Security Standard

- Secure Dial-Up Modem Connections
- Firewall Management
- Intrusion Detection Processes
- Security Patch Management
- Installed and Updated Antivirus Software
- Retention and Review of Operator, Application, and Intrusion-Detection Logs
The Best Offense is a Good Defense

- Realize that Security is a Never-Ending Process
- Think Like a Hacker
  - Use a Port Scanner to Identify Your Own Active, Unguarded Ports
  - Use a Ping Sweeper to Find Unauthorized or Forgotten IP Addresses on Your Own Domain
  - Use a Network Sniffer and/or Trace Route Tool to Verify Your Network Configuration is As Intended
References


2. Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems – Oman, Schweitzer, Frincke

3. Electronic Security of Real-Time Protection and SCADA Communications – Risley, Roberts, LaDow

4. Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusion – Oman, Schweitzer, Roberts

Available at www.selinc.com
5. The Hows and Whys of Ethernet Networks in Substations – Woodward


8. Methods for Securing Substation LAN Communications – Dolezilek

Available at www.selinc.com
References (3)


10. Securing Ethernet Products with VPN Technology – Risley, Marlow, Oman, Dolezilek

11. Setting and Using Secure Dial-Back Modems with Relays and Communications Processors – Oman

12. Low-Cost Authentication Devices for Secure Modem and Network Connections – Oman

Available at www.selinc.com