



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

The screenshot shows a web browser window displaying the Shodan search results for the query "PLC country:US". The browser's address bar shows the URL "shodan.io/search?query=PLC+country%3A%22US%22&page=1". The Shodan interface includes a search bar with the query, navigation tabs like "Exploits", "Maps", and "Images", and a top navigation bar with "SHODAN" and "PLC country:US".

TOTAL RESULTS
523

TOP COUNTRIES

United States	523
---------------	-----

TOP CITIES

College Park	101
New York	49
Ashburn	10
Washington	8
North Bergen	6

TOP SERVICES

Siemens S7	228
SSH	82
ProConOS	25
PCWorx	19
RDP	18

TOP ORGANIZATIONS

University of Maryland	101
Digital Ocean	65
Verizon Wireless	28
The Associated Press	28
Amazon.com	24

147.62.2.1
Ip.nomura.com
Nomura Holding America
Added on 2019-08-28 20:40:31 GMT
United States

```
220-Connected to ftp.nomura.com.
220-
220- Data, information and programs held on this system are private property,
220- confidential to the owner of this system, and may be accessed only by
220- authorized users and for authorized purposes.
220-
220- Unauthorised access to this s...
```

24.154.127.200
static-24-154-127-200-oominternet.net
Armstrong Cable Services
Added on 2019-08-28 17:19:47 GMT
United States, Wexford

DisplayName	NodeId	BrowseName	Value
Objects	i=85	0:Objects	
Server	i=2253	0:Server	
Auditing	...		

157.230.217.32
Digital Ocean
Added on 2019-08-28 17:41:43 GMT
United States, New York

```
Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: Technodrome
Module: v.0.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number: 6ES7 311-1CG02-0AB0
```

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

Official website of the Department of Homeland Security

CISA
CYBER-INFRASTRUCTURE

Search

About Us Alerts and Tips Resources Industrial Control Systems **Report**

ICS-CERT Landing > ICS-CERT Alerts > CAN Bus Network Implementation in Avionics

ICS Alert (ICS-ALERT-19-211-01) [More ICS-CERT Alerts](#)

CAN Bus Network Implementation in Avionics

Original release date: July 30, 2019

Print Tweet Send Share **STIX**

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

1 EXECUTIVE SUMMARY

CISA is aware of a public report of insecure implementation of CAN bus networks affecting aircraft. According to this report, the CAN bus networks are exploitable when an attacker has unsupervised physical access to the aircraft. CISA is issuing this alert to provide early notice of the report.

An attacker with physical access to the aircraft could attach a device to an avionics CAN bus that could be used to inject false data, resulting in incorrect readings in avionic equipment. The researchers have outlined that engine telemetry readings, compass and attitude data, altitude, airspeeds, and angle of attack could all be manipulated to provide false measurements to the pilot. The researchers have further outlined that a pilot relying on instrument readings would be unable to distinguish between false and legitimate readings, which could result in loss of control of the affected aircraft.

2 MITIGATIONS

CISA recommends aircraft owners restrict access to planes to the best of their abilities. Manufacturers of aircraft should review implementation of CAN bus networks to compensate for the physical attack vector. The automotive industry has made advancements in implementing safeguards that hinder similar physical attacks to CAN bus systems. Safeguards such as CAN bus cryptographic authentication and integrity protection could be implemented by the automotive industry to protect against physical attacks.

2:09 PM 9/3/2019

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

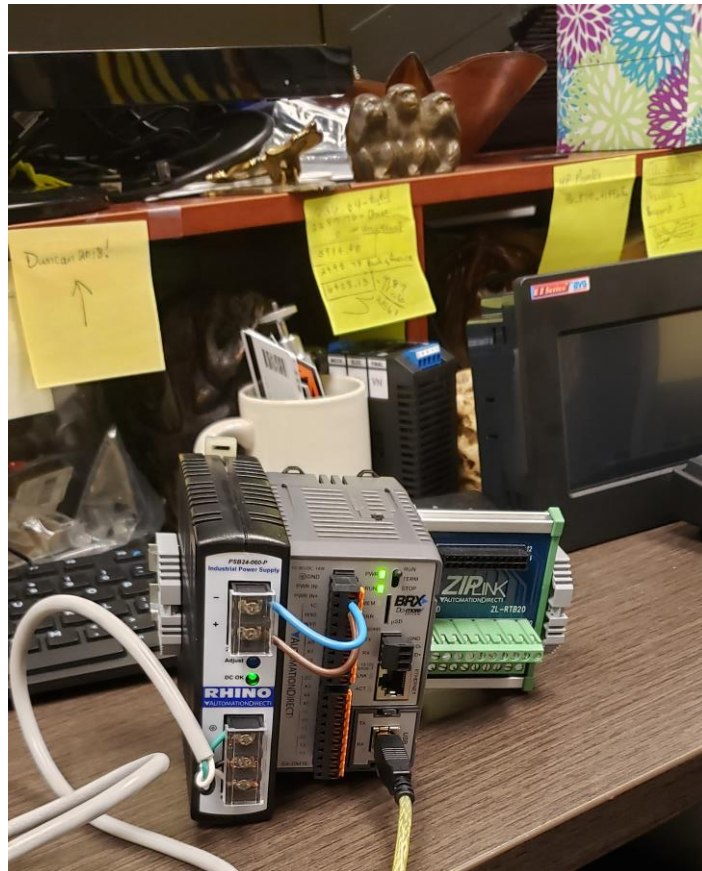
Kali Linux & IT Equipment



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