Cyber and Physical Security of Substations in Smart Cities
Self-driving car
Must be programmed to kill?

- Self-driving car

- Why it must be programmed to kill

Smart city Technologies

- Building
- IoT
- Communications (e.g., cloud service)
- Hardware and software
- Power system

Smart City
Transportation Technologies and threats

- **Technologies**
  - V2V and V2I
  - Cloud based communication
  - Connected driving
  - Vehicle platooning

- **Threats**
  - Car hacking
  - Change configuration
  - Sensor jamming attack
  - Change destination


© ABB Group
11/2/2015 | Slide 4
Building Technologies and threats

- **Technologies**
  - Occupancy based energy use
  - IoT connected smart building
  - Connecting to the micro or smart grid
  - Physical security

- **Threats**
  - Control HVAC system
  - Control lighting system
  - Load shedding (outage)

Source: http://www.energymanagertoday.com/
IoT Technologies and threats

- **Technologies**
  - Smart battery (roost)
  - Streetlights with gunshot detection (GE)
  - Wearable devices

- **Threats**
  - Control IoT devices
  - Privacy problem
  - Security key problem
  - Security update
  - Insecure cloud interface

Source: getroost.com, alarm.com, credit suisse
Hardware and software
Technologies and threats

- **Technologies**
  - IoT devices
  - Smart phones
  - Control devices

- **Threats**
  - Superuser
  - Hidden features
  - Backdoor by developers
  - Pre-installed malware
Power system
Physical and cyber attack

↑ Generator room at the Idaho National Laboratory was remote accessed by a hacker and a $1 Million diesel-electric generator destroyed. (U.S. Homeland Security photo)

← Two snipers attacked 17 transformers and 6 circuit breakers. Total of 52,000 gallons of oil spilled and $15.4M in estimated restoration costs.
Power system - substations
Current situation

- Attackers successfully compromised U.S. Department of Energy computer systems more than 159 cyber attacks between 2010 and 2014, a review of federal records obtained by USA TODAY finds.

- Between 2011 and 2014, there were 348 physical attacks and 14 cyber attacks on the grid that caused outrages or disturbances, according to electric utility data reported to the S. Department of Energy.

- In March 2014, the North American Electric Reliability Corporation (NERC) issued Order CIP-014-1 requiring transmission owners to assess the vulnerability of critical substations and develop and implement security plans. Once the vulnerabilities have been identified, the next step is to create a prioritized plan for addressing these vulnerabilities.

- The implementation schedule for this order starts in Oct 2015 and requires completion by August 2016

http://ireport.cnn.com/docs/DOC-1249770
Power system - substations
Are we ready for this?

<table>
<thead>
<tr>
<th>QUICKPOLL</th>
</tr>
</thead>
<tbody>
<tr>
<td>What steps has your utility undertaken to comply with NERC-CIP 14 requirements for physical security?</td>
</tr>
</tbody>
</table>

Poll Results (multiple answers allowed):

- Evaluated potential threats vulnerabilities and consequences: 46%
- Developed physical security plan to address vulnerabilities: 39%
- Engaged an independent third party to review assessments: 30%
- Have not yet completed any initiatives: 35%

Source: How secure is your substation? Physical security (Part I) - 3 strategic elements to protect your assets, ABB
Power system - substations
Worst scenario?

- 4 substations
- 9 transformers
- A coordinated attack to multiple substations?
- No connections to reroute the power?
- Outages and then cascading events?
Power system - substations
Mitigations – physical attack

- Underground cables to disguise location of substation
- GIS to camouflage critical substations
- Resilient bus configuration – more redundancy
- IEC 61850 based substation automation systems
- Physical separation of A & B set protection
- Perimeter fencing (bulletproof walls, cut proof fence, sensors and detection systems)
- Wireless communication for redundancy
- Physical protection of critical assets (bulletproof transformer, circuit breaker and control house)
Power system - substations
Access to data for multiple purposes

Who?
- Control Center Operators
- Protection Engineers
- Technicians

Why?
- Protection
- Control
- Monitoring

Corporate Offices
Power system - substations
Intrusion into a substation network
Power system - substations
Vulnerabilities of substations

- Remote access to substation user interface or IEDs for maintenance purposes
- Unsecured standard protocol, remote controllable IED and unauthorized remote access
- Some IED and user-interface have available web servers and it may provide a remote access for configuration and control with default passwords
- Well coordinated cyber attacks can compromise more than one substation – it may become a multiple, cascaded sequence of events
Power system - substations

Problems?

Confidentiality

Encryption

Requirement

Integrity

Interoperability problem

Authentication

No GOOSE and SMV

Availability

Intrusion detection system

Anomaly detection system

Risk assessment

Vulnerability assessment

Confidentiality

Availability

Integrity

Interoperability problem

Authentication

No GOOSE and SMV

Vulnerability assessment

Risk assessment

Anomaly detection system

Intrusion detection system

Requirement

Encryption
Mitigations – cyber attacks – anomaly detection system

## Power system - substations

Mitigations – cyber attacks – anomaly detection system

### SMMAD Algorithm

1. $\psi^G, \psi^{SV}, V_n^{GS} = 0; // Initialize$
2. capture $C_{pkt}; // Capture all packets in the substation network$
3. if ($C_{pkt}$ is IEC GOOSE);
   4. $G_{cp} = [G_{st}, G_{sq}, G_{ge}, G_{re}]; // Parse packet$
   5. if ($G_{cp}[G_{sm}, G_{dm}] \neq G_{cp-1}[G_{sm}, G_{dm}]); // Find different GOOSE
   6. make $G_{at new}; // Create new anomaly detection thread$
   7. $\alpha_{Th}^G \lor \beta_{s}^G \lor \gamma_{Ti}^G \lor \delta_{d}^G \rightarrow \psi^G; // Calculate GOOSE intrusion$
   8. if ($\psi^G = true$), set $V_n^{GS} = 1; // Detect GOOSE intrusion$
   9. else set $V_n^{GS} = 0; // No intrusion$
10. elseif ($C_{pkt}$ is IEC SMV);
11. $S_{cp} = [S_{mc}, S_{ds}, S_{id}, S_{sm}, S_{dm}]; // Parse packet$
12. $\varepsilon_{Th}^{SV} \lor \theta_{cn}^{SV} \lor \mu_{d}^{SV} \rightarrow \psi^{SV} // Calculate SMV intrusion$
13. if ($\psi^{SV} = true$), set $V_n^{GS} = 1; // Detect SMV intrusion$
14. else set $V_n^{GS} = 0; // No intrusion$
15. return $V_n^{GS}$;

---

Power system - substations
Mitigations – cyber attacks – anomaly detection system

- Detection of temporal anomalies is performed by comparing consecutive row vectors representing a sequence of time instants

\[ V_{h(i)} = \frac{\sum_{j=1}^{n} |\Omega(i,j) - \Omega(i+1,j)|}{n}, \quad i = 1, \ldots, 6, \]

- If a discrepancy exists between two different periods (rows, 10 seconds), the anomaly index is a number between 0 and 1

- A value of 0 implies no discrepancy whereas 1 indicates the maximal discrepancy

Host-based anomaly indicators
- \( \psi^a \) (intrusion attempt on user interface or IED)
- \( \psi^{cf} \) (change of the file system)
- \( \psi^{cs} \) (change of IED critical settings)
- \( \psi^{o} \) (change of status of breakers or transformer taps)
- \( \psi^m \) (measurement difference)

Power system - substations
Mitigations – cyber attacks – anomaly detection system

Attack Start

Attack End

Power system - substations
Mitigations – cyber attacks – anomaly detection system

Power system - substations
Mitigations – cyber attacks – cyber-physical testbed

EMS and DMS
Transmission Level Control Center
EMS & DMS (All/ST şekilde)
LAN (Ethernet Switch)
WAN (Ethernet/IP, IEC 61850)
Distribution Operation Center
DMS HMI (All/ST şekilde)
LAN (Ethernet Switch)
Distribution Operation Testing Simulator (All/STolf)

Substations
Substation
LAN (Ethernet Switch)
Firewall (CISCO)
Engineering Unit
GPS
Firewall (All/STolf)
ICD Server

Distribution System
Restorer Control
Distribution Communication Network
RF Radio
Automatic Restoration Software
AMI MAMIS

Renewable Devices
AMI
Meter Configuration
Meter Simulator
Customers

Research Stations
Transmission System
Distribution System
Substation Automation
Renewable Generation
Smart Meter

HMI: Human Machine Interface
LAN: Local Area Network
WAN: Wide Area Network
RTDS: Real Time Data Simulator
AMI: Advanced Metering Infrastructure
MAMS: Meter Data Management System
PLC: Power Line Communication
FRTU: Feeder Remote Terminal Unit
ICCP: Inter Control Center Communication Protocol
IPS: Intrusion Prevention System

Power system - substations
Mitigations – cyber attacks – coordinated cyber attack detection

References

Projects
[1] Collaborative Research: Resiliency against Coordinated Cyber Attacks on Power Grids, funded by National Science Foundation
[2] Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks (CoDef), funded by Department of Energy (DoE)

Papers
Thank you!

Junho Hong
Scientist
US Corporate Research Center (CRC), ABB Inc
Junho.hong@us.abb.com