Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks

Suhaila Ismail, Elena Sitnikova, Jill Slay

Towards Developing SCADA Systems Security Measures for Critical Infrastructures against Cyber-Terrorist Attacks

Suhaila Ismail, Elena Sitnikova, Jill Slay

Information Assurance Research Group, School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, Australia

suhaila.ismail@unisa.edu.au,
elena.sitnikova@unisa.edu.au, jill.slay@unisa.edu.au

Abstract. Security is essential in protecting confidential data, especially in Supervisory Control and Data Acquisition (SCADA) systems which monitor and control national critical infrastructures, such as energy, water and communications. Security controls are implemented to prevent attacks that could destroy or damage critical infrastructures. Previous critical infrastructure surveys point out the gaps in knowledge, including the lack of coordination between sectors, inadequate exchange of information, less awareness and engagement in government critical infrastructure protection (CIP) programs. Consequently, private sector and government organizations feel less prepared. This paper highlights existing vulnerabilities, provides a list of previous attacks, discusses existing cyber security methodologies and provides a framework aiming to improve security in SCADA systems to protect them against cyber-attacks.

Keywords: Critical Infrastructure, SCADA, Cyber Security, Security Assessment, SCADA vulnerabilities.

1 Introduction

Supervisory Control and Data Acquisition (SCADA) systems are used to monitor and remotely control critical infrastructure (CI) processes, such as electricity transmission, water supply and distribution, gas pipelines, government facilities and power generation plants. SCADA systems facilitate remote access to monitoring of real-time data and execute instructions or commands to remote devices and field devices [29]. As such, SCADA systems are essential and important in sustaining daily activities. Traditionally, SCADA systems were isolated systems that were not connected to or accessed by other networks. Each site or operation had its own SCADA system which originated in the 1960s [26]. Due to the need for shared information between the isolated SCADA systems network and cyber interdependencies that are part of the inescapable computerization and automation of infrastructures, the SCADA systems are now connected as a network. Pressures of modernization, integration, cost, and securi-

adfa, p. 1, 2011.

ty have forced SCADA systems to migrate from closed proprietary systems and networks to commercial off-the-shelf products and hardware, standard network protocols, and shared communications infrastructure [8]. This opens up SCADA systems in terms of security and their vulnerabilities.

According to a 2004 study on the Critical Infrastructure Protection (CIP) Survey of the Worldwide Activities, the main problem was the lack of coordination and inadequate exchange of information [3]. Symantec Corp. reported in the 2011 Critical Infrastructure Protection (CIP) Survey, that there was a decrease in awareness and engagement globally, as measured by the CIP Participation Index. Findings of the survey were organisations less aware, engaged and slightly more ambivalence about government CIP programs and global organizations feel less prepared [23]. The surveys indicated the government's CI plan and controls that protect SCADA systems are implemented by organizations providing the service. However, they are not fully aware of CI planning as a whole. Further discussions throughout the paper could be used to provide better understanding of SCADA systems security. More importantly, the paper provides an insight into developing a framework that can be used to assist critical infrastructure sectors.

The paper is organized as follows. It outlines some of the SCADA systems' vulnerabilities in section 2. Section 3 outlines previous attacks on SCADA systems as well as the impact of the attacks. Section 4 discusses the current security issues specific to SCADA systems, explains existing approaches for security assessments and proposes an initial framework for measuring security for SCADA Systems. Finally, section 5 concludes the entire paper and discusses future research.

2 SCADA Systems Vulnerabilities

The growing demands of connectivity between corporate networks and SCADA systems have created much vulnerability. Private and confidential information is widely accessible to the general public on the Internet, including structural maps networks, network systems configurations and names, etc. By obtaining this information, an intruder can then access the systems and manipulate the SCADA systems [11]. Access control might also be an issue if it is not properly administered. Appropriate skills and expertise as well as level of understanding of the systems security issues are essential. The documented cases show that most attacks originated from disgruntled employees who have the authority to access the systems, and arrange attacks without being easily detected. Another growing concern is the lack of real time monitoring because of the enormous amount of data that is being used in controlling the SCADA systems. Mobile communication systems that are integrated and used with the existing systems also pose a threat, and are quite difficult to consolidate [20]. Due to their vulnerabilities, critical infrastructures can be penetrated through application exploits, backdoor attacks, exploitation of operating systems, unauthorized access, exploitation of systems configurations, tampering, etc.

Cyber-Terrorism in the SCADA Systems context; Cyber-terrorism is defined as the use of Information Communications Technology (ICT) by terrorist groups and agents to promote extremist or aggressive tendencies, usually politically motivated and designed to leave a forceful or catastrophic impact. The perpetrator must use information systems or other electronic means to launch a cyber-attack against critical information infrastructures [28]. Also defined as "non-state actors' use of ICTs to attack and control critical information systems with political motivation and the intent to cause harm and spread fear to people or at least with the anticipation of changing domestic, national or international events" [1].

3 Previous Attacks on SCADA Systems

Table 1 provides a list of previously documented cases of deliberate or undeliberate attacks, or malfunctions of SCADA systems, as well as discusses the methods and the impacts of cyber-attacks. Initially based on [16], the survey has been expanded by further research on more recent cases that have been arranged in chronological order.

ATTACK/ YEAR	ATTACKER	ATTACKED	HOW ATTACK HAPPENED	THE IMPACT OF ATTACKS
Flame (2012)	Unidentified	Iran, Lebanon, Syria, Sudan,	Flame computer virus. Managed to evade detection by 43 different anti-virus, despite its size; 20MB [27]	Stole large quantities of information from various Iranian government agencies, and disrupted oil exports by shutting down oil terminals [27]
Gauss Malware (2012)	Unidentified	Lebanon, Israel, Palestinian, United States, United Arab Emirates	Collect information on infected systems, and steal credentials for banking and social network, email and IM accounts.	The Gauss code includes commands to intercept data required to work with Bank of Beirut, Byblos Bank, and Fransabank [13]
Night Dragon (2011)	Unidentified	Five global energy and oil firms	Using a combination of attacks including social engineering, Trojans and Windows-based exploits.	5 global energy and oil firms companies that operate SCADA were attacked. Operational blueprints were stolen [18]
DUQU (2011)	Unidentified	Iran, Europe	Windows-exploiting code similar to Stuxnet to attack Siemens industrial software [7]	Unidentified
Stuxnet (2010)	Unidentified	Iranian nuclear facility at Natanz. Stuxnet used four 'zero-day vulnerabilities	The worm employs Siemens' default passwords to access Windows operating systems that run WinCC and PCS7 programs.	Stuxnet altered the frequency of the electrical current to the drives causing it to switch between high and low speeds. The centrifuges fail at a higher than normal rate. [9]
Polish Trams (2008)	A teenage boy hacker	Polish Tram Systems	Unauthorized access by adapting a remote control to change the track points	12 people were injured in one derailment
Red October (2007)	Unidentified. Russian used in codes	Diplomatic and government, research institutes, energy nuclear, aerospace	Malware infiltrates computers and smartphones to obtain sensitive documents through email attachment	Infiltrated over 1000 high level government computers. Sensitive information being stolen; 7TB stolen data & 55,000 connection targets across Switzerland, Kazakhstan & Greece [19]

Tehama Colusa Canal (2007)	A former electrical supervisor	Tehama Colusa Canal Authority	Installed unauthorized software on the TCAA's SCADA systems.	Unidentified
Daimler Chrysler (2005)	Unidentified	Manufacturing plants and business	Zotob infected laptop connected to Daimler Chrysler's network	Infected business and industrial control network causing 13 manufacturing plants to shut production lines, loss $1.4m [5]
Davis-Besse Nuclear Power Plant (2003)	Unidentified	Power plants	SQL Slammer worm infected the Davis Besse nuclear power plant	Safety Parameter Display Systems and Plant Process Computer were disabled for several hours
CSX Corporation (2003)	Unidentified	CSX Corporation, Transportation Supplier in Florida, U.S.	A virus (email attachment) was reported to have shut down train signalling systems	No major incidents but trains were delayed. It shut down the signalling, dispatching and other systems at CSX Corporation
California Systems Operator (2001)	Unidentified attackers	California Independent Systems	Gained access into one of the computer networks	Unsuccessful attempt to penetrate systems, however, it lasted for 2 weeks [21]
Maroochy Water Systems (2000)	Disgruntled ex-employee	Maroochy Water Systems, Maroochy Shire	Hacked into a water control system. A series of attacks over a prolonged period	Flooded the grounds of a hotel and a nearby river with one million litres of sewage waste.
Gazprom (1999)	Disgruntled ex-employee	Gas company in Russia	Trojan Horse gain control of central switchboard, that controls gas flow in pipelines	Unidentified
Bellingham, WA Gas Pipeline (1999)	Failure of SCADA Systems	Bellingham, WA Gas Pipeline	The pipeline failed because the control systems did not during database development on the pipes while the pipes were in operation [25]	237,000 gallons of gasoline leaked from a 16" pipeline into a creek. The gasoline ignited and burned nearly 1 1/2 miles along the creek causing 3 deaths and 8 injuries [25]
Worcester, MA Airport (1997)	Hacker	Telephone Services Company	Hacker penetrated and disabled a telephone company computer that serviced Worcester Airport in Massachusetts	The telephone service to FAA control tower, airport security, weather service and several private airfreights were cut off. Financial losses & public safety
Salt River Project, Phoenix (1994)	An attacker	Government	Unauthorized access. Installed a backdoor. Altered login, password, computer systems files, root privilege	Critical data was accessed by attackers including water and power monitoring and delivery, financial, and customer and personal information.
Chevron Emergency Alert System (1992)	Disgruntled employee	Company and users	Unauthorized hacking of computers and programs and disabled the alarm	The systems did not operate for 10 hours and left affected people in 22 states at risk, including 6 unspecified areas of Canada
Siberian Pipeline Explosion (1982)	Vladimir Vetrov, KGB colonel	Siberian Pipeline	Unauthorized hacking and distribution of Trojan	Estimated at one-seventh the magnitude of bombs in World War II. Vaporized part of the Soviet Union's Trans-Siberian Pipeline [15]

Table 1. Summary of Previous Attacks on SCADA Systems (adapted from Miller et al., 2012)

4 Security of SCADA Systems

SCADA is described as a wide geographic distribution system. Stringent availability requirements and a heavy reliance on legacy systems introduce significant cyber security concerns while constricting the feasibility of many security controls [12]. The systems that govern these infrastructures must be able to highlight five main factors: ensuring security of the systems; emphasis on the reliability; ability to provide protection; ensuring the sustainability; and validating the cost effectiveness of the SCADA systems. Attacks on SCADA systems can be divided into three categories; attacks against or through the central controller, field units or the communication networks [10].These attacks could be physical attacks, malicious settings, malicious alterations, malicious alarms, denial of services, sniffing and/or spoofing.

Bearing in mind that in a typical SCADA System, availability of the system is emphasized and followed by integrity as well as confidentiality[6]. An earlier study [14] focused on compartmentalizing policies, to avoid overlap and ensure that each policy is effective including communication, personnel, data, physical and platform security as well as configuration and application management, manual operations and audit. [24] proposed a Real-time Monitoring, Anomaly Detection, Impact Analysis and Mitigation Strategy (RAIM) Framework, mainly for electric power generation and it consists of four main components: monitoring of the systems and devices; extracting and analysing data from the power instruments and devices; assess the system's vulnerability and potential attack impact; and mitigate risks based on previous intrusion attempts, intrusion scenario, or ongoing denial of service (DoS) attacks. In this paper, we propose a framework for SCADA cyber security measures (see Fig 1). It is derived from both Cyber-Terrorism SCADA Risk Framework [2] and NIST 2011 standards [22] as described in more detail further in the text.

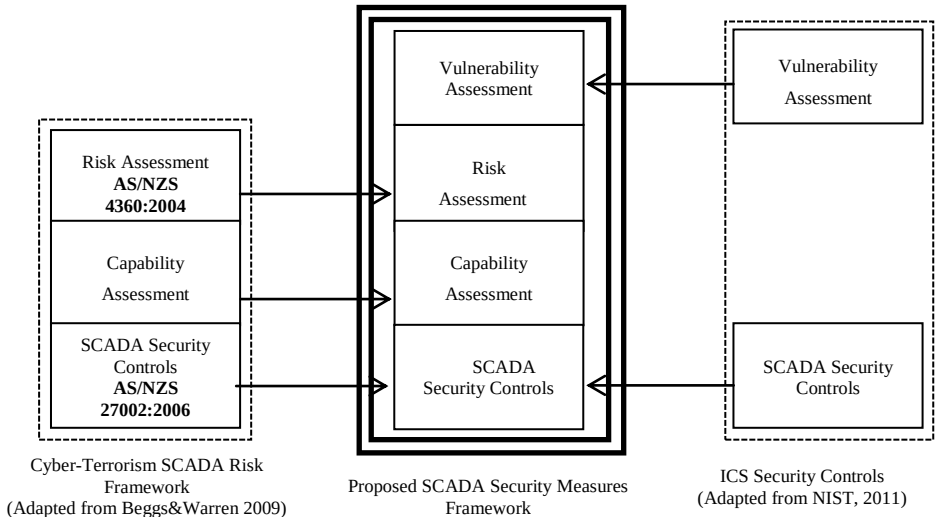

Fig. 1. Proposed SCADA Security Measures Framework

Vulnerability Assessment; is conducted to identify the vulnerabilities and security weakness in a system, and this means reviewing codes, settings, and logs for known security weakness [4]. A variety of security tools and techniques are used to identify and validate vulnerabilities, in order to secure the systems. The ICS Security Controls 2011 documentation outlined that the vulnerabilities for ICS could be grouped into Policy and Procedure, Platform and Network categories. These will assist in determining optimal mitigation strategies [22], and maximize the security of SCADA systems.

Risk Assessment; is used to identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to an organization, specifically to those organizations that employ SCADA systems. The outcome of a risk assessment could be used to determine the appropriate action in managing the information security risks to the SCADA system networks, which will then lead to appropriately selecting the best security controls to implement. The key areas in assessing risks are: communicate and consult SCADA; establish the context and framework; identify the risks associated; analyse and treat risks; and finally, monitor and review SCADA systems.

Capability Assessment; [2] stated that the capability model was designed to identify, examine and analyse the level of cyber-capability that a terrorist attacker needs to acquire in order to attack SCADA systems. The assessment model consists of eight levels to indicate the terrorist's cyber-capability with: political/motivation; advanced ICT skills; required tools and techniques; access to new advanced ICT; advanced knowledge of SCADA systems; ability to use internal resources and knowledge; ability to reconnaissance (scanning or probing); sufficient financial ability to attack SCADA systems [2]. Further research will be done to incorporate the three levels of cyber terror capability as aligned by [17] which include Simple-Unstructured, Advanced-structured and Complex-Coordinated. The indications will be developed after further research is conducted based on different cases of attacks compared to the previous work done.

SCADA Security Controls; in their framework, Beggs and Warren (2009) defined the SCADA Security controls according to AS/NZS 270002:2006, which covers SCADA Security Policy. This includes, security policy, organization information security, human resource security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, IS incident management, SCADA business continuity management and finally SCADA compliance. This paper adopts the SCADA security controls in the NIST 2011, which categorizes these controls into three groups, namely management controls, operational controls and technical controls.

5 Conclusion and Future Work

Based on understanding the importance of assessing security and ensuring organizations are well informed on security measures, this paper investigated issues in critical

infrastructures and SCADA systems security. It highlights SCADA systems vulnerabilities and provides a comprehensive list of cases of cyber-attacks and their impact on society, economy and environment. It further describes existing approaches and some best practices on SCADA security assessments and proposes a framework for SCADA security measures.

Our research aims to further study and enhance initial framework for measuring SCADA Systems security and its resilience against cyber-terrorist attacks. The first step is to define the existing standards, regulations and process in SCADA security systems and to examine the standards that have been defined in the national security policies. The next step is to evaluate the current SCADA systems security by measuring the SCADA security controls that have been implemented and assess their effectiveness, including:

- SCADA systems' vulnerability assessment;
- SCADA systems' risk assessment;
- SCADA systems' capability assessment; and
- SCADA systems' security controls.

By merging the four assessments criteria, it is hoped the framework will enhance the awareness and security levels, by assessing the vulnerabilities and risks involved as well as indicating the level of capability that a terrorist to penetrate the systems and security controls that needs to be put forward to ensure the security in organisations. This will be done by integrating the available procedures and guidelines and enhancing it to improve security. The final step will be to validate the framework through conducting focus groups sessions with the experts from the industry in order to verify that the framework could assist in increasing awareness and reducing security risks in an organisation. In order to address the issues and gaps arising from previous surveys, further research will focus on the three dimensions (people, process and technology) in improving security in SCADA systems.

6 References

1. Beggs, C.: Cyber-terrorism : a threat to Australia? Managing Modern Organisation with Information Technology- Information Resources Management Association (IRMA). pp. 472–475 Idea Group Publishing, San Diego, USA (2005).
2. Beggs, C., Warren, M.: Safeguarding Australia from Cyber-terrorism : A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption Keywords. Proc. 10th Aust. Inf. Warf. Secur. Conf. Ed. Cowan Univ. Perth West. Aust. 369–384 (2009).
3. Brömmelhörster, J. et al.: Critical Infrastructure Protection : Survey of World-Wide Activities. (2004).
4. Centre for the Protection Of National Infrastructure (CPNI): Cyber Security Assessments of Industrial Control Systems: Good Practice Guide. (2010).
5. Combs, M.M.: Impact of the Stuxnet Virus On Industrial Control System. XIII International forumModern information society formationproblems, perspectives, innovation approaches. pp. 5–10 (2011).
6. Dawson, R. et al.: SKMA – A Key Management Architecture for SCADA Systems. Proceedings of the 2006 Australasian workshops on Grid computing and e-research. pp. 183–192 Australian Computer Society Inc. (2006).

7. Espiner, T.: McAfee: Why Duqu is a big deal, http://www.zdnet.com/mcafee-why-duqu-is-a-big-deal-3040094263/.
8. Farris, J.J., Nicol, D.M.: Evaluation of Secure Peer-to-Peer Overlay Routing for Survivable SCADA Systems. 2004 Winter Simulation Conference. pp. 300–308 (2004).
9. Farwell, J.P., Rohozinski, R.: Stuxnet and the Future of Cyber War. Surviv. Glob. Polit. Strateg. 53, 1, 23–40 (2011).
10. Fernandez, E.B. et al.: On building secure SCADA systems using security patterns. Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW '09. p. 17 ACM Press, New York, New York, USA (2009).
11. Fernandez, J.D., Fernandez, A.E.: Scada systems: vulnerabilities and remediation. J. Comput. Sci. Coll. 20, 4, 160–168 (2005).
12. Hahn, A. et al.: Development of the PowerCyber SCADA Security Testbed [Extended Abstract]. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. pp. 1–4 (2010).
13. Kaspersky Lab: Gauss: Abnormal Distribution, http://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf.
14. Kilman, D., Stamp, J.: Framework for SCADA Security Policy. (2005).
15. Melito, S.: Software and Cold War: The Siberian Pipeline Explosion, http://defsecnet.com/software-and-cold-war-the-siberian-pipeline-explosion/.
16. Miller, B., Rowe, D.: A Survey of SCADA and Critical Infrastructure Incidents. Proceedings of the 1st Annual conference on Research in information technology - RIIT '12. p. 51 ACM Press, New York, New York, USA (2012).
17. Nelson, B. et al.: Cyberterror Prospects and Implications. , Monterey, CA (1999).
18. Nicholson, a. et al.: SCADA security in the light of Cyber-Warfare. Comput. Secur. 31, 4, 418–436 (2012).
19. Prigg, M.: The hunt for Red October, http://www.dailymail.co.uk/sciencetech/article-2263322/Operation-Red-October-revealed-The-astonishing-hacker-attack-infiltrated-55-000-high-level-government-computers.html#ixzz2KAIDcX4G.
20. Rautmare, S.: SCADA System Security. India Conference (INDICON). pp. 1–4 Annual IEEE (2011).
21. Stamp, J. et al.: Sustainable Security for Infrastructure SCADA. (2003).
22. Stouffer, K. et al.: Guide to Industrial Control Systems (ICS) Security. , US (2011).
23. Symantec: Symantec Critical Infrastructure Protection Survey. (2011).
24. Ten, C. et al.: Cybersecurity for Critical Infrastructures : Attack and Defense Modeling. IEEE Trans. Syst. Man, Cybern. ASystem Humans. 40, 4, 853–865 (2010).
25. Tsang, R.: Cyberthreats, Vulnerabilities, and Attacks of SCADA Networks, http://gspp.dreamhosters.com/iths/Tsang_SCADA Attacks.pdf.
26. White, J.: 12 Steps toward Cyber Resilience, https://www.isc2.org/infosecurity-professional-insights.aspx.
27. Yaron, O.: Flame virus had massive impact on Iran, http://www.haaretz.com/news/diplomacy-defense/flame-virus-had-massive-impact-on-iran-says-israeli-security-firm-1.433222.
28. Yunos, Z. et al.: Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework. 2010 Sixth Int. Conf. Inf. Assur. Secur. 21–27 (2010).
29. Zhu, B. et al.: A Taxonomy of Cyber Attacks on SCADA Systems. 2011 Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Soc. Comput. 380–388 (2011).