Understanding Vulnerabilities: How to Conduct Vulnerability Assessments to Know What Attackers Can, and Can't Do

Bryan L Singer, CISSP, CAP
Principal Investigator, Kenexis Security

Jim Gilsinn
Senior Investigator, Kenexis Security
Today’s Talk…

- The “top-down” is in process (corp to plants), now we need to see the “bottom-up”
- Not about cyber security “solutions…”
- Not about how to patch effectively or measure risk
- This is about how to qualify the problem to motivate action – in the terms that engineers and plant managers can understand
- Engineering problems require engineering solutions
The Challenge

- **Researcher:** You have 438 Critical Vulnerabilities!
- **Plant Manager:** So what?
- **Researcher:** I could take control of your PLC from the Internet and do X!
- **Plant Manager:** I’m not connected to the Internet.
- **Researcher:** I can write a worm that will make the PLC overspeed the turbine and put it into surge!
- **Plant Manager:** Good luck. There is a machine protection system separate from the PLC.
- **Researcher:** Well… fine.. You need to patch all these vulnerabilities!
- **Plant Manager:** I don’t shut down for 330 more days – is this important enough to warrant a shutdown?
- **Researcher:** Of course!
- **Plant Manager:** Why? I don’t process credit cards, I don’t run public websites.
- **Researcher:** I can take control of the boiler and blow it up!
- **Plant Manager:** So you set the PLC to over pressure the boiler?
- **Researcher:** Yes!
- **Plant Manager:** There are relief valves – have a nice day…
- And so on and so forth…
The Growing Cyber Security Challenge

- 2014 Data Breach Incident Report shows a three fold increase over 2013
- Over 256 incidents to OT networks were voluntarily reported by ICS owner/operators to ICS-CERT in 2013 alone (most go undetected or unreported)
- Most if not all major vendors have known vulnerabilities in their products reported to ICS-CERT

ADVISORIES
ICSA-13-352-01 NovaTech Orion DNP3 Improper Input Validation Vulnerability, 12/18/2013
ICSA-13-347-01 Siemens COMOS Privilege Escalation, 12/13/2013
ICSA-13-346-01 Cooper Power Systems Improper Input Validation Vulnerability, 12/17/2013
ICSA-13-346-02 Cooper Power Systems Cybertec DNP3 Master OPC Server Improper Input Validation, 12/12/2013
ICSA-13-340-01 RuggedCom ROS Multiple Vulnerabilities, 12/9/2013
ICSA-13-337-01 Electrys Director Gateway Improper Input Validation Vulnerability, 12/3/2013
ICSA-13-321-01A DNP3 Implementation Vulnerability, 11/21/2013
ICSA-13-327-01 Catapult Software DNP3 Driver Improper Input Validation, 11/19/2013
ICSA-13-327-02 GE Proficy DNP3 Improper Input Validation, 11/19/2013
ICSA-13-325-01 WellianTech KungView ActiveX Vulnerabilities, 10/22/2013
ICSA-13-282-01A Alstom e-Terracontrol DNP3 Master Improper Input Validation, 10/21/2013
ICSA-13-289-01 Cisco ASA and FWSM Security Advisories, 10/16/2013
ICSA-13-278-01 Inverness Wonderware InTouch Improper Input Validation Vulnerability, 10/9/2013
ICSA-13-095-01A Rockwell Automation FactoryTalk and RSLogix Vulnerabilities, 10/7/2013
ICSA-13-277-01 Philips Xper Buffer Overflow Vulnerability, 10/4/2013
ICSA-13-274-01 Siemens SCALANCE X-200 Authentication Bypass Vulnerability, 10/3/2013
ICSA-13-259-01 Emerson ROC800 Multiple Vulnerabilities, 9/26/2013
ICSA-12-018-01B Schneider Electric Quantum Ethernet Module Hard-Coded Credentials, 9/23/2013
ICSA-12-231-01B Sixnet Universal Protocol Undocumented Function Codes, 9/17/2013
ICSA-12-254-01 Siemens SCALANCE X-200 Web Hijack Vulnerability, 9/11/2013
ICSA-12-252-01 SUBNET Solutions Inc. SubSTATION Server DNP3 Outstation Improper Input Validation, 9/9/2013
Customer Concerns

- Some Indicators of Fragile and at Risk OT Networks
  - Unexplained process stoppages due to communication failures
  - Slow communications such as slow HMI updates
  - Data reconciliation / discrepancies between business and process support systems (e.g. MES, ERP, LIMS, Historians)
  - Unauthorized / unintentional remote connections to OT networks
  - Unauthorized changes to PLC’s, DCS, or other systems
  - Indicators of viruses, worms, rootkits, bots, or other malware reported from OT networks by IT staff
- Bottom Line: communication errors and network problems risk production uptime, threaten process safety, and open the shop floor to cyber security threats
Symptoms of ICS Network and Security Failures

- **Intermittent Failures**
  - Corrected by logic conditions in the system
  - Minimal to no process interruption

- **Nuisance Trips**
  - Logic interlocks, fail safes

- **Unplanned Outages**
  - Sustained process failures

- **Dangerous Failures**
  - Safety impacts
  - Extended outages
Vulnerabilities for Plant Managers

• We are doing it wrong….

• The Vendor X Software (Process.exe and mylog) does not handle input correctly and results in a logic error if it receives a zero or large byte datagram. If an attacker sends a datagram of zero byte size to the receiver over Port 1234 (user-configurable, not enabled by default), the attacker would cause a DoS condition where the service silently ignores further incoming requests.

• CVE-20XX-XXX has been assigned to this vulnerability. A CVSS v2 base score of 7.9 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).
Risk Management for Plant Managers: 3 Easy Steps

- What is it?
- Is it real?
- What do I do about it?

Safety Risks Require Action...
If you cannot qualify the risk AND give a solution, you are wasting their time
Cybersecurity for Water/Wastewater

• Executive Order 13636 - Improving Critical Infrastructure Cybersecurity, signed by President Obama on Feb. 12, 2013 – Directs adoption of NIST Framework

• AWWA Cybersecurity Guidance and tool: voluntary compliance program

• Water ISAC: [https://www.waterisac.org/about-us](https://www.waterisac.org/about-us)
Failure Modes for ICS

• Intermittent Failures
  – Corrected by logic conditions in the system
  – Minimal to no process interruption

• Nuisance Trips
  – Logic interlocks, fail safes

• Unplanned outages
  – Sustained process failures

• Dangerous failures
  – Kinetic and safety impacts
  – Extended outages
Device Vulnerabilities: The Reality

- Many see security as, “Attack at 8:01AM, at 8:03 the plant goes boom.”
- Compromising an individual BPCS is of limited value.
- Extended damages require compromise and disabling of multiple components.
- Most of this can be done without ever launching a true exploit.
- The combination of cyber security knowledge, process knowledge, and knowledge of control systems is required to move out of the nuisance trip to more significant failures.
Attack Modes for ICS

- Loss of View (LoV)
- Manipulation of View (MoV)
- Denial of Control (DoC)
- Manipulation of Control (MoC)
- Loss of Control (LoC)

- Model each part of the process in terms of how an attacker would bypass protective systems
Turbine Overspeed Scenario

- Engineering Steps to Create a Turbine Overspeed
  - In order to execute the overspeed, the attackers would begin by disabling the overspeed trip system.
  - This would be accomplished by “forcing” the output of safety valve (XV-22) in the safety controller.
  - Also, freezing the value of the speed transmitter (or transmitters, assuming a redundant voting configuration is used) will have the same effect.
  - Once the overspeed trip has been disabled, the load is disconnected from the generator by simply commanding the disconnect switch (HS-23) to the open position.
  - Depending on the specific arrangement of power distribution a similar effect can be achieved either by opening disconnect switch or switches at the generating facility itself, or exploiting SCADA systems to simultaneously open multiple disconnect switches at the electrical power consumers or distribution facilities.
D.1 Simplified Turbine for Power Generation Process Section
D.2 Simplified Turbine for Power Generation Process Section
Sample: Turbine Overspeed Attack Methodology

• Part 1 – Surveillance
• Part 2 – System Mapping
• Part 3 – Initial Infections and Compromise
• Part 4 – Information Exfiltration
• Part 5 – Preparing the Final Attack
• Part 6 – Maximum Damage

There is a crossover point in which cyber security attacks must yield to process attacks
How to Attack…

- Setpoints?
- Change the I/O of a controller?
- Set Alarm Conditions?
- Bypass a Safety System?
- Safety interlock?
- SIS?
ICS-CVA Process

- Required part of validation
- Performed:
  - After initial implementation
  - After major modifications
  - On a regular periodic basis (ISA 4.3.3.2)
- Requirements defined in industry standards
ICS-CVA Process (CONT’D)

• Documentation Collection
  – Network Architecture
  – Piping and Instrumentation Diagrams
  – Asset Inventory

• Network Traffic Capture
  – At each (managed) switch capture all traffic for given time period (e.g., Wireshark)
ICS-CVA Process (CONT’D)

• Live Hosts
  – Ping Sweep (typically nmap) to identify all of the devices
    – Verify Asset Inventory
    – Identify Unknown/Rogue Devices

• Port and Service Detection
  – Port Scan (typically nmap) per Device
    – Identify all open ports
    – Identify all active services
    – Identify operating system
ICS-CVA Process (CONT’D)

• Port and Service Detection
  – Service Detection
    – Banner grab (nmap or netcat)
      – Verify validity of open ports
    – Detect known vulnerable ports/services

• Vulnerability Scanning
  – Automated Scanning (nessus, neXpose)
  – Manual Scanning (nmap, netcat, metasploit)
  – Vulnerability Database (Kenexis)
ICS-CVA Process (CONT’D)

• Open-Source Intelligence
  – Determine information leakage of information (Google, Shodan, Maltego, ARIN, Custom Code)
    – Identify devices exposed to internet
    – Leaks of proprietary information (.doc, .pdf, etc.)
    – Ease of identifying devices
ICS-CVA Process (CONT’D)

• Process Vulnerability Analysis
  – P&ID
  – HAZOP for Max Damage/Impact Scenarios
  – Zone and Conduit/Security Level Analysis
  – Determine which vulnerabilities can be exploited to cause physical impacts
  – Failure Modeling
  – Attack Modeling
Results and Recommendations

• Cyber security improvements
  – Patching, policies/procedures, firewalls, etc.

• Process improvements
  – Upgraded firmware and hardware

• Facility siting and Physical security
  – Barriers to entry
  – Access control

• SIS in place of Controllers
  – Safety interlocks replaced by SIS
Summary

- Engineering problems require engineering solutions!
- Cyber Vulnerability Analysis and Vulnerability Discovery is a very useful exercise, but only stops at device impact
- Qualifying the threat means that the process must be considered
- ICS-CVA includes all of the above
Questions?

- Bryan L Singer, CISSP, CAP
  - Principal Investigator, Kenexis Security
  - Previous Chairman ISA/IEC62443 (ISA-99)
  - Co-Author “Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS” ISBN-10 1439801967
  - Bryan.singer@Kenexis.com

- Jim Gilsinn
  - Senior Investigator, Kenexis Security
  - Current Co-Chair ISA/IEC62443 (ISA-99)
  - Jim.Gilsinn@Kenexis.com
Questions?

Bryan L Singer, CISSP, CAP
Principal Investigator, Kenexis Security
Bryan.singer@kenexis.com