Cybersecurity of the Electric Distribution System

Dr. Murty V.V.S. Yalla, Fellow IEEE

President

Largo, FL

IEEE PES 2016 GM
Smart Distribution Working Group meeting
Monday, July 18, 2016, 2:30 PM to 3:00 PM
Outline of presentation

• Introduction
• Cyber attack on the Ukrainian Utility
• Concerns on Cybersecurity of Electric Distribution systems
• IEEE and other Standards on Cybersecurity
• Implementation example – Cybersecurity embedded in Distribution IEDs
• Conclusion
Introduction

• Modern electric power substation and feeder equipment (protection, automation and control IEDs) are being deployed with advanced communications networks which make them more vulnerable to cyber threats

• Smart meters and DER with smart inverters are increasing in numbers which are connected to the communications network

• Hackers can cause severe disruptions to electric grid if proper security measures are not taken

• Several IEEE as well as other standards are being developed to provide guidance and standardization in Cybersecurity area so that different electronic controls can communicate securely

• This presentation identifies concerns on Cybersecurity of electronic controls in the electric distribution area and provides an example of embedded cybersecurity implementation.
Who are the attackers?

- Nation States
- Organized Crime
- Other Criminal Elements
- Disgruntled Employees
- Terrorists
- Hackers
- Industrial Competitors
- Careless Employees
- Political
- Internal
- Financial
- Chaos
Cyber attack on the Ukrainian Utility

- It was 3:35 p.m. December 23, 2015 inside the Prykarpattyoblenergo control center (in the western Ukrainian region of Ivan-Frankivsk), which distributes power to the region. The cursor on the control center computer suddenly skittered across the screen of its own accord.

- The operator watched as the cursor navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline.

- A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm.
Cyber attack on the Ukrainian Utility

- Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.
- The operator grabbed his mouse and tried desperately to seize control of the cursor, but it was unresponsive.
- Then as the cursor moved in the direction of another breaker, the machine suddenly logged him out of the control panel.
- Although he tried frantically to log back in, the attackers had changed his password preventing him from gaining re-entry. All he could do was stare helplessly at his screen while the ghosts in the machine clicked open one breaker after another.
Cyber attack on the Ukrainian Utility

- The attackers didn’t stop there, they also struck two other power distribution centers at the same time, taking 30 substations (seven 110 kV and twenty three 35 kV) taken offline and leaving more than 225,000 residents in the dark.

- As if that weren’t enough, they also disabled backup power supplies to two of the three distribution centers, leaving operators themselves stumbling in the dark.

- The hackers also flooded all the customer service phone lines (TDoS attack) so that the scale of attack is not visible to the distribution system operators.
Cyber attack on the Ukrainian Utility

- It was a multi-pronged and highly coordinated attack
- Suspected malware – BlackEnergy 3/KillDisk
- The hackers apparently came through remote-desktop-logging feature into the distribution SCADA system
- Hackers also rewrote the firmware in the devices (serial to Ethernet converters) which communicate with the breakers so that operators cannot automatically restore power
- The hackers apparently had reconnaissance operation on the Ukrainian utility system for 6 months learning about their system before the coordinated attack
- The maintenance staff had to drive to each of the substations to manually close the breakers to restore power after several hours as the automatic restoration did not work due to rewriting of the firmware in the communications devices
Concerns on Cybersecurity of Distribution IEDs

- Modern Distribution systems incorporate IEDs which communicate with Distribution Management Systems (DMS).
- The protection/control IEDs and DMS typically send commands to open/close breakers, Reclosers and switches.
- The DMS also sends commands to raise/lower a tap position of a LTC transformer and Voltage Regulator, open/close capacitor banks etc.
- All these actions use communications and a cyber attack on the communications system can create serious issues.
Cyber attack on distribution Protection & control IEDs

- Compared to Generation plants and Transmission Substations the distribution system IEDs are not physically protected.

- Majority of these IEDs are outside the fence of a substation mounted on a pole near residential neighborhoods and highways and have no physical barrier to protect them.

- Unless end to end security is maintained it is not difficult to hack into any of these IEDs and send commands mimicking DMS system commands.
IVVC System Architecture

CC: Capacitor Controller
RC: Regulator Control
TC: Tapchanger Control

Central SCADA Master
Cyber attack on distribution volt-var control IEDs

Distribution volt-var control system uses IEDs to control LTC transformers, Voltage Regulators and pole-top capacitor banks

Typical radial Distribution Feeder with IEDs for controlling LTCs, voltage regulators and Capacitors
Cyber attack on distribution volt-var control IEDs

Attack during a night when the load is light and the tap positions are on the lower end will be most severe.

Hypothetical Example: Conditions before the attack
Substation Transformer (TC) shows a tap position of 8L
Voltage Regulators (RC#1, RC#2 and RC#3) show a tap position of 4L
Capacitor banks (CC#1 to CC#11) all are OFF

Conditions after the attack: the hacker drives TC and RC#1 to #3 to 16R. Switches all Capacitor banks to ON.

Now looking at the voltage on the feeder:

- **LTC transformer going from 8L to 16R will increase voltage by 15%**
- **Voltage regulator changing from 4L to 16R will increase the voltage by 12.5%**
- **Capacitor banks changing from OFF to ON position will increase the voltage by 5 to 10%**

The cumulative affect of these actions can have as much as 30 to 35% overvoltage on the feeder causing sever damage to pole-top distribution transformers and customer equipment.
Cybersecurity Standards

IEEE Standards

• IEEE Std 1686-2013 “IEEE Standard for Intelligent Electronic Devices (IEDs) Cybersecurity Capabilities”

IEC Standards

• IEC 62351

NERC Standards

• NERC Critical Infrastructure Protection (CIP) CIP-002 to CIP-011

NIST

• NISTIR 7628-2014 Rev 1, Guidelines for Smart Grid Cybersecurity: Vol. 1, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
Government Regulation on Cybersecurity

• NERC Critical Infrastructure Protection (CIP) Standards have been an increasing focus of both NERC, which is charged with developing them and FERC, which must review and approve Standards before they can become mandatory.

• The latest version V5 incorporates more stringent requirements including strong password construction, authentication and encryption.
NERC CIP Background

• FERC Order 706 Approved Version 1 CIP Standards on January 18, 2008
• NERC Version 3 CIP Standards Currently in Effect
• NERC Standard Drafting Team formed to Address ALL FERC Directives
• FERC Order 791 Approved Version 5 CIP Standards on November 22, 2013
• NERC Version 5 Revisions Drafting Team formed on January 29, 2014
• Version 5 Compliance Deadline for High Impact and Medium Impact BES Cyber Systems is July 1, 2016
• Version 5 Compliance Deadline for Low Impact BES Cyber Systems is April 1, 2017
NERC CIP Version 5 – Time line

- **RAI - Reliability Assurance Initiative**

- **Finalize Evaluation Criteria for RAI Pilots**
- **RAI Enforcement Pilot Evaluation**
- **FERC Compliance & Enforcement Filing if necessary**
- **Filing of revised CIP V5 Standards (Jan)**
- **RAI Compliance Pilot Evaluation & CIP V5 Implementation Study Integration**
- **CIP V5 Standards Ballot Periods (Q2-Q3)**
- **RAI & CIP V5 Training and Awareness**
- **RAI Compliance Design Finalized (Dec)**
- **RAI Steady State Compliance and Enforcement**

Effective July 1, 2016
NERC CIP V3/4 to V5

- **High Impact**
  - Large Control Centers
  - CIP-003 to 009 V3/V4 “plus”

- **Medium Impact**
  - Generation and Transmission
  - Control Centers
  - Similar to CIP-003 to 009 V3/V4

- **All other BES Cyber Systems (Low Impact) must implement a policy to address:**
  - Cybersecurity Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Incident Response
NERC’s mandatory CIP standards address following areas:

**CIP-002: Cybersecurity — BES Cyber System Categorization**

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of Cybersecurity requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

**CIP-003: Cybersecurity — Security Management Controls**

To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-004: Cybersecurity — Personnel & Training
To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems

CIP-005: Cybersecurity — Electronic Security Perimeter(s)
To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-006: Cybersecurity — Physical Security of BES Cyber Systems
To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
**CIP-007:** Cybersecurity — System Security Management  
To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)

**CIP-008:** Cybersecurity — Incident Reporting and Response Planning – To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements

**CIP-009:** Cybersecurity — Recovery Plans for BES Cyber Systems -- To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES
CIP-010: **Cybersecurity – Configuration Change Management and Vulnerability Assessments** – To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

CIP-011: **Cybersecurity – Information Protection** -- To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES)
CIP-005: Electronic Security Perimeter

Part 1.1 – Electronic Security Perimeters: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.

Part 1.2 - Electronic Security Perimeters: All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

- If External Routable Connectivity, must define an Electronic Access Point
- Only applies when there is External Routable Connectivity

Part 1.3 - Electronic Security Perimeters: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
Part 1.4 - Electronic Security Perimeters: Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.

- The process must identify how to authenticate the user

Part 1.5 - Electronic Security Perimeters: Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

- Traffic inspection is part of requirement
- Multiple layers of perimeter protection
- If firewall fails, IDS can trigger a secondary security measure
Part 2.1 – Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

- Cannot be located in the ESP
  - Must authenticate before getting access to any Cyber Asset inside the ESP
  - Does not force presence of encrypted traffic inside the ESP
- Intermediate System serves as proxy
- Allows for restrictive rules
- Protection from vulnerabilities on remote device
CIP-005: Electronic Security Perimeter

Diagram showing a network with a workstation connected to an enterprise network through a firewall/UTM. The network includes a VPN tunnel/Remote Desktop, leading to an intermediate system in the DMZ. Critical network protocols are also shown.
Part 2.2 – For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.

- Initiated from outside the ESP using routable protocol
- Only encryption requirement in CIP standards
- Protects Confidentiality and Integrity
- Note that traffic must be decrypted for inspection (Part 1.5)
Part 2.3 – Require multi-factor authentication for all Interactive Remote Access sessions.

- Does not include system to system process communications
- Replaces “strong technical and procedural controls”
- Multi-factor is well know security concept
  - Something you know
  - Something you have
  - Something you are
  - Somewhere you are
- Username is for “identification” not for “authentication”
As processing speeds of CPUs have increased, brute force attacks have become a real threat.

GPGPU cracking, for example, can produce more than 500,000,000 passwords per second, even on lower end gaming hardware.

Depending on the particular software, rainbow tables can be used to crack 14-character alphanumeric passwords in about 160 seconds.

Now purpose-built FPGA cards, like those used by security agencies, offer ten times that performance at a minuscule fraction of GPU power draw.

A password database alone doesn't stand a chance against such methods when it is a real target of interest. *That is the reason for using Multi-factor authentication*
Cybersecurity Implementation example -
- Capacitor Bank Controller

- Follows IEEE 1686 for local **authentication**
- **Intrusion Detection** via a micro-switch mounted on cabinet door
- RADIUS provides centralized **Authentication**, Authorization & Accounting
- IPsec/IKE provides **encryption** of data
IEEE 1686 “IEEE Standard for Intelligent Electronic Devices (IEDs) - Cybersecurity Capabilities”

IEEE-1686 IED Requirements

- Strong password construction
- No undisclosed bypass or “back door”
- Multiple access levels
- Non-modifiable audit trail
- Firmware Control
- Alarm Generation
Local password management (IEEE 1686)

Ability to create User ID/password combination for each user

![Password Change Interface](image)

The following rules are checked as you change the password -
1. Minimum length must be 8 character(s) and maximum length must be 20 character(s).
2. Must have at least one uppercase letter.
3. Must have at least one lower case letter.
4. Must contain at least one number.
5. Must have at least one non-alphanumeric character (e.g., @, %, _, etc.).
Intrusion Detection

- Intrusion detection via a microswitch which detects opening of the enclosure door.
- When the control enclosure door is opened by an intruder, a Report By Exception (RBE) message is sent to SCADA to alert the maintenance personnel.
Role-Based Access (RBA)

John Doe

Define Roles and corresponding permissions
Centralized Authentication, Authorization and Accounting

- Centralized User ID/Password management
  - Stored in server, not in individual IEDs
  - Reduced maintenance effort required
- Only one location needs change rather than changing them at thousands of IEDs
- Remote Authentication Dial-In User Service (RADIUS)
  - Networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use network services
Authentication Mechanism

If RADIUS configured:
Request through PC (GUI) or Front Panel HMI

If RADIUS NOT configured:
Local Authentication server

Primary
Radius Server 1

Secondary
Radius Server 2
Internet Protocol Security (IPSec)
IPSec VPN

Public Internet

Encrypted packets over public network forming a Virtual Private Network

Encrypted Data

Private dedicated Network no need for encryption

Unencrypted Data

Server
Laptop
Gateway 1
Gateway 2
Printer
PC
Data
Workstation A
Workstation B
Ethernet
Bridge
IPSec using Wireless modem

Vulnerability still exists between control and modem

Entire communication path between control and workstation is secured by encryption

IPSec tunnel on Modem ONLY

IPSec tunnel from IED to Gateway
Internet Protocol Security (IPSec)

Benefits of IPSec

- **Confidentiality** - by encrypting data
- **Integrity** - routers at each end of a tunnel calculates the checksum or hash value of the data
- **Authentication** - signatures and certificates
- **IPSec** is designed to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6” - (RFC 2401)

*All these while still maintaining the ability to route through existing IP networks*
Internet Key Exchange

• Given enough time, ANY encryption can be defeated

• For effective protection, IPsec must be deployed with some type of key exchange protocol

• Changing Encryption Key at a regular interval minimizes risk of hacking-
Diffie-Hellman Key Exchange Illustration

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret colours</td>
<td></td>
</tr>
<tr>
<td>Common paint</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td></td>
</tr>
<tr>
<td>=</td>
<td></td>
</tr>
<tr>
<td>Secret colours</td>
<td></td>
</tr>
<tr>
<td>Public transport</td>
<td></td>
</tr>
<tr>
<td>(assume that mixture separation is expensive)</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td></td>
</tr>
<tr>
<td>=</td>
<td></td>
</tr>
<tr>
<td>Common secret</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secret</td>
<td>Public</td>
</tr>
<tr>
<td>$a$</td>
<td>$p, g$</td>
</tr>
<tr>
<td>$a$</td>
<td>$p, g, A$</td>
</tr>
<tr>
<td>$a, s$</td>
<td>$p, g, A, B$</td>
</tr>
</tbody>
</table>

1. Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$.
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \mod p$
   - $A = 5^6 \mod 23 = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \mod p$
   - $B = 5^{15} \mod 23 = 19$
4. Alice computes $s = B^a \mod p$
   - $s = 19^6 \mod 23 = 2$
5. Bob computes $s = A^b \mod p$
   - $s = 8^{15} \mod 23 = 2$
6. Alice and Bob now share a secret (the number 2).
NIST Guide to IPSec VPN

NIST recommendations regarding encryptions, hash functions and key exchanges:

VPN must use FIPS-approved encryption algorithm

- AES-CBC (AES in Cipher Block Chaining mode) with 128-bit key is highly recommended

- Triple DES (3DES-CBC) is also acceptable but DES should not be used as it has been successfully attacked
NIST Guide to IPSec VPN

The Diffie-Hellman (DH) group used to establish secret keying material for IKE and IPSec should be consistent with current security requirements

- DH group 2 (1024-bit MODP) should be used for Triple DES and for AES with 128-bit key
- For greater security,
  - DH group 5 (1536-bit MODP) or
  - DH group 14 (2048-bit MODP) may be used for AES
- Larger DH groups will result in increased processing time
IKE policy settings

Gateway Tunnel Endpoint

Local
- Local Host IP + Mask: 0.0.0.0.0
- Local GW IP: 0.0.0.0.0
- Use Local

Remote
- Remote IP + Mask: 0.0.0.0.0
- Remote GW IP: 0.0.0.0.0

IKE Policy
- Exch. Mode: IKEv2
- IKE Policy: Preshared Key
- Authentication: SHA, SHA 256 Bit, SHA 384 Bit, SHA 512 Bit
- Encryption: Triple DES, AES 128 Bit, AES 192 Bit, AES 256 Bit

DHGroup:
- DH Group 1 (768 Bit)
- DH Group 2 (1024 Bit)
- DH Group 5 (1536 Bit)
- DH Group 14 (2048 Bit)
- DH Group 15 (3072 Bit)
- DH Group 16 (4096 Bit)

Maximum Retries: 3
Time Interval for Retransmission: 10 Sec
IPSec Policy settings

Gateway Tunnel Endpoint

Local
- Local Host IP + Mask: 0.0.0.0
- Local GW IP: 0.0.0.0
- UseLocal

Remote
- Remote IP + Mask: 10.10.3.26
- Remote GW IP: 10.10.3.26

IKE Policy
- Protocol: esp
- Perfect Forward Secrecy

Authentication:
- MD5
- SHA
- SHA 256 Bit (checked)
- SHA 384 Bit
- SHA 512 Bit

Encryption:
- Triple DES
- AES128 bit
- AES192 bit
- AES 256 bit (checked)
Policy Lifetimes

IPsec General Settings

Gateway Tunnel Endpoint

Local
- Local Host IP + Mask: 0.0.0.0.0
- Local GW IP: 0.0.0.0.0
- UseLocal

Remote
- Remote IP + Mask: 10.10.3.26
- Remote GW IP: 10.10.3.26

IKE Policy | IPsec Policy | Policy Lifetimes | Identities

IKE Policy LifeTime (Days:Hrs:Mins): 000:00:00

IPsec Policy Life Time (Days:Hrs:Mins:Sec): 000:01:00:00
## Throughput Performance

<table>
<thead>
<tr>
<th>IPSec mode</th>
<th>64 bytes</th>
<th>128 + 64 bytes</th>
<th>256 + 64 bytes</th>
<th>512 + 64 bytes</th>
<th>768 + 64 bytes</th>
<th>1024 + 64 bytes</th>
<th>1280 + 64 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>no IPSec</td>
<td>min 0.6 ms avg 2 ms</td>
<td>min 0.5 ms avg 1.7 ms</td>
<td>min 0.8 ms avg 2 ms</td>
<td>min 0.7 ms avg 2 ms</td>
<td>min 0.9 ms avg 2.2 ms</td>
<td>min 0.8 ms avg 2.3 ms</td>
<td>min 1 ms avg 2.3 ms</td>
</tr>
<tr>
<td>ESP 3DES HMAC SHA-256</td>
<td>min 2.2 ms avg 3.6 ms</td>
<td>min 2.6 ms avg 4 ms</td>
<td>min 3.2 ms avg 4.9 ms</td>
<td>min 4.8 ms avg 6.3 ms</td>
<td>min 6.4 ms avg 7.9 ms</td>
<td>min 7.7 ms avg 10.9 ms</td>
<td>min 9.2 ms avg 12.6 ms</td>
</tr>
<tr>
<td>ESP AES 128 HMAC SHA-256</td>
<td>min 2.7 ms avg 4.1 ms</td>
<td>min 3.5 ms avg 5 ms</td>
<td>min 4.9 ms avg 6.7 ms</td>
<td>min 8.3 ms avg 11.5 ms</td>
<td>min 11.8 ms avg 15.3 ms</td>
<td>min 15 ms avg 20 ms</td>
<td>min 18 ms avg 24 ms</td>
</tr>
<tr>
<td>ESP AES 256 HMAC SHA-256</td>
<td>min 3 ms avg 4.3 ms</td>
<td>min 4 ms avg 5.9 ms</td>
<td>min 6.2 ms avg 8.3 ms</td>
<td>min 10.8 ms avg 14.3 ms</td>
<td>min 15.3 ms avg 21.2 ms</td>
<td>min 19.8 ms avg 27.1 ms</td>
<td>min 25 ms avg 33 ms</td>
</tr>
</tbody>
</table>
Conclusions

- Modern protection, monitoring and controls in electric power systems with advanced communication are vulnerable to cyber attacks

- IEEE and other standards are available which address Cybersecurity requirements

- It is important to consider applying these standards to IEDs that are being integrated into substations and feeder equipment to provide secure communications

- NERC CIP mandatory standards cover BES and presently does not extend to distribution feeder equipment except for few special cases where a load shedding of 300 MW or more is used by the utility
Conclusions

• In the future, it is expected that NERC and other regulatory bodies (ex: PUCs) will make Cybersecurity standards mandatory in the distribution area.

• Advanced Cybersecurity features such as RADIUS for Authentication, Authorization and Accounting and IPSec VPN tunneling for secure communications via shared network can be embedded into IEDs which will provide secure communication inside substation as well as outside on distribution feeder equipment.