FireEye iSIGHT Intelligence

WHAT ABOUT THE PLANT FLOOR?

SIX SUBVERSIVE CONCERNS FOR INDUSTRIAL ENVIRONMENTS

Sean McBride

FireEye

APRIL 2017

INTRODUCTION

Industrial enterprises including electric utilities, petroleum companies, and manufacturing organizations invest heavily in industrial control systems (ICS) to efficiently, reliably, and safely operate industrial processes. Without the technology operating the plant floor, their business doesn't exist.

Board members, executives, and security officers are often unaware that the technology operating the economic engine of their enterprise invites undetected subversion.

This paper describes six key weaknesses that an adversary can use to undermine a plant's operation, providing real-life threat details and mitigation options.

THE SUBVERSIVE SIX CONCERNS FOR AN INDUSTRIAL ENVIRONMENT:


Unauthenticated protocols


Outdated hardware


Weak user authentication


Weak file integrity checks


Vulnerable Windows operating systems


Undocumented third-party relationships

UNAUTHENTICATED PROTOCOLS

Many ICS protocols operate without authentication—the ability to ensure that data comes from a trusted source. When an ICS protocol lacks authentication, any computer on the network can send commands that alter the physical process, such as changing the set point or sending an inaccurate measurement value to the Human Machine Interface (HMI). This may lead to incorrect process operation, which damages goods, destroys plant equipment, harms personnel, or degrades the environment. Source authentication is normally achieved by verification and use of cryptographic keys.

Threat Information

Unauthenticated protocols used to communicate between the sensor/actuator and the input/output of the PLC commonly include: Modbus, HART, CAN, Foundation Fieldbus, PROFIBUS, and many others.

- In 2013 Russian security researcher Alexander Bolshev discussed an attack technique that involves: 1) severing the HART connection; 2) connecting the wire to a specialized printed circuit board; 3) manipulating the output to exploit vulnerabilities in the software that uses the HART communications. Tools for these techniques are also publicly available. The researchers proposed adding additional functionality and protocol coverage.
- Since at least 2010, researchers from the University of Washington and University of California San Diego demonstrated their ability to connect their laptop to an automobile's on board diagnostics (ODBII) port and send CAN messages, controlling brakes, steering, windshield wipers, blinkers, and locks under certain automotive speed conditions.

Unauthenticated protocols used to communicate among the PLCs, and between the PLCs and management computers commonly include, but are not limited to: DNP3, Modbus/TCP, BACnet, EtherNet/IP, and various vendor proprietary protocols.

- Any user with access to a device that uses one of these protocols can communicate with it by simply using appropriate client software, such as various open source offerings.
- In 2012 researchers from Digital Bond demonstrated the following:
  - Using the Schneider Electric Modicon Quantum Modbus function code 90 to perform administrative actions including sending a STOP command and uploading new control logic. The researchers released a Metasploit module for this attack.
  - Using the functionality of EtherNet/IP to stop the CPU, reboot the controller, crash the CPU, and crash the Ethernet module of an Allen Bradley ControlLogix PLC.

MITIGATION

- ☐ Identify all unauthenticated protocols in use on process control networks to provide understanding of vulnerability level.
- ☐ Assess whether current equipment can support authentication options.
- ☐ Implement authentication options where feasible, such as DNP3 Secure Authentication and BACnet security.
- ☐ Assess whether the controlled process can withstand latency introduced by bump-in-the-wire authentication solutions.
- ☐ Implement bump-in-the-wire authentication solutions or VPNs.
- ☐ Incorporate deep packet ICS firewalls that block unauthorized commands from certain IP addresses.
- ☐ Configure restrictive access control lists and firewall rules.
- ☐ Request authentication features from vendors.

OUTDATED HARDWARE

ICS hardware can be operational for decades. This hardware, such as PLCs, RTUs, VFDs, protective relays, flow computers, and gateway communicators, may operate too simplistically or lack the processing power and memory to handle the threat environment presented by modern network technology.

Threat Information

- Since 2012, researchers at Digital Bond have pointed to the GE D20ME as an example of a vulnerable ICS device running outdated technology that is still (Feb. 2017) available for purchase (though GE released an updated version — the D20MX — in 2013).
- The U.S. Nuclear Regulatory Commission published that in August 2006, PLCs and VFDs at Browns Ferry Nuclear Generating Station malfunctioned as a result of excessive network traffic.
- In a report released in 2005 by the U.S. Department of Energy, Sandia National Laboratories indicates that at some previous date a ping sweep resulted in activation of a robotic arm, and that a separate ping sweep halted production at an integrated circuit production facility.
- The Repository of Industrial Security Incidents (RISI) reports two cases, one in 2002 and one in 1995, in which network scans caused PLCs to crash.

MITIGATION

- ☐ Consider upgrades for older devices that have network connectivity and support critical process control functions.
- ☐ Implement firewall rules to minimize network connectivity of devices with outdated hardware.

WEAK USER AUTHENTICATION

User authentication refers to the ability to ensure that only intended individuals can access a computer or use its programs. ICS users commonly authenticate by providing passwords. User authentication weaknesses in legacy control systems often include hard-coded passwords, easily cracked passwords, passwords stored in easily recoverable formats, and passwords sent in clear text. An attacker who obtains these passwords can often interact with the controlled process at will.

Threat Information

- One group of researchers actively maintains (September 2016) publicly available lists of hard-coded or default passwords for ICS devices. Attackers can easily review these lists and use the passwords where applicable.
- Researchers have disclosed dozens of vulnerabilities involving password weaknesses in ICS devices and software from numerous vendors. Attackers with access to these devices may exploit the weaknesses to access the devices or software.
- In 2009 Stuxnet took advantage of a hard-coded password within a Siemens S7 database to gain access to its target and ultimately manipulate the controlled process.

MITIGATION

- ☐ Match internal ICS device inventory against list of devices known to have hard-coded passwords.
- ☐ Monitor device logs and network traffic for attempts to exploit password weaknesses.

WEAK FILE INTEGRITY CHECKS

Integrity checking refers to the ability to verify the integrity and origin of data or code. This is normally achieved by cryptographic verification. We identify three instances in which integrity checking is deficient in ICS:

- Weak software signing
- Weak firmware integrity checks
- Weak control logic integrity checks

WEAK SOFTWARE SIGNING

Software signing is used to verify that software is from an authorized source. A vendor will either generate their own certificate or rely on a certificate authority to allow the client to verify the source. Lack of software signing allows attackers to mislead users into installing software that did not originate from the vendor. It also allows attackers to replace legitimate files with malicious ones.

Threat Information

- Starting in March 2015, researchers reported at least 10 DLL hijacking vulnerabilities in ICS software. Integrity checks would mitigate attempts to exploit these vulnerabilities.
- In 2014 Koala Group distributed Fertger malware by compromising ICS vendor websites and replacing a legitimate file with a malicious version. The incident indicates that even apparently trusted sources may be malicious. Those downloading the software would only notice the replacement by checking file integrity.
- In 2009 Stuxnet replaced a legitimate driver DLL with a malicious copy because there was no integrity checking.

WEAK FIRMWARE INTEGRITY CHECKS

Firmware is the code that enables an embedded device such as a PLC or an RTU to perform its functions. It is generally more difficult to change or update than software. An adversary who can upload firmware controls the entire operation of the device.

Threat Information

- In December 2015 Sandworm Team exploited weak firmware integrity checks in serial-to-IP converters from Moxa and IRZ to prolong power outages in Ukraine.
- In October 2015 researchers from CyberX used a firmware replacement vulnerability to discover additional vulnerabilities in a Rockwell Automation PLC.
- In July 2015 researchers from Digital Bond Labs discovered firmware upload vulnerabilities affecting ICS devices from Moxa.
- In 2013 a Master's degree candidate from the U.S. Air Force Institute of Technology demonstrated a firmware modification attack against a Rockwell Automation PLC.
- In 2009 researchers from Digital Bond demonstrated modifying firmware on PLCs from Koyo and Rockwell Automation.
- In 2009 the U.S. Department of Homeland Security (DHS) warned that adversaries may attack industrial environments by pushing rogue firmware uploads to controllers in a plant.

WEAK CONTROL LOGIC INTEGRITY CHECKS

Control logic refers to the process control program executed by a programmable controller such as a PLC. A lack of adequate control logic integrity checking means that the PLC accepts the logic without verifying that it was created by an authorized user using authorized engineering software. Such a user may alter set points and control equipment.

Threat Information

- In March 2016 researchers demonstrated a PLC worm that spread from one Siemens PLC to another by modifying control logic. The researchers argue that other PLCs using unencrypted protocols are susceptible to similar attacks.
- In July 2015 researchers demonstrated a PLC worm that spread from one PLC to another by modifying control logic. They implemented an SNMP scanner using this technique.
- In 2009 Stuxnet modified logic sent to target certain Siemens PLCs.

MITIGATION

- ☐ Configure the operating system to only run signed code.
- ☐ Test software and updates in a simulated environment prior to production deployment.
- ☐ Obtain software/firmware directly from the vendor and not third-parties.
- ☐ Work closely with vendor support to obtain file hashes and check hashes manually.
- ☐ Configure PLC access protection if available.
  - While this disallows modification of PLC logic on the PLC without an appropriate password, it is not of itself equivalent to integrity checking.
  - It is important to note that protection methods offered by some vendors are implemented in the engineering software rather than on the PLC, meaning that other software can still interact with the PLC with activity such as uploading or down-loading logic or firmware.
- ☐ Monitor the network for firmware and logic updates.
- ☐ In December 2010, Langer Communications marketed the Controller Integrity Checker tool to check logic integrity on Siemens PLCs.

VULNERABILITIES AFFECTING WINDOWS OPERATING SYSTEMS

Engineering workstations and HMIs often run outdated and unpatched Microsoft Windows operating systems, leaving them exposed to known vulnerabilities. In some cases, this means that adversaries may access industrial systems without needing control systems specific knowledge.

Threat Information

- Exploit kits frequently incorporate exploits for older and unpatched systems, even if patches are available. These can affect unpatched or outdated HMI computers accessing the Internet.
  - Over the course of 2015, numerous exploit kits targeted vulnerabilities in unsupported operating systems and vulnerabilities in supported operating systems where patches were available.
- Advanced threats, such as APT 17 and actors using Kraken malware, continue to target Windows XP and Windows Server 2003.
- Vulnerabilities in Windows 7 (support available through 2020), such as CVE-2011-5046, CVE-2010-4701, and CVE-2010-3227, also affect Windows XP (no longer supported).
- Publicly available exploit code exists for at least eight vulnerabilities affecting Windows server 2008 (Service Pack 1 and 2 supported to January 2020) and Windows Server 2003 (support ended in July 2015).

MITIGATION

- ☐ Maintain an inventory of operating systems used in an industrial environment that are unpatched or no longer supported. Plan to upgrade or apply patches at maintenance down times in accordance with ICS vendor guidance.
- ☐ Deploy compensating controls for vulnerabilities affecting these systems, especially when the vulnerabilities are known to have been exploited in the wild.

UNDOCUMENTED THIRD-PARTY RELATIONSHIPS

In our experience, ICS asset owners seldom document and track third-party dependencies in ICS software they operate. Many ICS vendors may not immediately know the third-party components they use, making it difficult for them to inform their customers of the vulnerabilities. Adversaries who understand these dependencies can target software the industrial firm may not even know it has.

Threat Information

- In January 2013 Russian researchers identified at least 15 third-party products used by Siemens WinCC. These products exhibited a total of over 1,800 vulnerabilities, one of which was disclosed in 1997.
- GarrettCom's Magnum 6K Switches are OEMed and marketed by GE as the Multilin ML800. Neither vendor makes this explicitly clear. Due to this, Multilin ML800 users may not be properly informed of a vulnerability that may affect the device because a government report attributes it only to GarrettCom's Magnum 6K Switches.
- Two other examples of third-party issues that affected ICS in recent years are Heartbleed and Poodle. Both weaknesses affected numerous ICS devices; however, many vendors did not release advisories until months after the weaknesses were publicized.

MITIGATION

- ☐ Request or require that ICS vendors provide a list of third-party software and versions used in their products, including open-source software.
- ☐ Examine ICS products to identify third-party software before operational deployment.
- ☐ Review vulnerability repositories such as the national vulnerability database to identify vulnerabilities affecting the third-party software.
- ☐ Obtain a structured vulnerability feed to receive notifications of new vulnerability disclosures affecting those third-party products.
- ☐ Request or require that the vendor provide notification of vulnerabilities affecting third-party software.
- ☐ Request or require that vendors validate patches for the third-party software to ensure interoperability.

CONCLUSION

A clear understanding of the Subversive Six weaknesses in plant environments aids corporate boards, executives and security officers to engage in knowledgeable conversation about ICS security, ask discerning questions, and make sound investments.

Plant managers, plant operators and field technicians who understand these issues are prepared to provide vital input to the feasibility of proposed technological solutions and maximize their utility once deployed.

Only FireEye iSIGHT Intelligence arms risk executives and security practitioners with actionable intelligence across the *entire* enterprise.

For more resources and reports from FireEye iSIGHT Intelligence, visit **www.fireeye.com/current-threats.html.**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye