AC 2012-3612: LARGE SCALE, REAL-TIME SYSTEMS SECURITY ANALYSIS IN HIGHER EDUCATION

Jordan Sheen, Brigham Young University

Jordan Sheen is a graduate student in the School of Technology at Brigham Young University (BYU). Sheen completed a B.S in information technology at BYU in 2011, where his main interests were in cyber security and embedded systems. In his graduate program, Sheen will focus on the security of critical infrastructure components. In his spare time, Sheen enjoys walking with his wife, wrestling with his three sons, and cooing for his infant daughter.

Dr. Dale C. Rowe Ph.D., Brigham Young University

Dale Rowe's is an asst. professor of IT and a director of the Cyber Security Research Laboratory. His research interests include securing critical infrastructure, open source cyber intelligence and threat analysis. He is a Certified Information Systems Security Professional (CISSP) and holds a GIAC certification as an Exploit Researcher and Advanced Penetration Tester (GXPN). He is also a member of the IET, a Chartered IT Professional of the BCS, vice-president of the ISSA Utah Chapter and a senior research advisor to the Cyber Security Forum Initiative (CSFI). He transitioned from industry to academia in 2010 when he moved from the UK to the USA. He is married with 5 children.

Dr. Richard G. Helps, Brigham Young University

Richard Helps' research interests are in embedded systems, human-computer interaction, and technical course design for rapidly-changing technologies. He is a member of ASEE, IEEE (and IEEE-CS), ACM, and SIGITE. He has been involved in ABET accreditation as a Commissioner and Program Evaluator and continues his involvement in SIGITE in developing and promoting IT programs.

©American Society for Engineering Education, 2012

Large Scale, Real-Time Systems

Security Analysis in Higher Education

Abstract

This paper discusses the positive and negative aspects of large scale, real time systems' security (e.g, SCADA and industrial control) as currently taught in higher education. Until recently SCADA and industrial control systems security (ICS) has not been a strong focus in university curricula. As a result of new cyber security education initiatives and wide spread attacks like Stuxnet and DUQU, it has become necessary to instruct students from information technology (IT) and engineering disciplines how to secure environments with thousands of real-time nodes, such as those in SCADA and ICS.

Computing disciplines address cyber security to varying degrees. However, the extent to which SCADA/ICS system security is currently incorporated varies from little to none. To help address this problem, this paper proposes an educational model where computing disciplines can focus on the cyber security aspects of SCADA/ICS that are more closely related to their core objectives. We propose an educational model in which all computing disciplines follow a more structured awareness of SCADA/ICS security issues. Electrical and Computer Engineering (ECE) students should use best design practices to securely develop embedded hardware. ISYS students should be aware of the business impacts involved in security failures of SCADA/ICS environments and policies. Computer Science will be responsible for developing secure software. IT should be responsible for developing secure systems, and using theoretical and experiential training in developing a secure system from end to end.

There are a number of tools to assist in this development. Some of the tools available include: standards and guidelines for security analysis and development, and simulation environments for experiential training. We recommend a framework be developed to further incorporate this model.

Introduction

Large scale, real-time embedded systems are used to support many industrial systems, including critical infrastructure such as those used for electrical supply[1] and water utilities[2], and are commonly called Software Control and Data Acquisition (SCADA) systems. The purpose of using SCADA in critical infrastructures "is to allow operators to monitor and control systems" and to ease workload and management[3]. The architecture of these systems can consist of vast arrays of components. In some cases, SCADA systems are large enough to span continents[4]. The management of SCADA systems was consolidated using personal computers to monitor processes by making requests for information from embedded devices commonly known as programmable logic controllers (PLCs). However, as SCADA systems began to integrate with personal computers, they were exposed to outside volatile networks, bypassing the common "security by obscurity" philosophy [5, 6].

Several instances occurred in the early 2000's that raised concern about the security of SCADA environments[7]. In 2003, the Slammer Worm infected the David-Besse nuclear power plant in Ohio. Although the facility was undergoing maintenance at the time, the worm compromised the workstations in the control room, and crashed the monitors showing the safety controls[8]. This system and other systems that were once perceived as being impregnable were suddenly becoming compromised around the globe[9], because of their exposure to the internet.

The discoveries of the vulnerabilities in some SCADA systems lead to a surge in the amount of research regarding the security of critical infrastructures. It also led to research attempting to classify the types of vulnerabilities found in SCADA systems, as compared to more conventional commercial IT system [10], to develop standards for them[11] and methods guidelines to protect them[12]. It became apparent from the research that the problem facing dozens of industries was the dependency on control systems that never had security as an integral part of their development lifecycle [13]. The results of this acknowledgement lead to research efforts where mechanisms were trying to retrofit legacy systems. However, retrofitting legacy systems does not provide a long term solution to the problem[14].

The purpose of this paper is to evaluate the approaches taken in higher education to address the problem facing SCADA security. The first section describes how higher education currently handles security in regards to SCADA/ICS environments. The second section discusses areas of focus pertaining to different disciplines. The third section discusses tools that can be used to expose students to SCADA/ICS topics.

Current Curriculum

Current curriculum in higher education seems to indirectly address critical infrastructure security concepts. Engineering disciplines discuss buffer overflows, information systems programs discuss the business impact of security issues, and IT programs cover cyber security challenges in systems. There are a few reasons why direct exposure to SCADA security topics has been limited.

One of the reasons deals with integrating effective examples into coursework. In 2009, researchers from Ege University in Turkey discussed the problems in introducing students to SCADA systems, and noted that SCADA equipment can be difficult to use for students, partly because it is difficult to replicate real-world environments in a lab. They also noted that the cost of equipment used can be excessive[15].

Another problem is scope. SCADA security is a topic where programs may not know how much of the topic to cover. We have noted a distinct lack of coverage even in many areas where it may be appropriate to cover these topics. It then becomes important for disciplines to understand what part of SCADA security applies to them, and how to teach it.

SCADA Security Education

To incorporate SCADA security into higher education, each field should focus on the areas that are most pertinent to their discipline. In order to do this, computing disciplines need to determine where they fit. We propose a model where SCADA security is distributed as a topic across 3 core disciplines: information technology, electrical and computer engineering, and information systems or business systems.

Each of these disciplines focuses on essential parts of SCADA environments. Figure 1 shows the focus from each discipline and how it contributes to SCADA security.

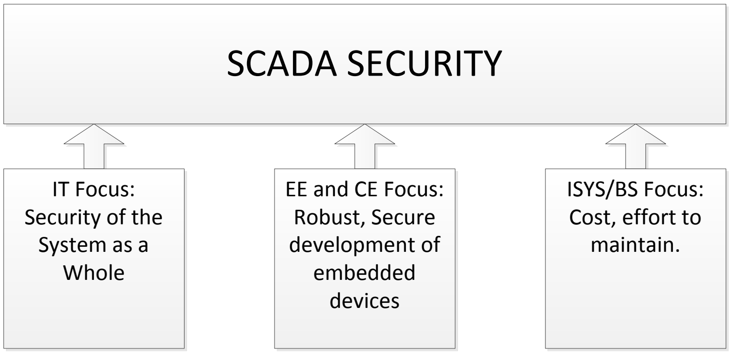
SCADA SECURITY
IT Focus: Security of the System as a Whole
EE and CE Focus: Robust, Secure development of embedded devices
ISYS/BS Focus: Cost, effort to maintain.

Figure 1 - SCADA Security Focus of Computing Disciplines

IT disciplines should focus on securing the system as a whole. EE and CE disciplines should focus on creating secure applications for embedded devices, as well as hardware. ISYS/BS fields should understand the technology involved and the impacts of security failures in business processes. We believe that as each computing discipline adopts the area of focus best suited for them, they will be able to incorporate SCADA education as a serious topic of study, and do so in a way that augments, rather than detracts from their core objectives.

Foundational Material

Technical disciplines should consider reviewing foundational material, and identifying opportunities to apply security practices to reinforce key concepts. In other words, include security across the curriculum from the ground up [16]. IT students may focus on secure integration and systems analysis, and ECE students may focus on the development of secure software and hardware. This approach should not entail a substantial shift in the core curriculum.

Aside from this implementation, one has to consider what other methods are beneficial in preparing computing professionals for SCADA security. Because technology changes rapidly, students should understand how to adapt to new technology, understand standards and guidelines for secure practices, and have experiential learning. Having an understanding of the theory of systems and systems design can help students adapt to changes.

In making a translation from engineering, IT, or computer science to SCADA systems the actual technology may not be difficult to understand. At BlackHat Federal 2006, Dick Maynor and Robert Graham noted the idea that for someone who understands topics like remote administration through telnet or SSH, the OSI network stack, and Linux administration the migration to critical infrastructure concepts should not be difficult[17]. If this assumption is correct, then helping students to understand SCADA systems should not be difficult when they have the appropriate foundation.

Exposure to SCADA/ICS Environments

To effectively expose students to SCADA/ICS environments they need an understanding of large scale system concepts, and practical experience to validate those concepts. The combination of these two things can provide experiential learning, and help students develop a practical understanding of the technology[18]. Recent work by Guillermo Francia offers suggestions on how to incorporate critical infrastructure modules into courses[19]. There are additional possible methods for increasing exposure to SCADA environments.

One way to give students experiential learning in SCADA/ICS security is to provide laboratory subjects on the topic. As noted earlier, this is not always easy to do. However, in the past few years, software has become available which allows the creation of virtual PLCs[20]. National Instrument's Lab View now has a product that enables the virtual development of PLC and the system interactions. Students can use this kind of software to develop a virtual environments with PLCs and gain experience in the design of these kinds of systems[21].

Using virtual environments makes it easier to use existing technology to develop diverse systems and adjust parameters in a multi-user setting. Theoretically, students could create virtual PLCs, and incorporate security tools such as intrusion detection/prevention systems, firewalls, and honeypots to analyze the security impacts on such a system. This kind of experiment allows students to understand security concepts using virtual technology.

In regards to security analysis the following is a list of modules that may be incorporated into SCADA security course modules:

- Network analysis of SCADA transmissions through the use of man-in-the-middle attacks (see Figure 2)
- Forensic analysis of component failures using commercial and open-source forensic tools
- Identifying flaws in parameter handling by fuzzing inputs, and network traffic used by PLC's, HMI's and other components.
- Performing penetration testing against SCADA systems
- Decomposition and filtering of SCADA protocols
- Mitigating denial-of-service attacks on SCADA components
- Analyzing the propagation of malware among programmable logic controllers
- Incorporating layer 3 security features such as IPSec

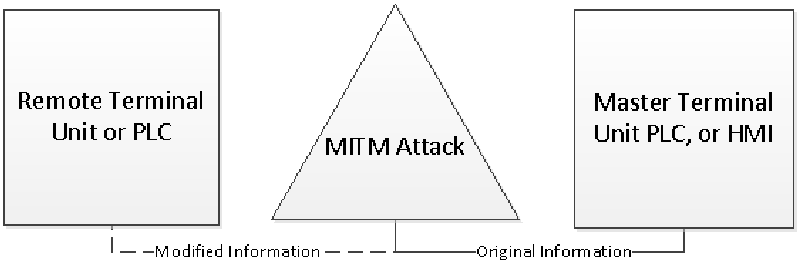

Figure 2 - Example of Man-In-The-Middle SCADA Attack Lab

SCADA security modules such as these should be performed with the ethical intent to understand and prepare against attacks on SCADA systems. Modules such as these may solidify understanding of SCADA systems, and provide ways to interest students in performing undertaking further research.

Conclusion and Future Research

As security of large scale embedded systems becomes more of a focus in academia, there will be a new challenge in how to educate students on these kinds of environments. The history of this education has been spread across disciplines. Different majors should approach SCADA/ICS differently focusing on the security aspects that are appropriate to their core objectives. Doing so will help students be more aware of the security issues facing large-scale, real time embedded systems. However, to do this effectively, there needs to be an increase in inter-disciplinary collaboration in both teaching and research. This will help identify key areas where interfaces between 'users and systems', 'systems and systems' and 'systems and components' require the effort of all involved to better secure these systems.

In order to expose students to these kinds of environments, educators should consider using experiential methods of teaching. Students can learn about these environments by learning about the protocols used in SCADA/ICS environments. Additionally, students can become more aware of these environments by creating virtual PLCs. Students can then become more aware of how these environments function in a fail-safe environment. We also believe that future research is needed to evaluate the effectiveness of these teaching methods across disciplines.

We believe that SCADA security should be considered as a key part of IT, ECE and ISYS curriculums that this can be implemented effectively by pervasively including it throughout related topics. Students with these key skills and knowledge will be better equipped to address critical infrastructure in the coming years.

References

1. Figueiredo, J. and J. Martins, *Energy Production System Management - Renewable energy power supply integration with Building Automation System.* Energy Conversion and Management, 2010. **51**(6): p. 1120-1126.
2. Jing, L., S. Sedigh, and A. Miller. *Towards Integrated Simulation of Cyber-Physical Systems: A Case Study on Intelligent Water Distribution*. in *Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on*. 2009.
3. Fernandez, J.D. and A.E. Fernandez, *SCADA systems: vulnerabilities and remediation.* J. Comput. Small Coll., 2005. **20**(4): p. 160-168.
4. ABB. *Transforming Asia's largest oil and gas company (Press Release)*. [cited 2012 February 3]; Available from: http://www.abb.com/cawp/seitp202/9adc5d69703dd004c1257515002ef352.aspx.
5. Igure, V.M., S.A. Laughter, and R.D. Williams, *Security issues in SCADA networks.* Computers &amp; Security, 2006. **25**(7): p. 498-506.
6. Cleveland, F. *IEC TC57 Security Standards for the Power System's Information Infrastructure - Beyond Simple Encryption*. in *Transmission and Distribution Conference and Exhibition, 2005/2006 IEEE PES*. 2006.
7. Dumont, D. *Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems*. in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. 2010.
8. Geer, D., *Security of critical control systems sparks concern.* Computer, 2006. **39**(1): p. 20-23.
9. Weiss, J., *Selected Case Histories (Chapter 15.1)*, in *Protecting Industrial Control Systems from Electronic Threats*2010, Momentum Press.
10. Hentea, M., *Improving Security for SCADA Control Systems.* Interdisciplinary Journal of Information, Knowledge, and Management, 2008. **3**.
11. Sommestad, T., G.N. Ericsson, and J. Nordlander. *SCADA system cyber security &#x2014; A comparison of standards*. in *Power and Energy Society General Meeting, 2010 IEEE*. 2010.
12. Keith Stouffer, J.F., Karen Scarfone, *Guide to Industrial Control Systems (ICS) Security* 2008.
13. Laboratory), I.I.N., *National SCADA Test Bed Substation Automation Evaluation Report.* 2009: p. 57.

14. Cardenas, A.A. *Research Challenges For the Security of Control Systems*. in *Hot Topics in Security (HOTSEC'08')*. 2008. Berkley, CA.

15. Sahin, S.O., M. Isler, Y, *Microcontroller-Based Experimental Setup and Experiments for SCADA Education.* Education, IEEE Transactions on, 2010. **53**(3): p. 437-444.

16. Rowe, D.C., B.M. Lunt, and J.J. Ekstrom, *The role of cyber-security in information technology education*, in *Proceedings of the 2011 conference on Information technology education*2011, ACM: West Point, New York, USA. p. 113-122.

17. Richard Maynor, R.G. *SCADA Security and Terrorism: We're Not Crying Wolf*. BlackHat Federal 2006 [cited 2012 March 10]; Available from: http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

18. Barry M. Lunt, J.J.E., Sandra Gorka, Gregory Hislop, Reza Kamali, Eydie Lawson, Richard LeBlanc, Jacob Miller, Han Reichgelt. *Curriculum Guidelines for Undergraduate Degree Programs in Information Technology*. 2008 [cited 2012 March 10]; Available from: http://www.acm.org/education/education/curricula/IT2008%20Curriculum.pdf.

19. Guillermo A. Francia, I., *Critical infrastructure security curriculum modules*, in *Proceedings of the 2011 Information Security Curriculum Development Conference*2011, ACM: Kennesaw, Georgia. p. 54-58.

20. M.K. Abuzalata, M.A.K.A., Shebel Asad and Mazouz Salahat, *Design of a Virtual PLC Using Lab View.* Research Journal of Applied Sciences, Engineering and Technology, 2010. **2**(3): p. 5.

21. Adamo, F., et al., *SCADA/HMI systems in advanced educational courses.* Ieee Transactions on Instrumentation and Measurement, 2007. **56**(1): p. 4-10.