Research Framework for SCADA Security Center of Excellence (COE)

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

Abstract—**This paper is concerned with the research framework for SCADA security center of excellence (COE). The trend of connecting SCADA systems to the Internet presents challenges for the security team to ensure the whole system is secure. One of the key challenges is how to effectively keep abreast with security developments and risks affecting SCADA systems due to newly discovered vulnerabilities and increasing threat actor motivations. To address these challenges, this paper seeks to propose a SCADA security center of excellence (COE) research framework that can produce outputs with practical applications. The proposed framework is a combination of repository and coach models gathered from other center of excellence reference models from IT as well as non-IT industries. Using this framework, relevant applied research can be conducted to produce output that can be immediately used by stakeholders to reduce the SCADA security risks and improve operational resilience.**

Keywords-component; ICS; SCADA; cyber threat; security vulnerability; center of excellence, research framework; mitigation

I. INTRODUCTION

There is a reliance on infrastructures that provide utilities and services vital to people's safety, security, health, and economic wellbeing in today's world. These infrastructures need to be properly secured and kept safe from both physical and cyber attackers. The term SCADA (Supervisory Control and Data Acquisition) is sometimes used in literature to refer to the systems that control and manage critical processes found in these infrastructures. Other terms used include Industrial Control Systems (ICS) and Distributed Control Systems (DCS). These systems can be very complex and are threatened by the same threat agents that affect IT assets [1]. There is therefore a need to research SCADA security from an academic as well as practitioner point of view.

There were 295 incidents that involved critical infrastructures reported to ICS-CERT (Industrial Control Systems Cybersecurity Emergency Response Team) in the United States between October 2014 to September 2015 [2]. According to the report, the critical manufacturing sector reported the majority of the incidents which mostly involved widespread spear-phishing attack [2]. The report went on to mention that the attacks were facilitated by "insufficiently architected networks" [2].

There is clearly a need to define the scope and focus of SCADA center of excellence research framework so that the most critical vulnerabilities that could potentially be exploited by attackers is given research priority and also to focus on research to make the system more robust in terms of cyber security.

One definition of a center of excellence is that it is a hybrid entity that provides thought leadership, technical improvement, applications knowledge, education and talent development, implementation support, benchmarking and best practices information, and uniform integration [3].

Frost et al. [4] defined a center of excellence as "an organizational unit that embodies a set of capabilities that has been explicitly recognized by the firm as an important source of value creation, with the intention that these capabilities be leveraged by and/or disseminated to other parts of the firm."

A center of excellence can be defined as having multiple dimensions, one of which is a company division that has expanded knowledge, usually by intercommunication with clients, providers and organizational peers [5].

For the purpose of this paper, the SCADA security center of excellence (COE) is taken to mean an organized group of specialists who are tasked to lead the way to technical excellence in research and development of security techniques for SCADA and control systems in general.

A framework to conduct research on SCADA vulnerability is critical to ensure proper focus and allocation of monetary resources as well as human capital to address the right issues at the right time and according to the right priority.

Establishing a suitable SCADA security framework requires an understanding of the risk in terms of threats, vulnerabilities and potential impact [6]. Therefore, the proposed framework incorporates vulnerability and threat assessment in order to understand the risks.

The term "SCADA" is often used in literature to refer to Industrial Control System (ICS) in general as well as when specifically referring to SCADA systems. This paper shall use this term to refer to any kind of control system including both DCS and SCADA.

II. THE MODELS

The proposed SCADA center of excellence shall be based on two distinct but complementary models [7]:

- The Repository model
- The Coach model

The two models will be explained further in the next sections.

The proposed framework shall address SCADA security research challenges including the following key areas [8]:

1. Improving access control to the SCADA network
2. Improving security inside the SCADA network
3. Improving security management of the SCADA network

The proposed framework shall look at the three research areas and will not focus on just specific problems in isolation, for example, assessing security in a SCADA network or a threat assessment of the latest zero-day vulnerability affecting a SCADA vendor. The idea is to look at an overall research framework with the aim of increasing the dependability, resiliency and robustness of the SCADA network to support its critical processes.

III. The Repository Model

Bookman [7] mentioned about the repository model during discussions on building mobile center of excellence. This paper proposes the same model to be adopted for the SCADA security center of excellence (COE).

The repository model means the COE shall have a repository of SCADA security best practice, SCADA security assessment methodology, and information on applicable security standards, as well as tools and templates ready for usage.

Rieger in [9] listed "Identify Key Stakeholders" as step one in the process of selecting a repository model. It is easy to understand why this step is very important to the success of the repository for the center of excellence.

The benefits of stakeholder analysis can be summarized as follows:

1. Helps to build awareness among the stakeholders and help them understand the goals of the repository
2. Gathers feedback from stakeholders so that their opinions can be used to improve the quality of the repository
3. Builds trust with the stakeholders to ensure their specific needs are being addressed
4. Expands resources in the repository through increased funds and assistance from the stakeholders

The list of stakeholders includes government and regulatory agencies, sector leads from various critical national information infrastructure sectors, universities and institutions of higher learning, SCADA vendors and systems integrators.

As an example, in Malaysia the following agencies can be included in the list of primary stakeholders:

1. National Security Council (*Majlis Keselamatan Negara*)
2. Ministry of Science, Technology and Innovation (MOSTI)
3. Sector leads from relevant critical national information infrastructure sectors (CNII):
   i. Malaysian Communications and Multimedia Commission (MCMC)
   ii. Energy Commission (*Suruhanjaya Tenaga*)
   iii. Ministry of Transport
   iv. National Water Services Commission (*Suruhanjaya Perkhidmatan Air Negara*)

In the Malaysian context, the above list is not exhaustive and can be improved by including local universities, SCADA vendors and system integrators.

The next important step in the repository model selection is needs assessment [9]. This is to ensure a common understanding of needs, goals, opportunities and impediments [9]. The process helps to determine current demand for a repository, specific service needs, management issues, policy development requirements, and content types. Potential problems in recruiting content providers or unique aspects of ingest workflow are likely to be discovered during the systematic needs assessment process [9].

Admittedly, the process steps listed above is not exhaustive but should serve as a good starting point for all SCADA center of excellence repository model creation.

IV. The Coach Model

The Coach model means the SCADA COE shall be a competency center to provide SCADA security expertise guidance and oversight [7], with the aim of helping to secure SCADA system deployment and providing SCADA security decisions as strategic advisor.

In order for the coach model to succeed at being effective in providing expert guidance there is a clear requirement for a proper research framework to produce applicable output that can be readily consumed by the target audience.

It is therefore necessary to introduce the overall research framework next. The proposed framework is adapted from work by Chen et al [10].

V. The General Research Framework

At the very outset, it is crucial that the COE identifies the important categories of information necessary to conduct SCADA security research. It is proposed that the information categories include SCADA technology direction, secure SCADA network architecture, SCADA security and vulnerability assessment, and sector specific SCADA security models.

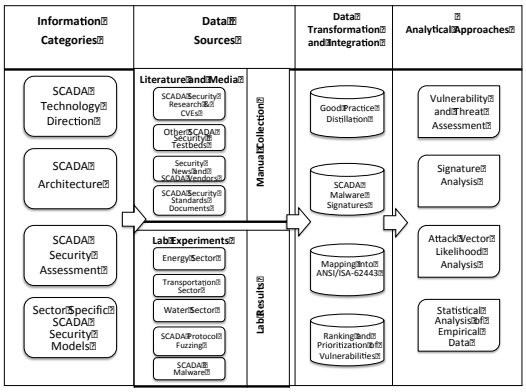
Next, the data sources for each information categories will have to be identified and collected. Data sources can include the literature, media and laboratory experiments. The available literature consists of journals, books and other publication types. Media can consist of newsworthy articles related to SCADA security events and happenings from around the world and across all industries.

Keeping up-to-date with the Common Vulnerabilities and Exposures (CVE) database at https://cve.mitre.org is another valuable source for input. Further details about vulnerabilities can be found at that website along with links to other useful websites that can help expand the knowledge about a particular topic.

Other than that, standards document and publications such as Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 [11], and ISA-99 standard [12] are valuable references.

The next table shows the SCADA Security Research Framework adapted from the work by Chen et al [10].

TABLE I. SCADA SECURITY COE RESEARCH FRAMEWORK[10]



VI. LABORATORY EXPERIMENTS

Laboratory experiments are another source of data for the SCADA center of excellence.

At a minimum it is suggested that laboratory experiments be constructed to model sector specific SCADA environment in order to understand the vulnerabilities and countermeasures for each sector.

Implementing a full-scale SCADA system for the purpose of testing alone can be too costly for most organizations. On the other hand, constructing a simplistic replica of a SCADA system may not give the full picture to the researcher especially when safety systems are omitted from the setup. This may introduce what is termed "the sky is falling" syndrome amongst security researchers when in fact there are other compensating controls which are normally implemented in real-world SCADA installations. One example of the compensating control is the use of safety instrumented systems (SIS) which can be computer based. SIS can include process shutdown systems, fire and gas detection systems and emergency shutdown systems [13]. Finding the right balance between practicality and reasonable accurateness is the challenge.

For standalone experiments it is often worthwhile to conduct SCADA protocol fuzzing and SCADA malware analysis. The motivation is to understand the vulnerabilities or malicious behavior of such threat agents but putting the findings into context requires widening the horizon to include engineering applications such as power industry SCADA environments. A key component often overlooked by security researcher is the safety network that includes the safety instrumented systems (SIS) designed to safeguard the process and bring everything to a fail-safe state before any real damage can happen.

These are some factors that should be considered by the SCADA center of excellence so that research output will be in-tune with priorities of the SCADA engineers, applicable and actionable.

VII. DATA TRANSFORMATION AND INTEGRATION

The data collected from experiments and gathered from literature and media will need to be normalized, transformed and integrated in order to be useful for the next steps.

Examples of data transformation and integration include distilling the data into good practices, SCADA malware signatures, mapping findings to standards like ANSI/ISA-62443, and ranking of discovered vulnerabilities.

During this process it helps to be mindful of the need to apply the research output in the context of real-world SCADA deployment and usage scenarios instead of being purely theoretical in nature.

VIII. ANALYTICAL APPROACHES

The next levels of abstraction to be applied include assessment of vulnerability and threats discovered, performing attack vector likelihood analysis and statistical analysis of empirical datasets.

The analytical approaches should strive to explicate the solutions to the three main research areas mentioned in section II. Ideally they should address three important principles as mentioned by Langner [14] with the aim to increase cyber robustness by combining them in the same system.

The principles mentioned by Langner are:

- blocking invalid input so that the chance for invalid output is reduced [14].
- limiting the chance of invalid output despite having invalid input entering the system [14]
- blocking invalid output from the process behavior [14]

The Institute of Electrical and Electronics Engineers (IEEE) [15] defines robustness as "the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions." A lot of control system failures can be attributed to the absence of robustness [16].

IX. CONCLUSION

A SCADA security center of excellence research framework must be designed such that the research output can be applied in a SCADA network environment found in a real-world installation. In addition to the research framework itself, the repository and coach models for the center of excellence were discussed. These models should be implemented in combination to increase their effectiveness. A few suggestions on the need for data transformation and analytical approaches to address the robustness requirement of SCADA systems were discussed. Finally, there has to be a balance between purely theoretical and practical research output so that the needs of the various stakeholders are met.

REFERENCES

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

[2] ICS-CERT Monitor November 2015 – December 2015, National Cybersecurity And Communications Integration Center, p. 4.

[3] Terence T. Burton, Success Through The Lean Business System Reference Model, McGraw-Hill, 2015, Chapter 6 (online version, no page numbers).

[4] Frost, T.S., Birkinshaw, J.M. and Ensign, P.C., 2002. Centers of excellence in multinational corporations. Strategic Management Journal, 23(11), pp.997-1018.

[5] Reger, G. and Zafrane-Bravo, C.E., 2002. Managerial implications of the research on centers of excellence-a conceptual view. In Engineering Management Conference, 2002. IEMC'02. 2002 IEEE International (Vol. 1, pp. 178-183). IEEE.

[6] Henrik Christiansson and Eric Luiijf, Creating A European Scada Security Testbed – Critical Infrastructure Protection, Springer, 2007 – p. 239

[7] Bookman, A. (2016). Webinar: Building a Successful Mobile Center of Excellence. [online] Propelics. Available at: http://www.propelics.com/resources/webinar-build-successful-mobile-center-excellence/ [Accessed 14 Jul. 2016].

[8] Igure, V.M., Laughter, S.A. and Williams, R.D., 2006. Security issues in SCADA networks. Computers & Security, 25(7), pp.498-506.

[9] Oya Y. Rieger, Key Principles in Assessing Repository Models, D-Lib Magazine, July/August 2007, Volume 13 Number 7/8

[10] Chen, H. (2016). Cybersecurity Research + Education: Hacker Web + AZSecure. [online] Artificial Intelligence Laboratory. Available at: https://ai.arizona.edu/research/cyber [Accessed 14 Jul. 2016].

[11] 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.

[12] 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.

[13] Hauge, S., Lundteigen, M.A., Hokstad, P. and Håbrekke, S., 2010. Reliability prediction method for safety instrumented systems–pds method handbook, 2010 edition. SINTEF report STF50 A, 6031.

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

[15] IEEE, Standard Glossary of Software Engineering Terminology, in IEEE Std 610.12-1990 , 1990 (Rev:2002)

[16] Kube, N 2013, 'Cybersecurity And SCADA In Critical Infrastructure', Pipeline & Gas Journal, 240, 2, pp. 46-47, Business Source Complete, EBSCOhost, viewed 1 September 2016.