Best Practices in Cybersecurity

Matthew E. Luallen
m@cybati.org
Define security ...

• What does security mean for Critical Infrastructure and Key Resources (CI/KR)?
  – Protection of authentic and accountable control
  – Assurance of information integrity
  – Timeliness of transmission and receipt of data
  – Confidentiality and classification of information

• Exact definition depends upon specific CI/KR; Always ask / define!
... with two default assumptions ...

- Anyone can listen to your conversations
  - It is not acceptable for any unauthorized person or system to affect the confidentiality, integrity or availability of communications of valued assets.

- Anyone can steal or misuse your assets
  - Any asset loss or misuse must be protected so that there is reduced loss of confidentiality, integrity or availability of the valued asset or NO further compromise of other assets.

- Therefore, the environment is contested territory and it is up to you to protect it
... while our Trusts are broken ...

- The past two years have seen **certificate authorities** compromised, including Verisign, Comodo, DigiCert, DigiNotar, and Gemnet.

- The DuQu worm directly exposed a vulnerability in **ClearType/TrueType fonts** impacting Microsoft Windows, which later was understood to also impact Apple Macs, iPhones, iPads, and other operating systems.

- ZTE Android operating system phones use **software encoded usernames and passwords**.

- RuggedCom, Garretcom, Schneider Electric, Siemens and others use **software encoded usernames and passwords**
What does security mean for Critical Infrastructure and Key Resources (CI/KR)?

- Protection of authentic and accountable control
- Assurance of information integrity
- Timeliness of transmission and receipt of data
- Confidentiality and classification of information

Exact definition depends upon specific CI/KR; Always ask / define!

Monitoring and Response

Too many definitions. What is yours?
• Control Systems are inherently difficult to secure due to their wide attack surface and geographic area
### Attack Vectors (1 of 2)

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>Skillset/Tools Necessary to Develop</th>
<th>Time to Develop</th>
</tr>
</thead>
</table>
| Man-in-the-Middle attack sending false commands to the PLC or operator’s workstations | - Ettercap/etterfilter scripting  
- Communications protocol analysis  
- Protocol reference manuals (e.g., vendor documentation or third-party software) | 3 days (validated) |
| USB Mouse with Teensyduino and scripted HMI control                          | - Arduino and VBScript programming  
- Soldering skills  
- HMI and control system protocol skills | 1 week (validated) |
| Denial of Service of control system components (devices and communication channels) | - Moderately skilled cybersecurity college student  
- PLC administration software  
- Command line networking skills | 1 day (validated) |

- Metasploit Module faulting MicroLogix controller (FTE NetDecoder, simple programming, 2 hours)
- Teensyduino PLC Technician Cable (3 days, 3 cables)
Attack Vectors (2 of 2)
Small-Scale Environment Analysis and Penetration

• Traffic Lights
  – Review the physical design (sensors and actuators)
  – Analyze the operating logic
  – Using cyber means, attempt to create an all green intersection

• Railroad
  – Review the physical design (sensors and actuators)
  – Analyze the operating logic
  – Using cyber means, attempt to derail the train
How do you sense, understand and act upon the change?

• Sense
  – Smell
  – Sight
  – Sound
  – Touch
  – Taste

  – CYBER

• Understand
  – Analyze
  – Process
  – Knowledge

• Act
  – Respond based upon current senses
  – Perform additional sensing based on feedback (Proportional Derivative Integral [PID] Control)
How does a PLC/PAC sense, understand and act upon change?

Processor

Toggle On/Off
Toggle 1
Toggle 2
Button 1
Button 2
Toggle 3

VAC VDC

Motor
Green
Yellow
Red
White

Copyright 2011-2012 – CYBATI/cybati.org
Workforce Productivity leads to Profitability

Productivity is due to automation using energy

• 427:1 versus 5:1*, this is today's technology-based society income gap versus the farm-based society income gap in the US of only 100 years ago.”

*Ratio is from "Decoding the Future with Genomics" - Juan Enriquez, [www.ted.com](http://www.ted.com) and bar charts are from the US Bureau of Labor Statistics [www.bls.gov/lpc/prodybar.htm](http://www.bls.gov/lpc/prodybar.htm)
Cyber Relationship

- 427:1 to 5:1
- 85 times the productivity of farm based societies
- We operate as a country of 25 billion people
  - 300 million real people
  - 24.7 billion virtual people

- The virtual people use electrons to store and process the bits of information
  - No conscious
  - Can be easily socially engineered if access is not restricted – this is cybersecurity
Limit Trust

• We are not designing to limit trust, we are doing just the opposite
  – Outsourced personnel managed by external resources in varied geo-political zones
    • Contractors hiring contractors hiring contractors managed by?
  – Data wirelessly communicated accessible to external COTS resources in varied geo-political zones
    • GPS, 802.11, Zigbee, GPRS, Operations, iPads
  – Virtualized resources migrating into clouds managed by external resources in varied geo-political zones
    • gotomyhmi.com and cloud service providers
  – Standardized hardware and software manufactured by external resources in varied geo-political zones
Best Practices

• Know Yourself, Your Trusts and Monitor and Respond to Them
  – Hardware
  – Software
  – Communications
  – Personnel

• We need cyber / skilled professionals to invent, procure, architect, build, maintain, operate and decommission industrial automation systems
Recently Accepted Conference Paper

• HICSS 46, January 2013

• Developing a Critical Infrastructure and Control System Cybersecurity Curriculum

• Identifies student projects, successes, failures and path forward