ICS, SCADA, IIoT and Cybersecurity

Presenter Information

- Gordon W Skelton, PhD, CISSP, CISA, CEH, CRISC, Security+
- President, Security and Analytics, LLC, Ridgeland, MS
- Senior Member IEEE
- Member ISC(2), ASIS, ISA, ISIS, NCMS (The Society of Industrial Security Professionals)
- Research in cybersecurity as applied to Enterprise Networks and Industrial Control Systems

Important Definitions

- SCADA – Supervisory Control and Data Acquisition
- ICS – Industrial Control System
- PLC – Programmable Logic Controller
- IoT – Internet of Things
- IIoT – Industrial Internet of Things

Why are we concerned?

- Changes to the industrial integration of enterprise networks (IT) and operating networks (OT)
- The “Shopfloor” is no longer isolated or “air gapped”
- Employing ethernet protocols in place of commonly used protocols
- Desire to incorporate data from manufacturing, production in decision-making, the use of “Big Data” for production analysis

Common Components

Programmable Logic Controller (PLC)	Remote Terminal Unit (RTU)
Human Machine Interface (HMI)	Control Server
Master Terminal Unit (MTU)	Intelligent Electronic Device (IED)
Data Historian	Engineering Workstation
Sensors	Actuators
Switches / Hubs	Firewalls

Communications Protocols

- PROFINET – Process Field Net
- EtherNet/IP
- Common Industrial protocol (CIP)
- Ethernet
- Modbus and Modbus TCP/IP
- DNP3
- Common IT Protocols found in ICS – HTTP, FTP, Telnet, ARP, ICMP

Profibus

PowerLink Ethernet

EtherCAT

Weaknesses of Communication Protocols

- No inherent security measures
- If using Ethernet, then traditional security issues exist – packet capture, injection of malicious attacks
- Identity theft
- Modification of messages
- Re-injection of traffic
- Eavesdropping, use of taps

Issues Surrounding Cybersecurity and ICS Protection

- Routine patching of operating systems is uncommon
- Limited memory and processing capabilities on PLCs
- Many of the communication protocols are hackable, containing inherent vulnerabilities
- Changes to programs – Ladder Programs – can be loaded directly to a PLC
- Lack of adequate training for technicians and engineering staff on cybersecurity

Types of Threats

Replay attack on SCADA – data is captured from normal operations and replayed while attack is occurring thus preventing monitoring staff from being alerted by alarms

Malware on enterprise network is able to access OT network and ICS through integrated networks (IT / OT) – Stuxnet Virus

Botnet of IoT

- Mirai botnet attack – created by a group of teens used various unsecured Internet cameras to create a botnet

Examining Your Own Systems

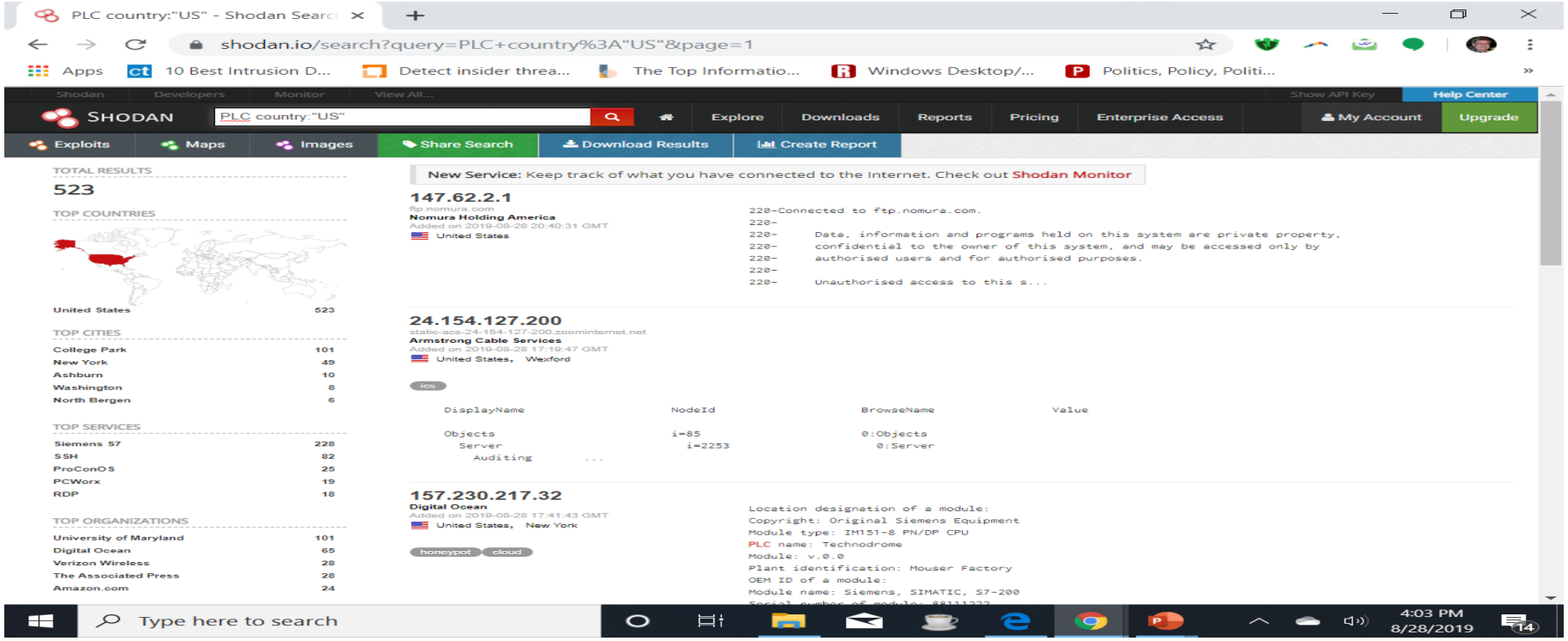
- Using Shodan https://www.shodan.io

or

- Censys.io https://www.censys.io

you can see if any of your industrial devices are available to individuals browsing the Internet

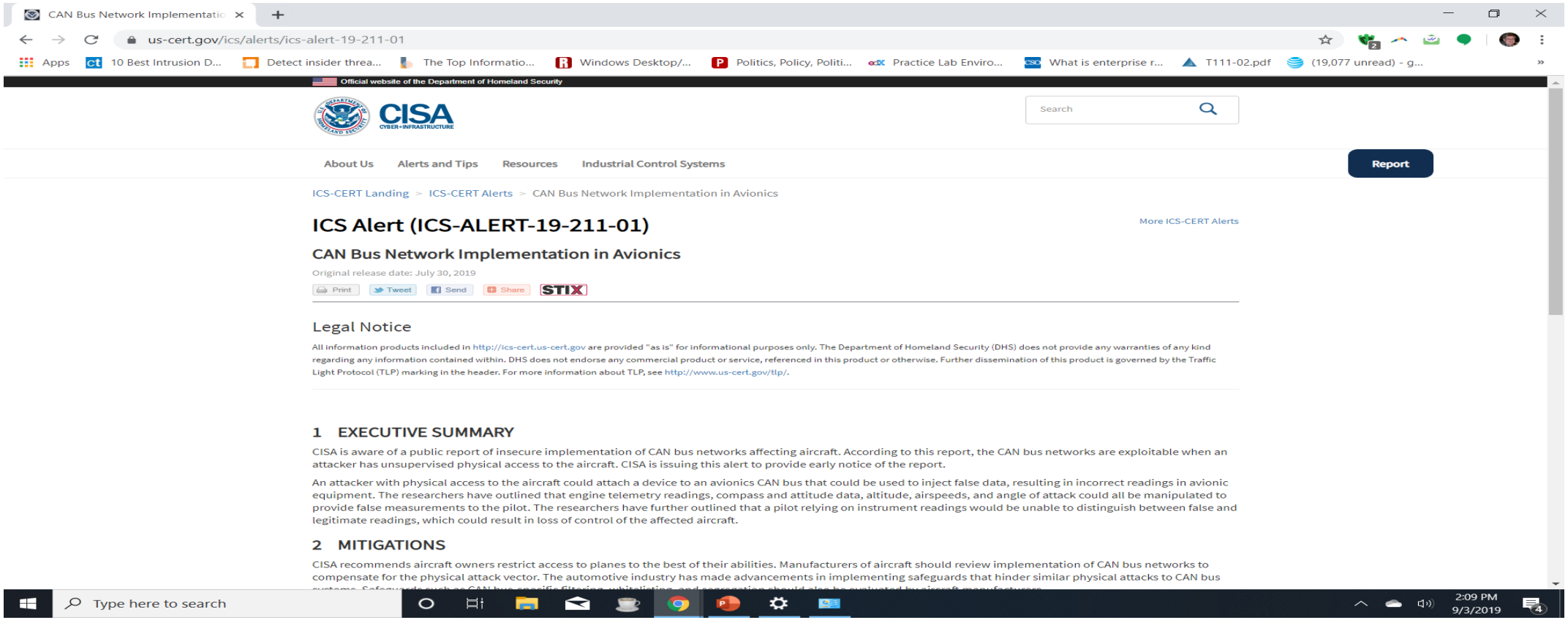
SHODAN Example



Key Vulnerability Reference Sites

- Industrial Control Systems: Alerts, Advisories, Reports - https://www.us-cert.gov/ics Site used to report discovered vulnerabilities and aids in their mitigation
- Industrial Control Systems Cyber Emergency Response Team – https://isc-cert.us-cert.gov
- Industrial Control Systems Information Sharing and Analysis – http://isc-isac.org
- SCADAhacker.com – https://scadahacker.com/library

Example from CERT-ICS



Helpful Reference Sites for ICS Security Concerns

- https://www.trendmicro.com/us/iot-security/
- https://scadahacker.com/resources.html
- https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

Kali Linux and Metasploit

- Kali Linux is a specialized version of Linux that contains various tools for scanning and vulnerability assessment
- Metasploit is included in Kali Linux and is used to select various exploits and scripts which are associated with various weaknesses and vulnerabilities within computer systems
- There are a number of different exploits that are related to SCADA & ICS

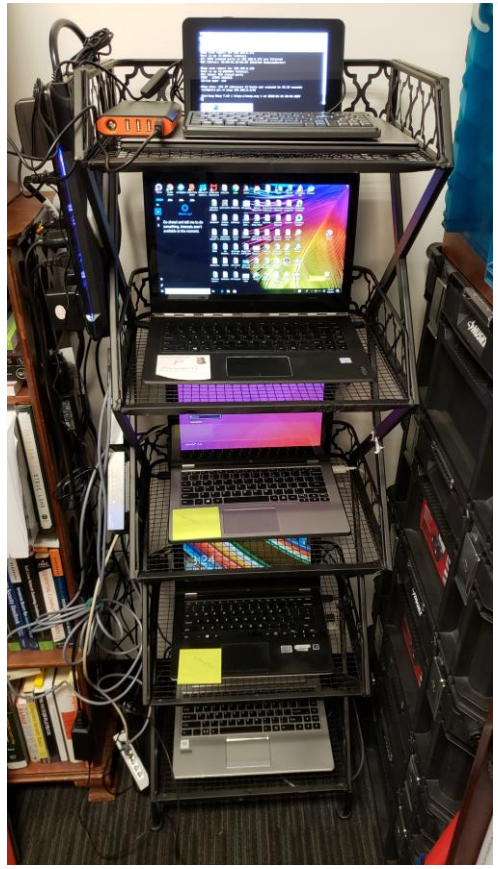
Hacking and Industrial Communications

- Each of the different communication protocols used in ICS has a known vulnerability
- Available on the web are numerous examples of how one can sniff these networks
- Remember, hackers don’t worry about crashing a system where as ethical hacker do

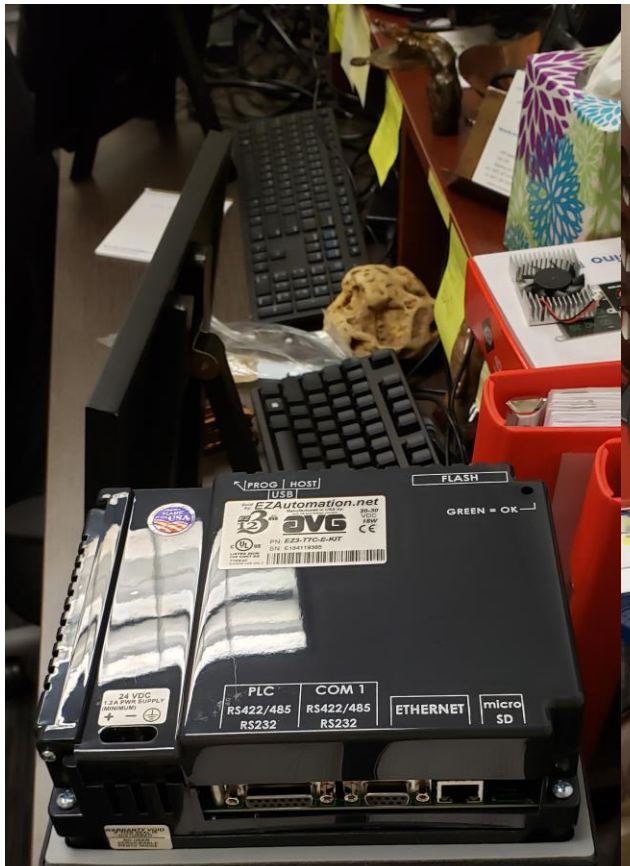
Testing / Experimentation Lab

- Lab contains both IT and OT components
- Closed network running Kali Linux, Windows 7, Ubuntu, Metasploitable,
- Integrated PLCs, SCADA, HMI, and other industrial components
- PLCs open to access and reprogramming for insider threats

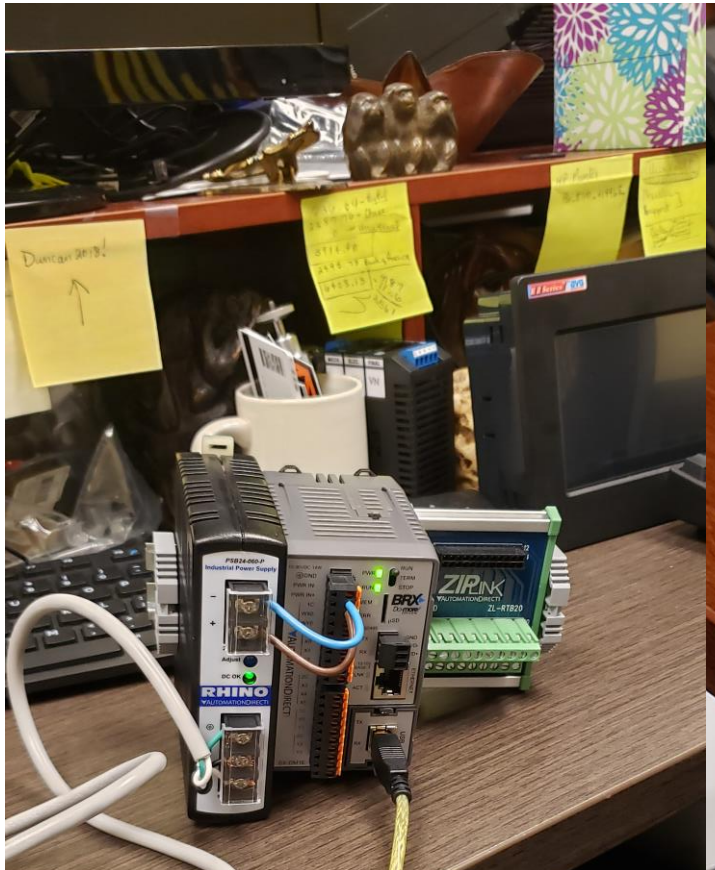
Testing / Experimentation Lab
Kali Linux & IT Equipment



Testing / Experimentation Lab
IDC / SCADA Equipment



Testing / Experimentation Lab
IDC / SCADA Equipment



Standards and Frameworks

Framework	Regulated	Non-Regulated	Related Industry
AWWA		X	Water/Waste-Water
ISA/IEC 62443		X	Non-Industry Specific
NEI 08-09	X		Nuclear Power
NERC CIP	X		Electric Utility
NIST SP800-82		X	Non-Industry Specific
NIST Framework for Improving Critical Infrastructure Security		X	Non-Industry Specific
NISTIR 8183 - Cybersecurity Framework Manufacturing Profile		X	Manufacturing
NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1		X	Critical Infrastructure

Examples of Non-traditional Systems That Can Benefit from a Cybersecurity Framework

- Advanced Metering Infrastructure
- Building Automation
- CCTV Surveillance Systems
- Digital Signage
- Electronic Security Systems
- Energy Management Systems
- Fire Alarm Systems
- Intrusion Detection Systems
- Public Safety / Land Mobile Radios
- There are many different systems that can benefit from NIST 800-52 rev. 2

Current Status of IoT Security Legislation Senate Bill 734 & House Bill 1668

- General Bill that originally included PLCs as “general-purpose computing devices”
- Changes to H.R. 1668 have exempted them; however, that is a concern because of the increase connectivity of OT to IT and thereby, indirectly to the Internet
- Primary purpose of the bills is “To leverage Federal Government procurement power to encourage increase cybersecurity for Internet of Things devices, and for other purposes.”
- There are, however, exemptions that allow a Federal agency to still select insecure devices as long as they are need for national security or research.
- The topic of IToT is not addressed directly in the legislation.

References

- incibe, “Protocols and network security in ICS infrastructures, “ Spanish National Cybersecurity Institute, May, 2015.
- NIST, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-92, Revision 2, May 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- Pascal Ackerman, Industrial Cybersecurity, Packt>, 2017.
- Sravani Bhattacharjee, Practical Industrial Internet of Things Security, Packt>, 2018.

References, Cont'd

- Steve Mackay, Edwin Wright, John Parm Deon Reynders, Practical Industrial Data Networks: Design, Installation and Troubleshooting, IDC Technologies, Elsevier Ltd., 2004.
- Lawrence M. Thompson, Tim Shaw, Industrial Data Communication, 5th Ed., International Society of Automation, 2016
- Trendmicro https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system
- Ronald L . Krutz, Industrial Automation and Control System Security Principles, 2nd Ed., ISA, 2017.

Questions & Answers & Notes

- The slides are available on my corporate website – www.securityandanalytics.com
- Continued research will be posted on that site
- Contact me @ gwskelton@securityandanalytics.com / 601.427.4760
- Business cards are available for all interested