Agency Profile

• Western Area Power Administration (WAPA), a federal agency owns and operates a number of ICS systems in its 15-state geographic footprint including:
  • Energy Management Systems (EMS) and/or Supervisory Control and Data Acquisition (SCADA) systems which are used to monitor/operate transmission infrastructure

• WAPA is one of four Federal Power Marketing Administrations and is located in the western United States

• WAPA is headquartered in Lakewood, Colorado, and has four regional offices, one customer service center, and a Washington D.C. liaison office
Power Marketing Areas

WAPA: Western Area Power Administration
BPA: Bonneville Power Administration
SEPA: Southeastern Power Administration
SWPA: Southwestern Power Administration

Note: Both WAPA and Southwestern market power in Kansas
In FY 2016, WAPA markets power to 700+ customers in 15 states

Products were coordinated from
- 4 power system operations centers
- 4 merchant marketing centers

Federal assets include
- 180+ hydropower units
- Part of the output from AZ coal plant
- 10,500+ MWs of installed capacity

Federal transmission assets include
- 300+ substations
- 17,000+ miles of HV transmission lines

Resulting in $1.4 billion in power and transmission revenues from
- 22.6+ GW-Hrs of net generation
- 3.0+ GW-Hrs of Purchased Power
The Problem Statement

- Industrial Control Systems (ICS) must operate reliably and securely in an ever increasing threat filled environment
- Pre-Internet, ICS were generally standalone systems with proprietary communication protocols
- Post-Internet, many ICS are interconnected and thus have greater exposure to threats (e.g., social media, mobile devices, and from the cloud)
- Since threat vectors constantly change and evolve, ICS owner-operators must be agile in their response to these threats
- What are some methods which could be implemented and deployed to protect an ICS?
Securing Industrial Control Systems

• The National Institute of Standards/Technology (NIST) has outlined an architectural framework to protect ICS networks from cyber security threats

• Segmenting/segregating networks
  • Separating ICS into separate security domains and separating the ICS logically and physically from other networks

• Using boundary protection devices
  • controls the flow of information between security domains and protects against malicious/accidental intrusions

• Using firewalls
  • controls the flow of network traffic between networks using different security protocols

• Implementing Defense-in-Depth Architecture
  • Multi-layered approach which uses overlapping security methods to minimize the impacts associated with the failure of one method

• Training and Education
  • Insider threats, mobile devices, and social engineering are additional concerns
What is Software Defined Networking (SDN)

**Ethernet Switch Today:**
- Control Plane instructs Data Plane “How” to forward packets
- Data Plane forwards packets

**Legacy Networking**

**Software Defined Networking**

Logical separation of the control plane to a centralized control plane.
How SDN Works: Network “White List”

Known and Allowed Traffic

- Ping B from A to B
- The SDN Controller makes a decision:
  1. I know what to do with ping.
  2. Pass it and remember for next time.
- “Working” traffic never leaves the switching fabric.

Unknown / New Traffic

- DNP3 B from A to B
- The SDN Controller makes a decision:
  1. What do I do with DNP3 from A to B?
  2. Pass it and remember for next time.
- “Centralized” decision of what to do with the flow.
How SDN Works: Network “Black List”

**Known and Denied Traffic**

1. FTP B from A to B
2. SDN Controller
3. Switch
4. Not allowed.

"Explicit" deny rule for flow.

**Known, Allowed, and Audited Traffic**

1. FTP B from A to B
2. SDN Controller
3. Switch
4. FTP B from A to B
5. SDN Controller
6. I might copy the packets to a logger, too.
7. I will alert people.

"Audited" traffic for authorized flow.
Using Software Defined Networks (SDN) to Secure Industrial Control Systems

• What will SDN do?
  • Allows the creation of an ICS “cloud”
  • Provides 100% visibility of connected devices & conversations
  • Policies can be triggered based upon operational states

• The software manages communications
  • Solutions are easily modeled
  • The application supports “what if” scenarios/simulations
  • Tool is highly visual and easy to understand/use

• Desired behaviors are defined in the software
• Management is abstracted from hardware
• Facilitates remote management and monitoring
Approaches for Implementing SDN for ICS

• Behavioral Based Industrial Network Simulation System
  • USE CASE 1: Operations Training
    • Utilize pre-built scenarios that are loaded into simulated network to train operations personal.
    • Provide hands on training in ‘live fire’ training system
  • USE CASE 2: Security Test Bed
    • Building and saving of models based upon recorded network traffic
    • Complete industrial network simulation allowing pentesting of simulation system
WAPA using a phased approach for implementing SDN

• Industrial Network Deployment
  • WAPA is segregating its network at our substations through the WAPA’s Security Enclave Support Center concept
    • Creates common/consistent security controls and support model for all WAPA environments
    • Infrastructure is segmented based on criticality and business use
    • Allows one common approach to manage/update Western Information Network deployment across the enterprise
    • Establishes a secure, isolated, and reliable network for WAPA’s Maintenance community
    • Establishes a scalable platform to meet future needs
Summary:

• ICS are moving towards newer network Technologies

• With introduction of new technologies like synchrophasers, data transfer, data security, and data integrity is paramount

• With cyber threats ever increasing, it is important to have a network that can quickly adapt to the desired security posture, to maintain business continuity