TOWARDS CYBER SECURED SCADA SYSTEMS

Hasan Dag[1], Alen Bohcelyan[2], Isil Yenidogan[1]
[1]Kadir Has University, Management Information Systems Department, Istanbul, Turkey
[2]UITSEC, Istanbul, Turkey
Corresponding author: Hasan Dag, e-mail: hasan.dag@khas.edu.tr

REFERENCE NO

ELEC-04

Keywords:
Smart Grid, Cyber Security, SCADA Systems

ABSTRACT

Cybersecurity notion has largely been related to, or has been perceived to be relevant to, the computer systems connected to Internet up to the recent years. However, its effect on critical infrastructures, such as those in electrical power systems, gas and oil, and communication systems etc., has only recently began to be studied. A recent cybersecurity research interest in the SCADA (Supervisory Control and Data Acquisition) systems, which is a special case of industrial control systems (ICS), is now gaining momentum. This interest is highly important and needs be widened especially as the word Smart "Things" (for example Smart Grid) applications and the use of the Internet of Things (IoT) devices become prevalent. We propose a systematic approach towards the assessment of cyber security related vulnerabilities for a given SCADA system, which includes: risk-value related to the vulnerabilities and a prioritized list of precautions to lower the risks mentioned.

1. INTRODUCTION

Cybersecurity notion have largely been related to, or have been perceived to be relevant to, the computer systems connected to Internet up to the recent years. However, its effect on critical infrastructures, such as those in electrical power systems, gas and oil, and communication systems etc., has only recently began to be studied. National Homeland Security (NHS) of USA has just recently released a detailed report on common cybersecurity vulnerabilities [1].

A recent cybersecurity research interest in the SCADA (Supervisory Control and Data Acquisition) systems, which is a special case of industrial control systems (ICS), is now gaining momentum [2]. This interest is highly important and needs be widened especially as the Smart "Things" (for example Smart Grid) applications and the use of the Internet of Things (IoT) devices become prevalent. Since the word "Smart" usually refers to the connectedness and the ability to remotely control, manage, and to exchange data, cybersecurity becomes more important than ever before.

This work will be generally devoted to the SCADA system security, but particularly that of electrical power systems rather than all types of SCADA systems in ICS [3]. This is due the fact that, electrical power systems are already highly interconnected extending to continents. Thus, any disruption in the continuity of electricity as a result of a cyberattack may lead to catastrophic results not only on the event location but also on all the interconnected countries as well. The geographical distribution of assets to very large areas and the need of communications among those devices for the control and management purposes make these systems more prone to attacks. Any communication channel with remote connection capability is prone to cyberattacks.

SCADA networks are made up of operational technologies (OT) and control devices integrated with information technologies (IT). OTs usually contain sensors, actuators, remote terminal units (RTUs), and computers etc., which are proprietary hardware and have their own communication protocols [4]. In addition to OT and IT, the SCADA networks also include the necessary applications to provide indispensable services, such as electricity, gas, and oil to customers, hence, they are considered to be national infrastructures. To the contrary to its importance as national infrastructures, the deployed devices generally remain in operation for more than 10 years with little or no modification [5]. This fact makes them more vulnerable to cyberattacks.

The main goal of SCADA systems have been the functionality, hence, not much attention has been paid to the security, especially cybersecurity. This weakness makes SCADA systems potentially vulnerable to all types of cyberattacks by both individuals and groups, or event countries hostile one another [6-7].

This paper proposes a model to identify those devices, assign risk values to each, and finally a workflow model to eliminate / lower the risks that may occur due to a cyberattack through the SCADA systems, especially those that are used in Smart Grids [2] and that are more prone to cyberattacks.

2. BACKGROUND

The last two decades witnessed a tremendous growth in Internet and services thereafter. This, however, has not come cheap. It brought together cybersecurity challenges for business and government organizations trying to protect their data and network against sophisticated, well-organized and most-likely well-financed hackers [8].

According to Juniper's research report, the cost of data breaches will reach to $2.1 trillion globally by 2019. This is almost four times the estimated cost of breaches in 2015 and it is due to the rapid digitization of consumers' lives and enterprise records [9]. The same research company also reports that, "*the majority of these breaches will come from existing IT and network infrastructure*" [10].

Smart Grid devices are made up of significantly by the Programmable Logic Controllers (PLC), sensors, switches, circuit breakers, capacitors, and so on. Most of these devices use different versions of firmware and they could be easily exploited by hackers since they are not designed to be secure in the first place, rather, they are designed to be functional. If those devices, which run on old versions of respective firmware or themselves are old, not replaced soon, they would put the system at hand into danger of being hacked causing catastrophic damages both economic and social.

Creey et al. [11] presented an overview of the security vulnerabilities industrial control networks and pointed out the vulnerabilities exist despite wide spread of both standards and the recommended practices published by organizations such as IEC, IEEE, and ISA.

Liu et. al. introduced a procedure for cyber-based intrusion attack on a power system network and they concluded that there is need for a cybersecurity framework for critical infrastructure [6-7]. Two scenarios are studied: one from outside the substation-level networks and one from within the substation networks. For each scenario, they run power flow for the IEEE 30-bus system to assess the vulnerabilities.

All types of ICS, especially those that are regarded as part of national infrastructure, are likely to be attacked either by individuals, groups, or even by countries for variety of reasons: whether it be money, espionage, or intimidation. The threat becomes more real as more and more IoT and "Smart" termed devices are being used in ICS. Any downtime of those ICS in national infrastructure category or major component compromises within them can result in catastrophic consequences both economic and social [3]. To this end, we propose a methodology to first assess the vulnerabilities of components in a SCADA system, then assign a risk-value to each component, and develop a deep learning based automated system to detect and prevents attacks.

4. THE PROPOSED MODEL FOR VULNERABILITY DETECTION AND RISK VALUATION

In this section we provide the details of the proposed methodology. For a general framework for SCADA the Purdue Model describing ICS can be used [12]. From the aforementioned model, there are four main levels in the model, each of which has different types of security vulnerabilities. The model's levels are:

a) Sensor network,
b) PLC network,
c) SCADA system, and
d) Management (application software) network.

The threats to each of these levels can arise from variety of sources. Such that,

i) from a person (whether a personal for the SCADA system or a personal of a contractor doing some work inside) using some sort of external devices, such as USB sticks, which may include rootkits, infected files, and macros to compromise the system at hand.
ii) from Internet, which can be used for all sorts of attacks, such as denial of service (DoS) attacks.
iii) from remote sources such as modem, Bluetooth, Wi-Fi, etc. Those sources can be used to attack the system.

4.1. Risk value model for SCADA components

Our proposed model includes four main steps:

a) Awareness creation
b) Internal and external personal handling
c) Continuous development of Defence in Depth
d) Reporting

4.1.1. *Awareness creation*

This step includes the creation of security awareness from both management and operational personal. It is widely understood fact that about 80% of security breaches arise from the internal personal. Not only the security related awareness, the economic and social consequences of the vulnerabilities need be taught to whole personal. Without halting the SCADA system, the operation personal can be trained on simulators by all types of attacks, vulnerability, and intrusions and their effect on their system. Then all personal in turn can be trained on the seriousness of cyberattacks. Involving both management and operational personal seem to be more successful. The training are recorded and each new employee then uses these videos. The videos, however, upgraded quite frequently to reflect new types of attacks, viruses and new scenarios the attackers may develop.

4.1.2. *Internal and external personal handling*

For a secure operation of a SCADA system the following steps are needed for all types of personal related to the system and the network they are permitted to operate on.

- Separation of operational and management networks (managerial decision)
- development of authorization rules for personal to operational and management level networks
- development of special and strict policies and procedures for contractors and sub-contractors
- conducting periodic and frequent security audits and writing security reporting
- development of policies for the use of the external devices, such as USBs and Laptops, to be connected to SCADA system
- development of policies for application and operational software installation and/or upgrade.

Once the above policies, procedures are developed an extensive re-training of the personal to be done. Actually, most of these policies and procedures need be developed by the related personal with professionals in both academia and industry.

4.1.3. *Continuous development of Defence in Depth*

This is probably the most important and technically more advanced part of the whole cybersecurity procedure.

1. *Determination of all types of devices with communication capability, which can be accessed or through which other components can be reached. The output of this step is a list of components, which are potentially vulnerable to breaches on a SCADA system.*

2. *Once on all of the components, especially those with communication channels, of a SCADA systems are determined, a risk value will be assigned to each one based on effect/damage level to occur should the intrusion originate from that particular component [2]. To be able to assign a risk-value to a particular device we run two types of simulations and based on the simulation results we assign a risk value. The simulations, for the time being, are:*
   a. *A steady state power flow: For example, if attack causes a sudden/unexpected load change*
   b. *A transient stability analysis. Again, in case of a sudden/unexpected load change, in case of any suspicious change on settings of generators, transformer, regulators etc.*
3. *We also propose as part of this Defence in Depth procedure an automatic-deep-learning based malware and intrusion detection agent. This agent gathers data while wondering through and scanning communicating channels, for example the ports, OS and apps, of the components found in step 1 of this procedure and develops a detection model incrementally. The output of this agent a list of potential backdoors for intrusions, a list of potentially dangerous apps, and version of OS with a suggestion when to replace/upgrade them.*

4.1.4 *Reporting*

Regular reporting of vulnerabilities for a successful cyber defence is a must. The reports need to include all details pertaining the components of each level of model proposed by Purdue [12]. A report by SANS institute [13] and numerous paper have clearly identified the controls and the details to be included in a security reporting document.

4. CONCLUSIONS

SCADA systems are characteristically different from any IT systems due to the requirements of functionality-first, uptimes, reliability, and durability etc. Thus, a conventional IT security procedure is not applicable to SCADA system. On the other hand, SCADA systems includes many components such as sensors, PLCs, RTUs, switches, gears, and instrumentation devices, most of which are quite old and runs on proprietary software. Thus, a totally new approach and methodology need be developed for the cybersecurity of the SCADA systems.

We have developed a four-staged methodology for the SCADA systems' cybersecurity. The first two steps are repeated for each case with the contribution of the management of SCADA owner. A software is developed for the first part of the third stage and tested on a couple of systems. Thus, this paper reports the followings for a more secured SCADA system:

- A software and work flow model are proposed to assess cyber security in SCADA systems in general, in power systems in specific.
- A systematic approach/model towards the assessment of cyber security related vulnerabilities of a given SCADA system, which includes:
  - Risk-value assignment to components of a SCADA system
  - A prioritized list of precautions to lower the risks and improve system security.

The developed software tested on some industrial control systems and initial results are quite promising. The development continues to make the software more automatic.

Nomenclature

DoS	Denial of Service
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IoT	Internet of Things
IT	Information Technologies
NHS	National Homeland Security
OT	Operation Technologies
PLC	Programmable Logic Unit
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

REFERENCES

[1] Nelson, T., and Chaffin, M., Common cybersecurity vulnerabilities in industrial control systems, *Control Systems Security Program. Washington DC: Department of Homeland Security (DHS), National Cyber Security Division*, 2011.

[2] Jarmakiewicz, J., Parobczak, K. and Maślanka, K., Cybersecurity protection for power grid control infrastructures. *Int. Journal of Critical Infrastructure Protection*, 18, 2017. pp.20-33.

[3] Nazir, S., Patel, S. and Patel, D., Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, 70, 2017. pp. 436-454.

[4] Cook, A., Helge J., Richard S., and Leandros, M., The industrial control system cyber defence triage process, *Computers & Security*, 70, 2017, pp.467-481.

[5] Galloway B, Hancke G. P., *Introduction to industrial control networks*. IEEE Communication Survey and Tutorials 15(2), 2011, pp. 860–880.

[6] Ten, C. W., Liu, C. C., and Govindarasu, M. Cyber-vulnerability of power grid monitoring and control systems. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, 2008, pp. 43-47.

[7] Liu, C. C., Ten, C. W. and Govindarasu, M., Cybersecurity of SCADA systems: Vulnerability assessment and mitigation. In Power Systems Conference and Exposition, 2009. pp. 1-3.

[8] Wechsler, P., Cybersecurity, *SAGE Business Researcher*, 2016, businessresearcher.sagepub.com/sbr-1775-98146-2715384.

[9] Whitepaper by Juniper, Cybercrime & The Internet of Threats, 2017.

[10] Research report by Juniper, The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, 2017.

[11] Creery, A., and Byres, E. J., Industrial cybersecurity for power system and SCADA networks, Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual. IEEE, 2005.

[12] Obregon, L., Secure architecture for industrial control systems, *SANS Institute InfoSec Reading Room*, 2015.

[13] 20 Critical Security Controls for effective cyber defence – *SANS institute* – Spring 2013.