Cyber Security

- Automation of energy systems provides attack surfaces that previously did not exist
- Cyber attacks have matured from teenage hackers to organized crime to nation states
- Centralized control is vulnerable, decentralized mitigates some of the risk
- NSA multi-layered defense-in-depth architecture is the standard
- Advanced analytics and cyber/physical event correlation provide protection against increasing threats
- Securing communications to end devices (Gens, Switch Gear, etc) -- which may not have intrinsic security -- is critical
- Role level protection at the end device versus traditional user interface roles is a critical capability
- Cyber threats are real and rapidly evolving as are the standards to build and deploy solutions to mitigate them
Cyber Security Concepts Demonstration

Joe McCormick - Boeing
Electric Grid Cybersecurity Risks (NIST)

- Greater communications complexity increases exposure to potential attackers and unintentional errors
- Networks linked to other networks may introduce common vulnerabilities spanning multiple domains
- More interconnections present increased opportunities for legacy and new cybersecurity attacks
- More network nodes means more entry points and vectors that potential adversaries might exploit
- Extensive data gathering and two-way information flows may broaden potential for compromises of data confidentiality and breaches of customer privacy
Distributing Operational Control

- Distributed grid control is necessary to achieve goals of increasing efficiency and resiliency of electric grid.
- Electric grid will become a grid of grids over the next 20 to 30 years with wide distribution of (renewable) energy resources and resulting microgrid technology.
- TCP/IP over multiple media will be the communications platform, replacing proprietary, un-routable protocols over phone lines and low-bandwidth wireless.
- Intelligence will be decentralized within the control, communication, and cybersecurity architectures.
  - Analogues in other areas include avionics, military command and control, and telecommunications.
Defense in Depth Cybersecurity Model

- Model created by US National Security Agency (NSA)
- Balanced “Best Practices” strategy
- NISTIR 7628 guidelines support this model
- Should be integral to Smart Grid deployment platforms
Evolution of Cybersecurity Requirements

**Current:**
- NERC CIP 002-009 applied to Generation and Transmission
- Various input sources including power industry players
- Very basic controls and processes on order of 20

**Over next 2 years:**
- NERC CIP will be applied to Distribution critical assets
- Input sources to NERC CIP will include NIST with NISTIR 7628, which is sourced on various DHS cybersecurity standards with many more controls on order of several hundred

**Beyond**
- Legislation calling for enhanced cybersecurity standards for critical infrastructure, which will require enforcement of cybersecurity over an even larger, more distributed set of controls
Protection at Every Level

Enterprise Network Security (ENS)

Secure Distributed Operational Service Bus (SDOSB)
C2SOS Demonstration

- Demo held in March
- ~20 industry representatives
- Showed how C2SOS can solve challenges facing the grid
  - Equipment failures
  - Intermittent renewables
  - Integration of new technologies
- Confirmed distinctive offering
- Advanced and strengthened technical and business relationships
- Further demos being held in NE and NW

**Smart Grid Live**

**Boeing Enterprise Network Security (ENS)**

Integrated Situational Awareness and Advanced Threat Detection for Securing the Grid

**Robert Esposito, Cyber Security Solutions Architect**
Agenda

- The Threat Lifecycle
  - Zero Day Advanced Threats

- What is Boeing ENS?
  - Behavioral Detection vs. Signature Detection
  - Boeing ENS Capability Details

- Workflow Discussion

- Live Demo
  - Intrusion Attempt Incident Response
The Threat Lifecycle

- **Reconnaissance**
  - Priority 3 – Blue

- **Intrusion / Penetration**
  - Priority 5 – Yellow

- **Communication Beacons**
  - Priority 7 & 8 – Orange

- **Suspicious Flows / Exfiltration**
  - Priority 9 & 10 – Red
Boeing Enterprise Network Security (ENS)

- Self Contained & Passive Advanced Malware Detection
- Integrated Non-Signature Based Detection Approach
  - Advanced Anomaly Based Detection
  - Advanced Malware Detection
  - Real-Time Network Forensics
  - Correlation and Workflow Enabling Accurate Detection
- Integrates best of Industry capabilities into one unit
- Safe and Secure Detection
  - ½ Rack, 14U Portable Pelican Case
  - Sanitization of Data Prior to Removal
- Detect APTs at the earliest phases
Features

- Prioritize alerts and present to the Network Analyst
- Correlate alerts from sensor components through the implementation of customized rule sets
- Case Management system for the aggregation of events & external data into individual cases that may then be presented to any audience

Benefits

- Single system for access by Network Analyst with custom dashboards to identify the severity of potential advanced threats
- Integrated drill down into individual components serving as the single point of entry for the Network Analyst
Anomaly Analytics

**Features**

- Up to 10 Gigabit/sec throughput
- Behavioral based anomaly detection
- Traffic inspection supporting full layer 7 extensible analysis
- Entropy based statistical algorithms to identify advanced threat behaviors

**Benefits**

- Ability to identify advanced threats in early reconnaissance - Phase 1
- Ability to identify advanced threats in communications establishment - Phase 3
- Ability to identify advanced threats in data exfiltration - Phase 4
Malware Detection System

**Features**

- 1Gigabit/Sec throughput of analyzed web traffic
- Early detection of malicious activity through fingerprinting of malicious communications before the affects are actually seen in the network
- Proprietary virtual machine mechanism to avoid advanced malware detection
- Evaluated to EAL-2

**Benefits**

- Locate malware as it enters the network before a system is infected.
- See potential intrusions that are blocked by existing systems or patches.
- Identify advanced threats across Phases 2 - 4
Network Forensics

Features

- 2Gigabit/Second throughput scalable to larger installations
- Full packet classification and storage to include non-standard packet formats for meta-data querying
- Seamless session retrieval and reconstruction and rendering to support case management and archiving
- Intuitive visualization environment to identify additional stored documents leaving the network

Benefits

- Provides the Network Security Analyst with the tools to research the affects of Advanced Persistent Threat.
- Arms the Network Security Analyst with context in tailoring existing countermeasures to respond to attacks.
Boeing ENS: Non-Intrusive & Passive Monitoring

Traffic Feeds
- Internet
- Monitor inside or outside firewall

ENS System Data
- Data Access Switch (Eigerman)
- Traffic Anomaly Analytics (Narus)
- Malicious Intrusion Detection (FireEye)
- Malware C&C Detection (Narus & FireEye)
- Network Forensics (Solera)

ENS Network Analytics
- Security Info and Event Management
  - Operator Console
  - Event Report and Log
  - Instant Device Web Portal Accessibility
  - Primary Portal (ArcSight)

ENS Dynamic Analytics
- Threat Analysis
  - Advanced Analysis
  - Forensics
  - SME Collaboration (ArcSight & Other)
- Visualization
  - Sit Awareness
  - Role Based (ArcSight & Other)

Network Security Operator
Network Security Analyst

Copyright © 2011 Boeing. All rights reserved.
Discovered Phase 1 Activity Reconnaissance

(Blue – Priority 3 & 4)
Example Phase 1 Event Pattern
Discovered Phase 2 Activity Intrusion Attempt

(Yellow – Priority 5 & 6)
Phase 2 Intrusion Attempt Behaviors Observed

Malicious Capabilities Observed in the VM

- **Data Theft:** Yes
  - Keystroke logging observed

- **Malicious Behavior:** Yes
  - Startup behavior anomalies observed
  - Cryptographic operations performed
  - Running processes listed
  - Malware trying to detect the presence of a debugger
  - Critical error message boxes hidden
  - Tracking Sleep/SleepEx API Call

**OS Change Summary**

<table>
<thead>
<tr>
<th>Type</th>
<th>Files</th>
<th>Registry Keys</th>
<th>Network</th>
<th>Access Control Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count</td>
<td>8</td>
<td>130</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

Malware Binary: 06/25/12 05:58:49
Discovered Phase 3 Activity Outbound Suspicious Communications

(Orange – Priority 7 & 8)
### Malware Report

<table>
<thead>
<tr>
<th>Malware</th>
<th>Events</th>
<th>Sources</th>
<th>Targets</th>
<th>First Event (UTC)</th>
<th>Last Event (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan.Generic.DNS</td>
<td>594</td>
<td>14</td>
<td>1</td>
<td>04/24/12 14:08:10</td>
<td>05/07/12 14:14:51</td>
</tr>
<tr>
<td>Bot.Mariposa.DNS</td>
<td>1437</td>
<td>4</td>
<td>1</td>
<td>04/24/12 14:02:14</td>
<td>05/06/12 02:25:26</td>
</tr>
<tr>
<td>Trojan.TDServ.DNS</td>
<td>121</td>
<td>4</td>
<td>1</td>
<td>04/24/12 14:20:05</td>
<td>05/05/12 15:21:52</td>
</tr>
<tr>
<td>Trojan.Vobfus.DNS</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>05/04/12 14:34:38</td>
<td>05/04/12 14:34:38</td>
</tr>
<tr>
<td>InfoStealer.Banker.Zbot.DNS</td>
<td>247</td>
<td>4</td>
<td>1</td>
<td>04/24/12 14:10:28</td>
<td>05/03/12 20:42:25</td>
</tr>
<tr>
<td>Bot.Rustock.D.DNS</td>
<td>39</td>
<td>2</td>
<td>1</td>
<td>04/24/12 14:15:14</td>
<td>05/03/12 14:08:22</td>
</tr>
<tr>
<td>Trojan.FakeAlert.DNS</td>
<td>115</td>
<td>3</td>
<td>1</td>
<td>04/24/12 14:10:21</td>
<td>05/03/12 14:06:55</td>
</tr>
<tr>
<td>Rogue.FakeAV.DNS</td>
<td>309</td>
<td>3</td>
<td>1</td>
<td>04/24/12 14:03:01</td>
<td>05/03/12 13:22:53</td>
</tr>
<tr>
<td>Trojan.Gen.D.DNS</td>
<td>161</td>
<td>3</td>
<td>1</td>
<td>04/24/12 14:25:14</td>
<td>05/03/12 12:29:54</td>
</tr>
<tr>
<td>Trojan.Krap.DNS</td>
<td>115</td>
<td>3</td>
<td>1</td>
<td>04/24/12 14:49:34</td>
<td>05/03/12 12:00:26</td>
</tr>
<tr>
<td>Trojan.Renos.DNS</td>
<td>38</td>
<td>2</td>
<td>1</td>
<td>04/24/12 14:47:36</td>
<td>05/03/12 11:39:27</td>
</tr>
<tr>
<td>Trojan.TDSS_TDL.DNS</td>
<td>149</td>
<td>2</td>
<td>1</td>
<td>04/24/12 14:07:11</td>
<td>05/03/12 10:28:37</td>
</tr>
<tr>
<td>Trojan.Flipper.2.DNS</td>
<td>76</td>
<td>2</td>
<td>1</td>
<td>04/24/12 14:40:42</td>
<td>05/03/12 09:43:56</td>
</tr>
<tr>
<td>Trojan.Downloader.Bredolab.DNS</td>
<td>38</td>
<td>2</td>
<td>1</td>
<td>04/24/12 14:04:42</td>
<td>05/03/12 08:55:54</td>
</tr>
<tr>
<td>Bot.Monkif.DNS</td>
<td>36</td>
<td>2</td>
<td>1</td>
<td>04/24/12 22:26:47</td>
<td>05/03/12 08:25:24</td>
</tr>
<tr>
<td>Bot.Koobface.DNS</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>04/25/12 11:08:55</td>
<td>05/02/12 22:25:15</td>
</tr>
<tr>
<td>Suspect.W32.AdInstall.PBCXP</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>05/01/12 13:05:24</td>
<td>05/01/12 13:08:14</td>
</tr>
<tr>
<td>InfoStealer.Banker.SpyEye.DNS</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>04/29/12 15:51:23</td>
<td>04/30/12 20:27:58</td>
</tr>
<tr>
<td>Exploit.ToolKit.BlackHole</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>04/24/12 19:56:08</td>
<td>04/24/12 19:55:08</td>
</tr>
</tbody>
</table>
Discovered Phase 4 Activity Suspicious Data in Motion

(Red – Priority 9 & 10)
Very little traffic to foreign countries is suspicious

Most of the traffic is from United States
Legacy WWW Server Discovered

Very little traffic to foreign countries is suspicious

Most of the traffic is from United States
Workflow Provides Efficient Operations

Discovery

What’s the priority?
• Higher priority alerts have the greatest business impact

Analysis

What is it?
• Detailed Forensics

Case Creation

What are the details?
• Ticket Type & ID
• Stage
• Frequency
• Operational Impact
• Security Classification
• Consequence Severity

Case Management

• Initial
• Follow-up
• Final

• Research notes, attachments, PCAPs
• Ownership Tracking

Course of Action

• Block/Shutdown, monitor, other

Protection & Case Resolution

• Closed

Detailed metrics available
• Time to resolution
• Analysts involved, etc
Boeing ENS Live Demo – Phase 2 Intrusion Attempt Incident Response

- Security Operations Center Analyst Investigates Phase 2 Intrusion Attempt
- Further Incident Details Gathered
- Case Created with Integrated Case Management System
- Case Assigned to Incident Response Team (CERT)
Boeing Operations Service Bus Architecture

NIST Smart Grid Priority Areas

Enterprise Network

Data Center

Enterprise Service Bus

Distribution Management

Advanced Meter

Electric Transportation

Electrical Storage

Demand Response

Wide Area SA

advanced cyber security protection

Operations Network

Operations Center

Substation

Substation
Secure Distributed Operations Service Bus

Distributed service bus provides secure two-way communications

• Designed for tactical / field environments
• Architecture provides plug-n-play modularity at application, sub-system, and device level
• Information assurance designed-in
  • Protected transport
  • Role-based access control at application and transaction levels
• Distributed security agents
• Network Performance Management - Bandwidth and Quality of Service Management
• No central hub – eliminates scalability and vulnerability issues
Protected Transport Unencrypted/encrypted
Role Based Access Control (RBAC)

- Occur at the application layer in a communications protocol stack
- Provides higher level of access control than the application provides for allowing legacy applications to be supported

Three Cases
- Unauthorized User trying to authenticate onto the system to execute a command
- Authorized User trying to execute an unauthorized command
- Authorized User trying to execute an authorized command
RBAC: Unauthorized User Attempting Access
RBAC: Authorized User Attempting to Execute an Unauthorized Command

Activate role that does not belong to user

Activate correct role

Access interface that does not belong to user/role
RBAC: Authorized User Successfully Authenticating and Executing a Command

C:\\Documents and Settings\\b1040472\\ echo \%USERNAME\%
C:\\Documents and Settings\\b1040472\\cd c:\tmp\testapp
C:\\tmp\testapp\\scRoleMgr -A
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsSafetyTextLog1.6172
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsTextLog1.6172
No Active Roles Found.
C:\\tmp\testapp\\scRoleMgr -I
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsSafetyTextLog1.4844
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsTextLog1.4844
Inactive Roles:
  TEST-ROLE
  TEST-ROLE-EMPTY
C:\\tmp\testapp\\scRoleMgr -a TEST-ROLE
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsSafetyTextLog1.6648
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsTextLog1.6648
Role activated.
C:\\tmp\testapp\\scRoleMgr -A
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsSafetyTextLog1.3140
Text Logging started Successfully to C:\TEMP\\2012-09-20.scRoleMgr.CommsTextLog1.3140
Active Roles:
  TEST-ROLE
C:\\tmp\testapp\\SimpleRMIClient.exe
Text Logging started Successfully to C:\TEMP\\2012-09-20.SimpleRMIObjectCommsTextLog1.936
Running app - press ctrl-c to exit
RMI getCommand [IServer;echo:Init Message]
OMI setString [This message is from simpleRMIObject: 0]
Questions?