Hybrid Approach for Assessing Security Vulnerability and Increasing the Resiliency of Industrial Control System (ICS)

Ruhama Mohammed Zain
CyberSecurity Malaysia
Seri Kembangan, Malaysia
Email: ruhama [AT] cybersecurity.my

Abstract—**Critical infrastructures are found in the modern world and include power generation and transmission, gas, water, and other utilities, transportation systems and others. This paper is concerned with securing Industrial Control Systems (ICS) that are controlling many critical infrastructures. TCP/IP is being used to connect ICS systems because it is more efficient than the proprietary protocols of decades ago and is also more cost effective. However, the convergence of ICS systems into the corporate IT network presents challenges for the security team to ensure the entire connected system is secure. One of the unique challenges is how to safely perform security assessments on ICS systems due to its proprietary protocols and intolerance to down time. To address these challenges, this paper seeks to explain how ICS systems can be secured from a cyber security standpoint by a hybrid approach that combines conventional vulnerability assessment methods and strategies to increase the resilience of the ICS components by making it more robust and less fragile. The methods are chosen from existing security assessment methodologies and best practices. Using this approach we will be able to assess the vulnerabilities and offer another perspective on how to defend against them which is not so much tied to risk but performance and control driven. The results of this work could offer solutions to increase cyber security within the critical infrastructures.**

Keywords-component; ICS; SCADA; cyber threat; security vulnerability; assessment methodology, mitigation

I. INTRODUCTION

People in the modern world rely on infrastructures that provide utilities and services essential to their safety, health, economic wellbeing and security. These infrastructures are controlled and managed using Industrial Control Systems (ICS) or sometimes referred to as SCADA systems. Industrial Control Systems (ICS) operators used to manually adjust switches and knobs to control the running of electricity generation plants, water treatment plants and similar systems. Advancement in technology has made it possible to replace the manual controls and also to remotely operate controls. The systems have grown in scale and complexity, ranging from localized networks to those operating across large geographical distances through private corporate networks and the Internet. As the use of Industrial Control Systems (ICSs) has grown, system providers have migrated to standard system platforms and off-the-shelf software using standard operating systems and the TCP/IP protocol [1]. This has increased their exposure to cyber security threats similar to what is normally faced by an office network and so there is a great need for asset owners to thoroughly assess the security of their ICS network. The similar nature between threat agents that target IT and ICS assets is also mentioned by [2].

A survey of incidents impacting SCADA and critical infrastructures [3] highlighted several well-known cases starting from 1982 with the Siberian pipeline explosion (which was attributed to a trojan attack), until 2012 when the "Flame" malware was discovered stealing data and deleting information from infected machines. In between those two events we had other incidents including the infamous Stuxnet attack against the Iranian uranium enrichment facility in 2010 [3].

The key point to remember is that ICS or SCADA systems control physical processes and when the system functions are deliberately or inadvertently disturbed there is a real danger of physical harm or damage to the process output or worse, a negative impact to the surrounding environment. A physical impact could include the release of hazardous materials, damaging kinetic forces (e.g., explosions) and exposure to energy sources (e.g., electricity, steam) [1].

There has been a steady growth in ICS related incidents in the United States that impacts critical infrastructures owned and operated by US organizations [4]. In 2011, there were 140 reported incidents. In 2012 this had increased to 197 reported incidents and the response team was deployed onsite on six occasions [4]. In 2013, 257 incidents were reported. Although this increase may be partly due to increased awareness on the importance of incident reporting, it is interesting to note that the incidents included confirmed threats that utilized different threat vectors. In 2014, the scope of incidents encompassed a vast range of threats and observed methods for attempting to gain access to both business and control systems infrastructure [5]. Reported cases included unauthorized access and exploitation of Internet facing ICS/Supervisory Control and Data Acquisition (SCADA) devices, exploitation of zero-day

vulnerabilities in control system devices and software, malware infections within air-gapped control system network, SQL injection via exploitation of web application vulnerabilities, and strategic website compromises (watering hole attacks) [5].

Taking into account the criticality of the systems being controlled and managed by ICS there is clearly a need to safely assess the security of the ICS network to identify vulnerabilities that could potentially be exploited by attackers and to make the system more robust in terms of cyber security.

This will constitute part of the recommended defense-in-depth strategy by the U.S. Department of Homeland Security [6].

Further support of performing technical audits of SCADA devices and networks can be found in [7] where it is identified as one of the steps to improve the cyber security of SCADA networks.

The term "SCADA" is sometimes used to represent both ICS in general as well as when specifically referring to the ICS system that is of the SCADA variety. This is unavoidable due to popular usage in the press as well as in some government publications, for example in [7].

II. The Theoretical Definition of Security

Manunta [8] proposes a definition of security that encompasses the aspects of security that can be applied or extended all the way from the security of the individual to national defense. The security components are then used to define the formula for security:

$$\text{Security} = \grave{O}(A, P, T)Si \qquad (1)$$

Where A = asset, P = protection, T = threat, Si = situation

This paper shall not look at the multi-dimensionality of security as in (1) but will instead focus on the specific problem of assessing security in an Industrial Control System (ICS) network using an effective methodology that does not jeopardize the stability and safety of the ICS network under assessment. Further to that idea we will also mention steps to increase the robustness of the ICS network itself such that not only security (as narrowly defined here) is improved but also the overall resiliency and dependability of the ICS to continue running the process operations.

III. The IT Network Security Assessment Methodology

The conventional network security assessment methodology usually involves four distinct high-level components [9]:

1. Network reconnaissance to identify IP networks and hosts of interest
2. Bulk network scanning and probing to identify potentially vulnerable hosts
3. Investigation of vulnerabilities and further network probing by hand
4. Exploitation of vulnerabilities and circumvention of security mechanisms

The problem with applying this conventional assessment methodology against an ICS network is due to the sensitivity and lack of robustness of the ICS network components to withstand even a simple port scan of open ports on the device. There have been reports of unintentional outage and disruption caused by common port scanning activity using port scanner tool. Examples of adverse impacts caused by ping sweeps are mentioned in [10]. Unintentional security incidents caused by vulnerability scanning and penetration testing are also described in [10].

Clearly a different approach is required to conduct assessment on a live ICS network that will balance the need to be thorough and the need to be careful about the sensitive nature of the ICS devices.

IV. The Modified Assessment Methodology for ICS Networks

In order to mitigate problems associated with active scanning, there are suggested techniques for performing inventory or vulnerability scan on an ICS network segment. Table I lists the recommended actions [10].

The inventory of ICS systems and network assets can be done using automated tools but only after testing them in a non-production network to verify that they do not adversely impact the production system [10].

The key idea is not to generate any disruptive traffic on the ICS network while the actions are being carried out. For example, active vulnerability scanning or network scanning is not done against a production network. This is also mentioned in [7] under step number 9, where scanning of non-production environment is mentioned. In this way, we avoid the risk of improper error handling of the SCADA components when subjected to various test packets generated by conventional network mapping and vulnerability identification tools. After the network inventory data and list of vulnerabilities are gathered, they are checked for consistency and accuracy. This will require manual inspection of each item in the list and cross checking with the CVE database at https://cve.mitre.org. Further details about the identified vulnerability can be found at that website along with links to other useful websites that can help us narrow down and confirm that the vulnerability is not a false positive.

TABLE I. RECOMMENDED ACTION FOR ICS SECURITY ASSESSMENT

To Be Identified	Usual IT Action	Suggested ICS Actions
Hosts, nodes, and networks	Ping sweep (e.g., nmap)	• Examine router configuration files or route tables • Perform physical verification (chasing wires) • Conduct passive network listening or use intrusion detection (e.g., snort) on the network • Specify a subset of IP addresses to be programmatically scanned
Services	Port scan (e.g., nmap)	• Do local port verification (e.g., netstat) • Scan a duplicate, development, or test system on a non-production network
Vulnerabilities within a service	Vulnerability scan (e.g., nessus)	• Perform local banner grabbing with version lookup in Common Vulnerabilities and Exposures (CVE) • Scan a duplicate, development, or test system on a non-production network

V. WHY FRAGILITY IS MORE RELEVANT THAN RISK

ISA-99 defines risk as "an expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence" [11]. A security incident is then defined as a threat that exploits a specific vulnerability at a point in time. So risk can be viewed as tied to an event that may or may not happen depending on future behavior of potential attackers [12]. Unfortunately this risk may be exaggerated by security researchers and vendors of security product or downplayed by asset owners [12].

Langner in [12] argued that a control system engineer or a stakeholder in an automated technical process care more about not losing control over reliability and maintainability of an installation that is growing in cyber complexity. Therefore the concepts that would be of interest to the control system engineer and asset owner are cyber fragility, which is not desirable, and cyber robustness, which is desirable.

This is of course quite different from the conventional view that requires the presence of threats that might exploit an existing vulnerability, that might cause a certain degree of impact, before risk is deemed as being at a certain value that may or not require a countermeasure depending on the accepted risk level.

VI. FACTORS THAT MAY CAUSE CYBER FRAGILITY

Cyber fragility is defined as "the deficient ability of an automated process to withstand variations of normal conditions even when variation is within the limits of typical operating environment characteristics" [12]. As an example, a process controller that shuts down when a patch is applied to a server that requires a reboot of the server. In this case, the cause of cyber fragility is benign in nature and initiated by a friendly party (the system administrator).

The second problem that can cause cyber fragility is sensitivity to cyber noise [12]. In fact some of the recommended actions listed in Table 1 above is to avoid the problem of cyber sensitivity where ICS devices reacts abnormally when subjected to a network scan (ping scan, port scan, TCP SYN scan, etc.)

The third problem stems from the fact that in today's control system installations there are other systems in the control network that have the means to change setpoints, ladder logic, firmware or even force outputs via legitimate commands [12]. If we add in the worst case scenario of a threat agent (attacker or malware) inserting itself into the mix then we have a complete list all possible parties that may affect change (either desirable or not) to the controlled process.

VII. MAKING SCADA SYSTEMS MORE ROBUST WILL INCREASE SECURITY

Cyber "robustness is the ability to continue normal operations despite contingencies, the ability to withstand changes in procedure or circumstance, and the ability to cope with variations in the operating environment with minimal or no damage, alteration, or loss of functionality" [12].

There are three important principles that can increase cyber robustness especially when they are combined in the same system. The first principle is blocking invalid input so that the chance for invalid output is reduced [12]. This principle has a corollary in the web application security arena: "*It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application*" [13]. Other strategies include reducing network exposure and limiting user access.

The second principle is to limit the transfer function range. This means even if invalid input is entered into the system, the resulting output is not invalid. This principle can be implemented by hardening the system; reducing or eliminating unused software and services; controlling code execution and preventing configuration tampering [12].

The third principle is to block invalid output in process behavior by having alarms and monitors that alert the operator before the physical process is affected [12].

VIII. OTHER STRATEGIES TO INCREASE ROBUSTNESS AND SECURITY

NIST SP800-82 recommends that the ICS network be separated from the corporate network [9]. Any connections between the two should be minimal and only through a firewall and a demilitarized zone (DMZ). One security mechanism to connect the two networks is through a unidirectional gateway or data diode [14].

ISA standard 99 (ISA-99) proposes to divide functional areas of an industrial control system (ICS) into different security levels and recommends separating these areas into "zones". This strategy is referred to as another aspect of "defense in depth" approach where the network is segmented into "security enclaves" [14]. An enclave is defined as "a closed group of assets similar to the functional 'zone and conduit' model supported by ISA-99" [15]. The security enclave is made secure by placing firewalls, intrusion detection and prevention systems where applicable at each demarcation areas. Communication between security enclaves is only allowed and possible via pathways called network "conduits". Depending on security requirements, two popular security technologies can be used inside the conduits: firewalls and Virtual Private Networks (VPNs) [16].

IX. CONCLUSION

Standard vulnerability assessment action steps must be modified and adapted for use in ICS or SCADA network environment due to the fragility of the ICS protocol implementation and to prevent abnormal behavior of the system under assessment. In addition to performing vulnerability assessment, three principles to increase the cyber robustness of ICS network were discussed [12]. These principles should be implemented in combination to increase their effectiveness. Finally, the strategy of implementing zones and conduits (or security enclave and pathways) is recommended in support of the defense in depth philosophy of cyber security.

REFERENCES

[1] Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, Adam Hahn , Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2 Final Public Draft, 2015, pp. 10-39.

[2] Tyson Macaulay, Bryan Singer, Cybersecurity for Industrial Control Systems, CRC Press, 2012, p. 54.

[3] Bill Miller, David C. Rowe, A Survey of SCADA and Critical Infrastructure Incidents, ACM, 2012, pp. 2-4.

[4] The US Industrial Control Systems Cyber Emergency Response Team, ICS-CERT, Year in Review 2013, p. 16.

[5] ICS-CERT Monitor September 2014 – February 2015, National Cybersecurity And Communications Integration Center, pp. 1-2.

[6] Homeland Security, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, 2009.

[7] U.S. Department of Energy, Infrastructure Security and Energy Restoration Committee, 21 Steps to Improve Cyber Security of SCADA Networks, 2007.

[8] Manunta, G., "What is security?", Security Journal. 12, 1999, pp. 57-66.

[9] Chris McNab, Network Security Assessment, 2nd Edition, O'Reilly 2007, p. 4.

[10] Keith Stouffer, Joe Falco, Karen Scarfone, Guide to Industrial Control Systems (ICS) Security, 2011, pp. 49,56-59.

[11] International Society of Automation (ISA), Security for Industrial Automation and Control Systems Part 1:Terminology, Concepts, and Models, ANSI/ISA-99.00.01-2007, 2007, p. 17.

[12] Ralph Langner, Robust Control System Networks, Momentum Press, 2012, pp. 3-45.

[13] Open Web Application Security Project, Input Validation Cheat Sheet, https://www.owasp.org/index.php/Input_Validation_Cheat_Sheet, 2014

[14] Hamid Okhravi, Fredrick T. Sheldon, Data Diode in Support of Trustworthy Cyber Infrastructure, ACM, 2010, pp. 1-4.

[15] Eric D. Knapp, Industrial Network Security, Syngress, 2011, pp. 17-26.

[16] Eric Byres, Using ANSI/ISA-99 Standards to Improve Control System Security, Tofino Security White Paper, 2012, p. 3.