Modern Applied Science; Vol. 11, No. 6; 2017
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

Industrial Network Security – A Critical Review

Omar Salim Kidege[1] & Stanislaw Paul Maj[2]

[1] Orxy Gtl, Doha, Qatar

[2] Engineering Institute of Technology, Western Australia

Correspondence: Stanislaw Paul Maj, Associate Dean (Research), Engineering Institute of Technology, 1031 Wellington St., West Perth, Western Australia, 6005. Tel: 1300-138-522. E-mail: paulm@eit.edu.au

Received: March 26, 2017 Accepted: April 13, 2017 Online Published: April 17, 2017

doi:10.5539/mas.v11n6p24 URL: https://doi.org/10.5539/mas.v11n6p24

Abstract

In advanced societies all aspects of commerce and industry are now based on networked IT systems. Failures of these systems have the potential to be extremely disruptive. The term Critical Infrastructure (CI) is used to define systems (private and public) considered vital to national interests whose interruption would have a debilitating effect on society. It is recognized cyber security threats to CIs range from malicious to state sponsored. The threats are typically continuous and evolving in sophistication. This paper is primarily focused on Process Control Networks (PCNs). PCNs are used as the basis of industrial process control in a wide range of applications (manufacturing, oil and gas, water etc.). Given the importance of this industrial sector there are a range of guidelines considered to be exemplars of best practice. However given the constantly evolving sophistication of hackers the true measure of security is penetration testing – not something that is practical in industrial systems.

Keywords: Cyber security, Critical Infrastructure, Process Control Networks

1. Introduction

1.1 Critical Infrastructure

Modern society is dependent on systems called Critical Infrastructure. There are several definitions of CI such as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, national health or safety, or any combination of those matters*.(DCSINT H., 2006)". Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government (Government C, 2015). The nation's critical infrastructure provides the essential services that serve as the backbone of an economy. CI may be further subdivided as follows:

1. Physical – Physical assets may include both tangible property (e.g., facilities', components, real estate, animals, and products) and the intangible (e.g., information). Physical protection becomes an even more difficult task when one considers that 85% of the nation's critical infrastructures are not federally owned. Proper protection of physical assets requires cooperation between all levels of the government and within the private sector.

2. Human – Human assets include both the employees to be protected and the personnel who may present an insider threat (e.g., due to privileged access to control systems, operations, and sensitive area and information). Those individuals who are identified as critical require protection as well as duplication of knowledge and authority.

3. Cyber – Cyber assets include the information hardware, software, data, and the networks that serve the functioning and operation of the asset. Damage to our electronic and computer networks would cause widespread disruption and damage, including casualties. Cyber networks link the United States energy, financial and physical securities infrastructures (DCSINT H., 2006)

1.2 Industrial Control Systems

Process Control Networks (PCNs) are networks that mostly consist of real-time industrial process control systems (PCSs) used to centrally monitor and (over the local network) control remote or local industrial

equipment such as motors, valves, pumps, relays, etc. PCNs are used in all kinds of (production) environments. Examples of these environments include chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, traffic signal management and water purification and distribution infrastructure (Alvaro A. C., 2008). Process Control Systems are also referred to as Supervisory Control and Data Acquisition (SCADA) systems or Distributed Control Systems (DCS) (Australian Gov., Nov 2016). SCADA, or Supervisory Control and Data Acquisition, is just one specific piece of an industrial network, separate from the control systems themselves, which should be referred to as Industrial Control Systems (ICS), Distributed Control Systems (DCS), or Process Control Systems (PCS). Each area has its own physical and logical security considerations, and each has its own policies and concerns (Eric K., 2011). Control systems are computer-based systems that *monitor* and *control* physical processes. These systems represent a wide variety of networked information technology (IT) systems connected to the physical world. Depending on the application, these control systems are also called Process Control Systems (PCS), Supervisory Control and Data Acquisition (SCADA) systems (in industrial control or in the control of the critical infrastructures), or Cyber-Physical Systems (CPS) (to refer to embedded sensor and actuator networks). Control systems are usually composed of a set of networked agents, consisting of: sensors, actuators, control processing units, and communication devices. Most industrial control systems have a hierarchical structure (Alvaro A. C., 2008).

1.3 Cyber Security Threats

In the USA the President's Commission on Critical Infrastructure Protection (PCCIP) defined critical infrastructure as *"a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services"* (W.D.Wilde and M.J.Warren, 2008). According to Lean E Panetta (Former US secretary of defense) *"A Cyber-attack perpetrated by nation or violent extremist group could be as destructive as the terrorist attack in 9/11'* (Garamone J., 2012). Some of the world's biggest companies have also been victims of cyber-attacks. In August 2012, Saudi Aramco, the Gulf kingdom's national oil producer, reported an attack that damaged 30,000 computers on its network (Garamone J., 2012). As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems—energy production, water, gas, and other vital systems—become more important, and heavily mandated (Eric K., 2011). To evaluate the degree of vulnerability of cyber threats to Industrial Control Systems penetration tests were performed on approximately 100 North American electric power generation facilities, resulting in more than 38,000 security warning and vulnerabilities which were then analyzed to help identify common attack vectors and, ultimately, to help improve the security of these critical systems against cyber-attack (Eric K., 2011). The results suggested a security climate that was lagging behind other industries (Eric K., 2011). To assist in 'hardening' Process Control Networks vendors have provided a wide range of guidelines for implementing network security measures (Tino H., @2012). This paper is an analysis of these guidelines.

2. Method

Guidelines are designed to address system vulnerabilities. Identifying these vulnerabilities may then be used to evaluate vendor guidelines. The top ten of vulnerabilities for control networks are (Security D.H., 2008):

1. Inadequate policies, procedures and culture governing control system security.
2. Poorly designed PCNs that fail to compartmentalize communication connectivity fail to employ sufficient "defense-in-depth" mechanisms, fail to restrict "trusted access" to the control system network, that rely on "security through obscurity" as a security mechanism.
3. Badly configured operating systems and embedded devices that allow unused features and functions to be exploited; untimely (or impossible) implementation of software and firmware patches; inadequate or impossible (refer to example with robotic arm) testing of patches prior to implementation.
4. Use of inappropriate or inadequately secured wireless communication.
5. Use of non-dedicated communication channels for command and control and non-deterministic communication such as Internet-based PCNs. A lack of adequate authentication of control system communication-protocol traffic.
6. Lack of mechanisms to detect and restrict administrative or maintenance access to control system components; inadequate identification and control of modems installed to facilitate remote access; poor password standards and maintenance practices; limited use of VPN configurations in control system networks.
7. Lack of quick and easy tools to detect and report on anomalous or inappropriate activity among the

volumes of appropriate control system traffic.

8. Dual use of critical control system low-bandwidth network paths for noncritical traffic or unauthorized traffic.
9. Lack of appropriate boundary checks in control systems that could lead to "buffer overflow" failures in the control system software itself.
10. Lack of appropriate change management or change control on control system software and patches.

In addition to the above security threats may be not only external, but internally based (Security D.H., 2008).

3. Results

The four main international vendors of industrial process control systems are Yokogawa, Honeywell, Siemens and Schneider Electric. Guidelines provided by each of these vendors were analyzed (table 1).

Table 1. Analysis of Vendor guidelines

Vendor	Cyber Security Guidelines
Yokogawa	1. Identifying what systems need to be protected, 2. Separating the systems logically into functional groups, 3. Implementing a defense-in-depth strategy around each system, and 4. Controlling access into and between each group. 5. Policies 6. Procedures 7. Physical Security 8. Network Security 9. Host Based Security
Honeywell	1. Vulnerability assessment 2. Threat assessment 3. Risk analysis 4. Cyber security training 5. Development of security policies and procedures 6. Implementation of security Technology Defense in Depth 7. Global threat intelligence 8. Incident detection and remediation 9. Timely response to the changing threat landscape 10. Training and awareness
Siemens	1. Physical security 2. Policies, procedures and training 3. Security cells and DMZ 4. Firewalls and VPN 5. System Hardening 6. Preventing wide range of attack 7. Malware detection and prevention
Schneider Electric /Invensys	1. Assess Critical Infrastructure vulnerabilities to cyber or physical attacks. 2. Develop plans to eliminate significant vulnerabilities. 3. Propose systems for identifying and preventing attempted major attacks. 4. Develop plans for alerting, containing and rebuffing attacks in progress. 5. Rapidly reconstitute minimum essential capabilities in the aftermath of an attack. 6. Coordination among private and public CIs protection (Interdependency) 7. Network management system

From table 1 it can be seen that there are common elements but of themselves represent only guidelines. In summary CIs PCNs security can be archived by following below recommendations:

- Critical Infrastructures threats and vulnerabilities analysis to cyber or physical attacks to be done.
- Create strategy to remove major vulnerabilities.

- Suggest systems for pinpointing and stopping attempted significant attacks.
- Create action plans of self-healing if system is attacked
- Vendors of the CIs PCNs must be part of the CERT (Computer Emergency Response Team)
- Defense in depth strategy to be made mandatory for all CIs
- Policies and procedures
- Uniform government regulations and standards to be applied by all CIs PCNs vendors

These are used to inform Standard Operating Procedures which in turn define operational practices. Operational practices considered essential are (Invensys, 2012):

- Always apply and maintain the latest Invensys-authorized Operating System (OS) and application patches.
- Always use current anti-virus definitions
- Update authorized application software
- Enable Network / Intrusion Prevention System
- Do not use a USB stick unless it has been scanned and confirmed that is free of problems with *dat* file.
- Harden Servers and Workstations. Hardening Non-DCS assets is a requirement and typically will not have a negative effect on the DCS. Hardening DCS assets may be performed and will vary from Non-DCS assets hardening.
- Change defaults "admin" passwords.
- Control user rights
- Always implement Backup and Restoration
- Take inventory of network assets
- Use physical network isolation when possible
- Use logical network segmentation (secure zones) when possible with restrict Firewall Rules
- Enable Firewall logging
- Use Network Management System (NMS)
- Don't click links or files that aren't verified
- Create incident response plan

4. Discussion

One of the main problems with Cyber Security is that the threats are constantly evolving in frequency and sophistication (Artur A., 2014) . Whilst guidelines may be adhered to, informed by best practices standard operating procedures it can be concluded that threats may still exist in the real world of CIs PCNs. Security experts agree that, given adequate time and resources, any system – even hardened, relatively segregated, industrial control systems – can be penetrated by determined external hackers or careless or disgruntled employees. However, clearly, there are ways to reduce the risk to an acceptable level (as low as reasonably practical) and to do so without compromising the basic functionality of the system (Arc AG., 2014).

One of the major drawbacks is that none of the major vendors recommend Intrusion test of the PCN. Performing network penetration testing on Industrial Control Systems (ICS) should not be taken lightly. There are many things that can go wrong. These systems were designed and built to control and automate some real world process or equipment. Given the wrong instructions, they could perform an incorrect action causing waste, equipment damage, injury, or even deaths (Duggan, David P., 2005).

References

Artur, A. (2014). Legal Aspect of Cyber Security. *Legal Aspect of Cyber Security*, 1-70.

Government, C. (2015, 12 01). Public Safety. *Critical Infrustructure*, 2-5.

Alvaro, A. C. S. A. (2008, 07 15). Research Challenges for the Security of Control Systems. 1-10.

Arc, A. G. (2014). Yokogawa's Comprehensive Lifecycle. *Approach to Process Control System Cyber -Security*, 1-20.

Australian, Gov. (Nov 2016). Critical Infrustructure Protection. In NOREA, *Process Control System and*

Network Security (p. 1). Pearth: NOREA.

DCSINT, H. I. (2006). Critical Infrastructure. *Threats and Terrorism*, 3-80.

Duggan, D. P. (2005). Penetration Testing of Industrial Control Systems. 1-7.

Egan, M. M. J. (2007, March). Anticipating Future Vulnerability:Defining Characteristics of Increasingly Critical Infrastructure-like Systems. *Contingency and Crisis Management*, *15*(1), 4-17.

Eric, A. M. L. (2003). Critical Infrastructure Protection in The Netherlands. In U. E. Gattiker (Ed.), *EICAR Conference Best Paper Proceedings 2003* (pp. 1-19). Netherlands: EICAR Denmark c/o TIM-World ApS.

Eric, K. (2011). *Industrial Network Securing Critical Infrastructure*. (J. Broad, Ed.) London: Elsevier.

European, C. (2013, 8 28). COMMISSION STAFF WORKING DOCUMENT. *on a new approach to the European Programme for Critical Infrastructure Protection*, 1-17.

Garamone, J. (2012, October 11). Panetta Spells Out DOD Roles in Cyberdefense. *DOD News*, p. 1.

Invensys. (2012). CISP CYBER SECURITY BEST PRACTICES. *CISP CYBER SECURITY BEST PRACTICES*, 2.

John, M. P. P. (2004, oct 1). Critical Infrastructure and Key Assets. *Definition and Identification*, 1-19.

O'Rourke, T. D. (2007). Spring 2007. (T. R. Briggs, Ed.) *Critical Infrastructure,Interdependencies,and Resilience*, 1-8.

Richard, L., & Church, M. P. (2008). Identifying Critical Infrustructure. *The Median and Covering Facility Interdiction Problems, 94*(3), 491-502.

Rosslin, J. R., M. K. C. S. S. C. H. (2013). International Journal of Control and Automation. *Common Threats and Vulnerabilities of Critical*, 1-6.

Shenoi, S. (2017). International Journal of critical Infrustructure Protection. 1.

Security, D. H. (2008). Introduction to Control Systems, Security for IT Professionals.

Security, U. D. (2016, October 14). Critical Infrusture Security. *What is Critical Infrustructure*, 3.

Tino, H. (2012, 02 09). Head of Marketing & Promotion SIMATIC HMI. *Industrial Security*, 38.

Wilde, W. D., & Warren, M. J. (2008). Australian Information Warfare and Security. *Visualisation of Critical Infrastructure Failure*, 48.

Wangdi, Y. V. D. (2011, June). Critical Infrastructure Cyber Threat – A Case Study. *IJCSNS International Journal of Computer Science and Network S 20 ecurity, 11*(6), *June 2011*, 4.

Warren, M. J. W. W. (2008). Visualisation of Critical Infrastructure Failure. *Australian Information Warfare and Security Confrence* (p. 63). Australia: Edith Cowan University Resaerch Online.

Wikipedia. (2006). Critical Infrustructure. *European Program For Critical Infrustructure Protection*.

Yokogawa, B. (2014). Plant Network Security. *How to defend your plant against threat 2014*, 63.