Identifying and Managing Network Zones

2013 CIP Workshop, Irving, TX
May 22, 2013

EDMOND ROGERS
ejrogers@illinois.edu
University of Illinois at Urbana-Champaign
Edmond Rogers, CISSP

• Vulnerability assessment background:
  – Penetration testing.
  – Risk assessments.
  – Fuzz-testing certain proprietary protocols.

• Compliance/industry outreach:
  – NERC CIP SME (SERC).
  – Member of CSSWG (NERC).

• Critical infrastructure industry experience:
  – Utility.
  – Banking.
  – Telecom.
TCIPG Statistics

• Builds upon $7.5M NSF TCIP CyberTrust Center, 2005–2010.
• $18.8M over 5 years, starting Oct. 1, 2009.
• Funded by Department of Energy, Office of Electricity and Department of Homeland Security.
• 5 universities:
  – University of Illinois at Urbana-Champaign
  – Washington State University
  – University of California at Davis
  – Dartmouth College
  – Cornell University
• 20 faculty, 20 senior technical staff, 37 graduate students, 5 undergraduate students, and 1 admin.
TCIPG as Catalyst for Accelerating Industry Innovation

- Utilities
- Vendors/Tech Providers

TCIPG

- Pilot Deployment
- Sector Needs
- Data Access to Equipment
- R&D Collaboration
- Solutions Validation and Assessment
- Products Incorporating Solutions
TCIPG Impacts all Aspects of the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity

**Build a Culture of Security**
- Conduct summer schools for industry
- Develop K-12 power/cyber curriculum
- Develop public energy literacy
- Directly interact with industry
- Educate next-generation cyber-power-aware workforce

**Assess and Monitor Risk**
- Analyze security of protocols (e.g., DNP3, Zigbee, ICCP, C12.22)
- Create tools for assessing security of devices, systems, & use cases
- Create integrated scalable cyber/physical modeling infrastructure
- Distribute NetAPT for use by utilities and auditors
- Create fuzzing tools for SCADA protocols

**Protective Measures/Risk Reduction**
- Build secure, real-time, & flexible communication mechanisms for WAMS
- Design secure information layer for V2G
- Provide malicious power system data detection and protection
- Participate in industry-led CEDS projects
- Create fuzzing tools for SCADA protocols

**Manage Incidents**
- Build game-theoretic response and recovery engine
- Develop forensic data analysis to support response
- Create effective intrusion detection approach for AMI
- Participate in industry-led CEDS projects

**Sustain Security Improvements**
- Offer testbed and expertise as a service to industry
- Anticipate/address issues of scale: PKI, data avalanche, PMU data compression
- Act as repository for cyber-security-related power system data
UIUC Smart Grid Testbed
CIP 005 Eye Chart

• Requirement R1 calls for the documentation of an Electronic Security Perimeter (ESP) and the access points to the ESP.

  – R1.1 – “Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).”

  – R1.3 – “Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).”

  – R1.6 – “The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.”
Documentation of ESP

• There are no prescriptive measures on how to document the ESP.

• Auditors maintain that they will advise when they see something that is “wrong.”

• Auditors cannot give advice on what is “right.”

• The utility only finds out it is wrong through the course of their periodic audits.
ESP Documentation

• Many utilities use a combination of statically generated compliance artifacts.
  – Visio-type diagrams.
  – Firewall configurations.

• These documents are sometimes used to define the ESP and security controls surrounding the ESP.
Security Controls

• Security controls called out for in R2 ask that the utility document organizational processes and technical and procedural mechanisms for control of electronic access.

  – R2.1: Deny access by default.

  – R2.2: Only ports and services required for operation are enabled.

  – R2.4: Strong procedural and technical controls for access to the ESP.
Vulnerability Assessment

• The vulnerability assessment requirement of CIP 005 calls for a review of controls.
  – R4.2: “A review to verify that only ports and services required for operations at these access points are enabled.”
  – R4.3: “The discovery of all access points to the Electronic Security Perimeter.”

• The review of ports and services available in a firewall are not easily ascertained without the use of a tool or the expenditure of significant man hours.
The Need for a Tool

• Utilities primarily use firewalls to establish access points to their critical systems.

• Reviewing long and often complex firewall configurations (sometimes exceeding thousands of lines) is time-consuming.

• There is usually no automated method to verify the diagram of the ESP.

• Audits are typically scheduled to last only a matter of days.
The World Today

• Corporate wants data.

• Accessing the data impacts the bottom line.
  – Energy is being traded in different time increments.

• PMU (Phasor Measurement Units).
  – Provide real-time measures (60 times a second).

• Smart grid
  – “The tail that wags the dog.”
Challenges Faced

• Scale
  – Replace the old stuff (not feasible)

• Internet connectivity
  – Email
  – Web usage
  – FTP

• Business lines
  – Real-time data (telemetry)
  – Historical data

• Vendors
Problem: Original View

- Access controlled by configuring potentially many firewalls.
- Subtle errors are common.
Heart of Analysis: Rule Graph

Analysis is based on identifying paths through the "rule graph." Each hop in the path corresponds to "policy implementation."
At the Core: Connectivity Map

Provided:

– A detailed description of the network topology.
– The rulesets for all the firewalls in that topology.
– Description of the global access policies to enforce.

NetAPT discovers every path possible between every pair of subnetworks (including every pair of devices in a specific network of interest) and reports any traffic in violation of the global policies.
At the Core: Connectivity Map

Documentation of all flows that can reach a critical cyber asset are required for CIP-005 compliance.

⇒ Global policies would be “deny access to this list of critical networks.”

⇒ Analysis will report all the traffic allowed to reach these networks.

⇒ Users can visualize and quickly identify the flows that could be potential alleged violations.
Topology Inference

Firewall configurations contain elements of connectivity info.

- **CIDR descriptions of subnetworks facing FW interfaces.**
- “Route” statements.
- VPN descriptions.

NetAPT topology inference engine based on Sandia National Labs ANTFARM tool.

Database-based approach that “grows” knowledge of topology out from the elemental connectivity data.
Topography Inference

Firewall configurations contain elements of connectivity info.

• CIDR descriptions of subnetworks facing FW interfaces.
  • “Route” statements.
  • VPN descriptions.
Topology Inference

Firewall configurations contain elements of connectivity info.

- CIDR descriptions of subnetworks facing FW interfaces.
- "Route" statements.
- VPN descriptions.
Topology Inference

Firewall configurations contain elements of connectivity info.

- CIDR descriptions of subnetworks facing FW interfaces.
- “Route” statements.
- VPN descriptions.
Demo
Analysis

• Analysis can be performed by establishing global policies in the tool.

• Analysis will show all incoming traffic allowed to networks defined in the global policy statement.

• Analysis can also demonstrate sound security controls and conformance to “security best practice.”
Example of an EMS Network
EMS-Specific Traffic Highlighted
Ports and Services

• In addition to highlighting all incoming traffic, NetAPT can also show traffic flows for specific ports.

• Through filtering application flows can be documented.

• The corresponding diagrams can also be used to demonstrate complex network connectivity.
Network Map
ICCP Traffic Highlighted
Annotated Results File

• NetAPT has an annotated results file.

• After analysis is performed, data can be annotated so that it can be easily sorted in a spreadsheet via CSV export.

• All fields from the analysis are imported to a CSV file along with the annotations.
Connectivity Map Saved to CSV File

The CSV file has the following columns:

- **Path #** (index number for the traffic flow)
- **Source**
  - Source firewall
  - Source node (IP address or network)
  - Source port
  - Source group (access group – if used)
- **Destination**
  - Destination firewall
  - Destination node (IP address or network)
  - Destination port
  - Destination group (access group – if used)
- **Service** (user-assigned note field)
- **Note** (second user-assigned note field)
- **Rules** (rule from firewall that created the traffic flow)
- **Policies** (policy match that caused the traffic flow entry)
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path #</td>
<td>Source Firewall</td>
<td>Source Node</td>
<td>Source Port</td>
<td>Source Group</td>
<td>Destination Firewall</td>
<td>Destination Node</td>
<td>Destination Group</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.1.2</td>
<td>172.30.1.2</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.32.1</td>
<td>172.30.32.1</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.67.19</td>
<td>172.30.67.19</td>
<td>any</td>
<td>group:EMS_WAN_RE</td>
</tr>
<tr>
<td>5</td>
<td>4 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.67.3</td>
<td>172.30.67.3</td>
<td>any</td>
<td>group:EMS_CAMPUS</td>
</tr>
<tr>
<td>6</td>
<td>5 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.8.10</td>
<td>172.30.8.10</td>
<td>any</td>
<td>group:CORP</td>
</tr>
<tr>
<td>7</td>
<td>6 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.8.20</td>
<td>172.30.8.20</td>
<td>any</td>
<td>group:CORP</td>
</tr>
<tr>
<td>8</td>
<td>7 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.8.30</td>
<td>172.30.8.30</td>
<td>any</td>
<td>group:CORP</td>
</tr>
<tr>
<td>9</td>
<td>8 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.8.40</td>
<td>172.30.8.40</td>
<td>any</td>
<td>group:CORP</td>
</tr>
<tr>
<td>10</td>
<td>9 CORP-OFFICE</td>
<td>172.30.0.1</td>
<td>any</td>
<td>n/a</td>
<td>172.30.8.50</td>
<td>172.30.8.50</td>
<td>any</td>
<td>group:CORP</td>
</tr>
<tr>
<td>11</td>
<td>PrimaryEMS</td>
<td>172.30.64.10</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>12</td>
<td>PrimaryEMS</td>
<td>172.30.64.11</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>13</td>
<td>PrimaryEMS</td>
<td>172.30.64.20</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>14</td>
<td>PrimaryEMS</td>
<td>172.30.64.30</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>15</td>
<td>PrimaryEMS</td>
<td>172.30.64.40</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>16</td>
<td>PrimaryEMS</td>
<td>172.30.64.50</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>17</td>
<td>PrimaryEMS</td>
<td>172.30.64.60</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>18</td>
<td>PrimaryEMS</td>
<td>172.30.64.70</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>19</td>
<td>PrimaryEMS</td>
<td>172.30.64.80</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>20</td>
<td>PrimaryEMS</td>
<td>172.30.64.90</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>21</td>
<td>PrimaryEMS</td>
<td>172.30.64.11</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>22</td>
<td>PrimaryEMS</td>
<td>172.30.64.12</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>23</td>
<td>PrimaryEMS</td>
<td>172.30.64.13</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>24</td>
<td>PrimaryEMS</td>
<td>172.30.64.14</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
<tr>
<td>25</td>
<td>PrimaryEMS</td>
<td>172.30.64.15</td>
<td>any/tcp</td>
<td>group:EMS</td>
<td>172.30.65.100</td>
<td>172.30.65.100</td>
<td>any/tcp</td>
<td>group:EMS</td>
</tr>
</tbody>
</table>
Filters for Rule sets

• With the tool, ruleset files can be quickly parsed to find areas of concern.

  – Rules with netmasks greater than /24.

  – Rules with “any” for source or destination.

  – Rules with publicly routed (Internet) IP addresses.

  – Deny by default rules.
Demo
Using NetAPT in Assessments

• Allows for complete review of firewall configurations.

• Verifies all access points to the ESP (CIP 005 R2 and CIP 005 R4.3) and provides verification of Electronic Security Perimeter documentation (CIP 005 R1).

• Provides a means to review ports and services allowed to cross access points to the ESP (CIP 005 R2, and CIP 005 R4.3).
Thank You