SCADA Security

SCADA Network Security
Jodi Jensen
Operations Support Manager
Western Area Power Administration

Substation Network Security
Tyler Stinson
Substation Communications Engineer
Xcel Energy

MRO Webinar 6/29/2017
SCADA Network Security

SCADA Functions
Network Isolation and One-Way Data Flow
Architecture Considerations
SCADA Functions

Control Signals
Telemetry from Field Devices
System Visibility
Network Perimeter Control

- Minimize/Eliminate IP Connections that traverse the SCADA network boundary
- Push data out of the SCADA network using unidirectional gateways and one-way taps
Architecture Considerations

- IP vs. Serial Communications to RTUS
- Pushing SCADA data out through a unidirectional gateway or tap allows:
  - Outgoing ICCP to reside on a separate network
  - State Estimation to reside on a separate network
  - Historian to reside on a separate network
  - View Only ACE Calculation on a separate network
  - View Only SCADA on a separate network
- Push Security, Health, and Configuration Monitoring data out as well
Substation Network Security

Securing Field Networks and Devices
Recent Cyber Security Events

Ukraine 2015
Initiated by spear-phishing emails and was preceded by months of planning and reconnaissance. First successful cyber attack resulting in power outages.

WannaCry/Petya
Ransomware utilizing the EternalBlue exploit and DoublePulsar tool believed to be leaked from the NSA. Spreads through networks via SMB.

Ukraine 2016
Crash Override malware used to cause power outages. Malware is modular, ICS-specific, and can easily be tailored for most SCADA systems.

Cyber attacks are trending towards being more sophisticated and affecting critical infrastructure more than previous attacks.
Substation Network Challenges

- Highest consequence targets
- Large number of field devices, many are older and insecure
- Fewer security tools available
- Insecure protocols
- Growing need for data from substations
Identify

- Identify the operational function and network requirements of substation devices
  Use to isolate non-control devices from control networks (Fault Recorders, Revenue Meters, etc.)

- Define the control network ESP to be small
- Identify privileged access
  Look for ways to make access more granular
Protect

- Secure Device Configuration
  
  Master IP Address. Set DNPIP = 0.0.0.0 to accept requests from any DNP-IP address.

- Expect more from Manufacturers
  Signed firmware updates, additional access and network security

- Protocol Security Options

- Physical switch for remote access
  Control access by using SCADA to enable devices

- One-way hardware for outbound data

  - Port Enable (Y, N)
  - Maximum Access Level (ACC, 2AC)
  - Speed (300 to 38400 bps)
Detect

What tools are available to send alerts when there are changes?

- Device configuration changes
- Abnormal or Increased traffic on networks
- Authentication oddities
- SCADA protocol control alerts

Look for ways to combine data from multiple systems to detect events.
What options do you have to contain issues?

- Network Isolation
  Physically separate control network from other networks
- Limit privileged accounts
  By region, device type, etc.
Respond

What options do you have to respond to an event?

- Set substation to Local mode
- Disconnect local networks
- Apply changes to large number of substations
  .... this could also be a vulnerability