Nov 29, 2012

INDUSTRIAL AND SCADA SYSTEMS MAY BE INCREASINGLY TARGETED FOR CYBERATTACK

Dr. Clay Wilson

Director for Cybersecurity Policy Graduate Studies

University of Maryland University College

Clay.wilson@umuc.edu

December 22, 2012

Contents

Introduction

In a July 19, 2012 essay in the Wall Street Journal, President Barack Obama warned that "the cyber threat to our nation is one of the most serious economic and national security challenges we face."

Industrial control systems are the likely targets for future cyberattacks, partly because their cybersecurity controls are inadequate to prevent modern, targeted attacks. Industrial control systems are also commonly called Supervisory Control And Data Acquisition (SCADA) systems. SCADA systems are used to manage facilities for most critical national infrastructures including power, energy, water, transportation, and telecommunication, and they also control the delivery mechanisms for essential services, such as pipelines.

In 2011, a pump at a public water utility in Springfield, Illinois was destroyed after cyber attackers gained access to a SCADA system controlling the device, according to a security expert who said he obtained an official report about the incident (Vijayan, 2011) (Rushe, 2011).

In 2009, the Wall Street Journal reported that the industrial control systems operating a portion of the U.S. electric power grid had been hacked, supposedly to create secret openings so the attacker could get back in with ease. Analysts, including Richard Clarke, have observed that the most likely reason for penetrating the grid's controls was to counter American military superiority by threatening to damage the underpinning of the U.S. economy through disruption of the SCADA control systems of critical infrastructure facilities (Clarke, 2011).

In November 2011, Michael Welch, the deputy assistant director of the Federal Bureau of Investigation's Cyber Division, reportedly told attendees at the Flemings Cyber-Security conference in London that unknown attackers had compromised the industrial control systems monitoring the infrastructures in three U.S. cities and could have done a lot of damage. The attackers had control of the city's systems and could have performed a variety of malicious activities, such as dumping raw sewage into the lake and shutting down a power plant at a mall, according to Welch. For security reasons, more details about the hacker attacks were not disclosed at the conference (Rashid, 2011).

Market analysts believe that the total market for SCADA products is expected to grow at nearly 10 percent for at least the next five years. The increasing reliance on these automated systems also makes them a target for more cyberattacks (Reed, The Increased Threat of Attacks on SCADA Systems, 2011). And because SCADA systems have persistent cybersecurity vulnerabilities, future exploits will increasingly target industrial control systems.

This report will explain that vulnerabilities for SCADA systems persist for two primary reasons: partly because many industrial control computers use outdated operating systems which are difficult to update; and also, cybersecurity specialists sometimes do not appreciate that operation of SCADA systems is also dependent upon physics of materials in motion, and also on chemical reactions. These constraints impose a different set of priorities for designing and implementing effective cybersecurity controls for industrial control systems.

SCADA and Industrial Control systems

SCADA systems normally contain a Programmable Logic Controller (PLC), which is a collection of solid state circuit boards used for communications between controllers. Some SCADA systems are placed in remote locations that are hardened against weather, and are designed to run nonstop for months or years. Through Internet connections to SCADA systems, managers can have precise and remote control of their infrastructure machinery. This arrangement also reduces the required number of workers in the field.

Industrial control systems were originally designed to operate in isolation, without connection to other networks. As a result, cybersecurity controls were not built in. However, SCADA systems collect data that can be used to generate useful reports, and more recently these systems were connected to the business management systems for faster access to this data. Business systems are connected to the Internet, and once a system is connected via TCP/IP to another (with others in between them), numerous openings are created to penetrate the target system (Shaw, 2012).

Shodan

In late 2009, a new search engine called Shodan, originally intended to improve security and discover information about machines linked to the Internet, revealed that many SCADA computers that automate water plants and power grids were wide open to exploitation by hackers. The Shodan search engine has reportedly revealed water-treatment facilities, power plants, particle accelerators and other industrial control systems that may have security vulnerabilities. Shodan users reportedly also found and accessed the cyclotron at the Lawrence Berkeley National Laboratory. (Whitney Shefte, Sohail Al-Jamea and Robert O'Harrow Jr, 2012).

The Shodan search engine allows users to find devices connected to the Internet based on city, country, latitude/longitude, hostname, and involved operating systems. Shodan is now widely available to most researchers and hackers on the Internet, and can be used to identify and geographically locate even poorly or unprotected computers – and increasingly, industrial and SCADA systems fall into this category. Such activity can be used for espionage to gather information to prepare future cyberattacks.

DHS issues warnings about SCADA vulnerabilities

In February 2012, ICS-CERT issued a warning to utilities to monitor for cyberattacks through Internet connections that allow remote access to control systems. The ICS-CERT warning explained that many organizations have been seeing a large number of access attempts by remote attackers. (CERT, 2012). In October 2012, ICS-CERT issued an advisory (#12-097-02A—3S), warning of vulnerabilities affecting programmable logic controllers (PLCs) and SCADA systems. Researchers had publicly released a description of these vulnerabilities, and also released two exploit tools that could be used to attack the PLC and SCADA vulnerabilities to obtain control over a facility. The identified PLCs and SCADA equipment with the published vulnerabilities are used to run power plants, oil pipelines, military

environments and ships. DHS warned that the new exploitation tools could crash or restart the vulnerable devices.

SCADA vulnerabilities and exploits are openly published

Some researcher organizations acting as "white-hat" hackers send alerts to SCADA equipment vendors about newly-discovered cyber vulnerabilities that affect their products. If no response is returned, they proceed to openly publish cyber exploits that can disrupt that same SCADA equipment. This is advertised as part of their business to promote penetration testing services. (See http://erpscan.com/services/sap-penetration-testing/). Problems most often found when researchers examine SCADA systems are back doors that enabled hackers to download passwords or sidestep security completely. For example, the General Electric D-20 controller uses the same microprocessor installed in Apple computers two decades ago. The company that made the D-20 operating software stopped updating it in 1999 (Whitney Shefte, Sohail Al-Jamea and Robert O'Harrow Jr, 2012).

Countries are developing cyber weapons that attack SCADA systems

In 2010, the U.S. stood up its Cyber Command, located at Fort Meade in Maryland. In August 2012, the U.S. Air Force announced that it was requesting concept papers for building offensive cyber weapons with capabilities for cyber warfare attack, to destroy, degrade, deceive, and corrupt targeted computer systems (Hoover, 2012). Also in August 2012, the Air Force Research Laboratory reportedly gave six contracts valued at up to $300 million under a program called Agile Cyber Technologies (ACT) tasking them to remain on standby to provide cyber weapons to the U.S. on-demand (Reed, Coming soon on demand: Cyber weapons, 2012).

In 2012, DARPA announced a $110 million research program named Project X, reportedly intended to give U.S. military commanders the capability to target and disable specified computer systems anywhere on the Internet. The research also seeks to create pre-planned attack and counter-attack scenarios that do not involve human intervention before they are launched (Nakashima, 2012).

Stuxnet is an example of malicious code used to target and destroy industrial and SCADA systems. Stuxnet code reportedly was created several years ago jointly by the U.S. and Israel, and then quietly launched against nuclear industrial facilities located in Iran. It operated undetected for several years, and infected a specific type of industrial controller at Iran's uranium-enrichment plant in Natanz, causing almost 1,000 centrifuges to spin out of control. The malicious code sabotaged the industrial facilities by reprogramming the Programmable Logic Controllers (PLCs) to operate erratically, while also hiding the incident from the network operators by displaying false readings on the monitoring dashboard (Zhu, 2010).

Stuxnet was designed for physical sabotage of industrial control equipment and systems. Stuxnet injected malicious commands into the PLC at the nuclear facility, and also was able to hide the injected code from facility staff in Iran. When programmers in Iran operated the infected controllers and tried to view the computer code in the PLC, they could not see the malicious code injected by Stuxnet. After the

malicious code was finally discovered and analyzed, Iran was left with its own copy of Stuxnet, which it can now reverse-engineer and later modify for its own purposes. Many SCADA facilities worldwide remain vulnerable to another Stuxnet-style attack.

In response to being targeted by Stuxnet malicious code, Iran reportedly has now created its own new Cyber Command. Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, reportedly said that the Iranian military was now prepared "to fight our enemies" in "cyberspace and Internet warfare," a formula that may imply aspirations to go on the offensive (Kemp, 2012). Other observers have predicted this evolution to creation of new cyber commands, as nations move to create to protect their national security in cyberspace (C Demchak, 2011, pp. 34, 50).

Priorities for SCADA cybersecurity are reliability and safety

What is often not fully understood by many cybersecurity specialists is that the operation of SCADA systems places unique constraints on how cybersecurity can be implemented. Industrial equipment is designed to monitor chemical reactions, or move materials and/or energy, such as water or electricity, and the laws of physics that govern the movement of these materials and monitor the energy must be carefully understood and obeyed by the engineers and operators. These materials move with powerful forces, and industrial controllers must communicate feedback signals and interact with each other within milliseconds to avoid overpressures or extreme torque events that can disrupt or destroy equipment, disrupt service to customers, or possibly injure workers. These constraints have caused engineers to develop a set of priorities to insure safe and reliable operation of industrial equipment. These same constraints have also affected the priorities for implementation of cybersecurity controls when applied to industrial facilities.

Standard cybersecurity best practices have been developed and refined over the years by focusing on traditional office IT systems. For these traditional office systems, the best practices for cybersecurity are intended to achieve three primary goals, often referred to as “CIA”:

- Maintain confidentiality
- Protect message integrity
- Insure system availability

However, in the world of industrial systems, the goals for cybersecurity are placed in a different order, with a different priority that emphasizes availability and safety:

- Insure system availability (plus safety)
- Protect message integrity
- Maintain confidentiality

The major focus for industrial systems cybersecurity is availability/safety. So, the traditional “CIA” cybersecurity goals for office IT systems has been reversed to “AIC” for industrial systems. It cannot be

emphasized too strongly that, for industrial engineers, reliability and safety are the most significant security priorities.

Industrial equipment can be slowed by perimeter security controls

Because of the constraints described above, some traditional cybersecurity practices and procedures that are standard for office IT systems may not work as well for SCADA systems. For example, because industrial SCADA equipment must send monitoring signals to other industrial controller equipment within milliseconds, traditional antivirus software or network intrusion detection devices will not fit very well. This is because scanning network transmissions for malicious code would significantly slow down the high speeds that are required for real-time interactions between industrial equipment. Since this could adversely affect system availability and safety, many industrial systems do not install network scanning software as part of their cybersecurity program. Often, many industrial networks often lack the kinds of perimeter and host defenses that are typically found protecting standard office computer networks.

Highly-skilled experts are not always on site

Organizations that maintain SCADA networks may not have the scanning tools or capabilities to detect cyber intrusions, nor do they have enough personnel with necessary skills to properly and quickly evaluate and recover a SCADA system after a suspected cyberattack (Bradley, 2011). Traditional CERT teams are equipped to respond to emergencies that involve cyberattacks against office IT systems. However, most may not be equipped to protect or evaluate a SCADA system that is experiencing a cyberattack.

Because automated systems enable reductions in personnel, often when a problem requires emergency action, not enough trained personnel are on-site to protect reliability and safety of the SCADA systems that may be under attack. When problems require emergency actions, planning manuals may not provide solutions for every incident that might occur. Therefore, SCADA equipment vendors must be available to login remotely to fix problems that the industrial facility personnel cannot handle. However, maintaining this type of remote access for SCADA vendors also keeps the door open for possible cyberattack.

Cybersecurity is poorly repackaged for industrial systems

Engineers sometimes complain that software coders responsible for configuration management of SCADA systems do not understand the engineering constraints or the physics that the industrial systems must control. Today, equipment is designed by programmers who follow design concepts that are placed before them, without actually having a good understanding of the processes the equipment is designed to monitor. The greater the complexity of the industrial application, the greater is the need for software programmers to understand how the equipment communicates, and exactly how that equipment is interconnected to other SCADA systems.

There is currently a lack of college curricula for industrial cybersecurity and a lack of industrial cybersecurity professional certifications. Most workers that are now becoming involved with industrial cybersecurity are coming from working with traditional office IT systems, where best practices for cybersecurity have been refined for several years. However, these best practices have often been repackaged for industrial systems without fully appreciating the special requirements and constraints that are also involved. Joe Weiss, a well-known expert on cybersecurity issues for industrial control systems, has stated that the lack of understanding on the part of programmers or traditional security professionals can sometimes make SCADA systems less reliable without actually increasing the cybersecurity (Weiss, 2010, p. 211).

Software patches are applied infrequently

Office IT best practices require regular updates to apply the latest security software patches. However, an industrial facility cannot install software patches as frequently. In fact, software patching for an industrial facility, whether larger or smaller, may be an expensive and disruptive operation. For example, to install a security patch update onto the control systems for a gas or coal-fired turbine generator requires careful planning and several involved steps:

- The power generation equipment must be shut down
- The equipment must be allowed to cool down (while observed by personnel)
- The control systems must then be turned off and disconnected to install the patch
- The control system must be restarted
- The power generation equipment must be restarted

It has been estimated that this process can cost between $1 million to $1.5 million dollars, depending on the size or number of power generators involved. The duration for this process may require several days. At the same time, the customers who are served by the power generator expect their service will not be interrupted due to installation of a software patch.

Software patches require extensive testing

Because reliability is most important, there is little or no tolerance for a software security patch that might cause disruption after the complex installation process is finished. Therefore, security patches must undergo extensive testing to verify that they will maintain systems stability, while they are closing security gaps. This is complicated when a security update is planned for a SCADA operating systems that is not actively supported by the original vendor.

Conclusion

The security priorities for industrial systems differ from the security priorities that are common to office IT systems. The most important priorities for industrial systems are maintaining availability and safety, followed by protection of integrity and confidentiality.

Industrial systems are highly vulnerable to cyberattacks because they lack many of the defensive cybersecurity tools that are common to office IT systems. However, this is because the security priorities for ICS systems are different. These differences need to be more fully understood by vendors that write programs for industrial controls systems, and by other cybersecurity specialists and CISOs (Chief Information Security Officers) as they make plans to improve cybersecurity for industrial systems.

Meanwhile, the U.S. and other countries are creating Cyber Commands, and possibly constructing cyber weapons that can duplicate or exceed the capabilities demonstrated by the recent Stuxnet attack against industrial facilities in Iran. The Shodan search engine is available to researchers and hackers, and through careful operation it continues to reveal the configuration and geographic location of vulnerable industrial systems.

Highly-skilled experts are being displaced by increased reliance on automation, and one result is that instruction manuals may not be fully adequate to handle unexpected cybersecurity emergencies that arise at industrial sites. Software patches for industrial control systems are not applied frequently because planning can be complex, the process can be expensive, and service disruptions are not easily accepted by utility customers. Many industrial control system networks do not employ intrusion detection and prevention tools, or basic network logging because these security controls would slow the real-time process required for industrial systems.

To date, there have been remarkably few documented intentional cyberattacks on U.S. critical infrastructure networks (Tsang, 2009). Perhaps we have been lucky so far.

END

Contact information for the author:

Clay Wilson, PhD, CISSP,< Clay.Wilson@umuc.edu >

Dr. Wilson is a member of the Landau Network Centro Volta, International Working Group. He has presented at National Defense University on the topic of cybercrime, and at the Cyber Conflict Studies Association on the cyber capabilities of terrorist groups. He has moderated for the National Nuclear Security Administration for discussion of Nonproliferation for Cyber Weapons, and has presented on the same topic at the Defense Cyber Investigations Training Academy. Dr. Wilson is a former analyst for national defense policy at the Congressional Research Service.

Bibliography

Bradley, T. (2011, Nov 20). *Water Utility Hacked: Are Critical Systems at Risk?* Retrieved Nov 26, 2012, from PC World:

http://www.pcworld.com/article/244359/water_utility_hacked_are_our_scada_systems_at_risk_.html

C Demchak, P. D. (2011, Spring). Rise of a Cybered Westphalian Age. *Air University Strategic Studies Quarterly*, pp. 32-61.

CERT, U. (2012, Feb 23). *ICS-ALERT-12-034-01—SSH SCANNING ACTIVITY TARGETS CONTROL SYSTEMS*. Retrieved Nov 26, 2012, from DHS ICS-CERT ALERT: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-034-01.pdf

Clarke, R. (2011, Jun 15). *China's Cyberassault on America* . Retrieved Nov 26, 2012, from The Wall Street Journal: http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html?mod=wsj_share_facebook

Hoover, N. (2012, August 30). *Air Force Seeks Offensive Cyber Weapons*. Retrieved Sep 1, 2012, from Information Week: http://www.informationweek.com/air-force-seeks-offensive-cyber-weapons/240006574

Kemp, S. (2012, Jun 7). *Cyberweapons: Bold steps in a digital darkness?* Retrieved Sep 20, 2012, from Bulletin of the Atomic Scientists: http://www.thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness

Nakashima, E. (2012, May 30). *Washington Post*. Retrieved Sep 04 2012, 2012, from With Plan X, Pentagon seeks to spread U.S. military might to cyberspace: http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

Rashid, F. (2011, Dec 1). *FBI Admits Attackers Compromised SCADA Systems in Three U.S. Cities*. Retrieved 26 2012, Nov, from eWeek: http://www.eweek.com/c/a/Security/FBI-Admits-Attackers-Compromised-SCADA-Systems-in-Three-US-Cities-548815/

Reed, J. (2011, Sep 26). *The Increased Threat of Attacks on SCADA Systems*. Retrieved Nov 26, 2012, from Defense Tech: http://defensetech.org/2011/09/26/the-increased-threat-of-attacks-on-scada-systems/

Reed, J. (2012, Sept 5). *Coming soon on demand: Cyber weapons*. Retrieved Oct 30, 2012, from Foreign Policy: National Security: http://killerapps.foreignpolicy.com/posts/2012/09/05/coming_soon_on_demand_cyber_weapons

Rushe, D. (2011, Nov 20). *Cyber-attack claims at US water facility*. Retrieved Nov 26, 2012, from The Guardian: http://www.guardian.co.uk/world/2011/nov/20/cyber-attack-us-water-utility

Shaw, W. T. (2012, Nov 20). *SCADA System Vulnerabilities to Cyber Attack*. Retrieved Nov 26, 2012, from Electric Energy Online: http://www.electricenergyonline.com/?page=show_article&mag=23&article=181

Tsang, R. (2009, Nov 20). *Cyberthreats, Vulnerabilities and Attacks on SCADA*. Retrieved Nov 2012, 2012, from Goldman School of Public Policy at UC Berkeley: http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf

Vijayan, J. (2011, Nov 20). *Hack Suspected for Illinois Water Pump Sabotage*. Retrieved Nov 26, 2012, from Computer World: http://www.pcworld.com/article/244352/hack_suspected_for_illinois_water_pump_sabotage.html

Weiss, J. (2010). *Protecting Industrial Control Systems from Electronic Threats.* New York: Momentum Press.

Whitney Shefte, Sohail Al-Jamea and Robert O'Harrow Jr. (2012, Jun 3). *Cyber search engine Shodan exposes industrial control systems to new risks*. Retrieved Nov 27, 2012, from The Washington Post: http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html

Zhu, B. (2010, Nov 20). *A Taxonomy of Cyber Attacks on SCADA Systems*. Retrieved Nov 24, 2012, from Berkeley Northside Research Group: http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf