ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 5, December 2014

Why Computer Security Matters to Electrical Engineers?

Binto George

School Of Computer Sciences, Western Illinois University, Macomb, IL, United States

ABSTRACT: In this paper we analyze two computer security incidents of particular interest to electrical engineers: "Stuxnet" worm attack on Iran's nuclear enrichment facility; and the "Project Aurora" by Idaho National Laboratory that exposed the vulnerability of power grids. Based on these incidents, we think that a secure system development method can mitigate security vulnerabilities in Industrial Control Systems (ICS). Such method must include systems, people and processes within an organization. Both technical and human factors should be considered. We discuss a Secure System Development Cube Cycle based on the 3P Method as a potential solution.

KEYWORDS: SCADA Security, ICS Security, Secure System Design

I. INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) system enables supervision and remote control of power plants, substations, and switching centres. While SCADA has been effective in reducing costs, improving efficiency and increasing coordination among centres, the two security incidents point to the need of having a secure system development method to ensure the safety and security of the infrastructure. In this paper, we discuss a Secure System Development Cube Cycle that involves the thorough review at each stage of the system development lifecycle from three perspectives (the 3P Method), namely, ***Use***, ***Defense***, and ***Offense***. The idea presented in this paper combines the 3P method[1] with the current software engineering practices and the research in the field of computer security, software engineering and usable security. The 3P Method has been found to be effective in teaching computer security courses. We believe such a method will be instrumental in designing, building and maintaining secure Industrial Control Systems (ICS).

II. SECURITY INCIDENTS

A. Stuxnet

Stuxnet [2] attack on Iran's Natanz nuclear enrichment facility was unprecedented in many ways. Stuxnet quietly spread through the Internet without damaging any of the Microsoft Windows computers. The worm took great pains to verify a number of unique parameters to ensure that it affects only the target facility. Like many SCADA networks, for security reasons, Natanz network had an "air gap" with no direct connection to the outside network. Interestingly, however, Stuxnet was able to jump the air gap and infect the Programmable Logic Controllers (PLC) . Stuxnet used six zero day exploits and stolen digital certificates to make its way undetected. Stuxnet was able to spread through USB flash drives, network shares, print spoolers and Siemens Step 7 software project files. While we are not sure, it is believed that Stuxnet was introduced into the SCADA network by an insider with a flash drive.

Once inside, Stuxnet was able to manipulate the rotational speed of centrifuges. At times, the worm slowed down the centrifuges to affect the quality of uranium enrichment. Other times, Stuxnet drove the centrifuges at high speed to eventually damage them. The attacks, when unleashed, lasted only a few minutes. Also, there were several days between consecutive attacks. All these cleverly hid Stuxnet from Iranian engineers who likely found the anomalies hard to fix and frustrating.

B. Project Aurora

The second incident is the experiment conducted by Idaho National Laboratory under the code name "Project Aurora" [3]. In a simulated cyber attack, researchers were able to access the control system of a diesel power generator weighing 27 tons. By opening and then closing the digitally controlled relay when the generator was out of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 5, December 2014

synchronization with the power grid, the attack was able to cause significant damage to the diesel engine and the generator.. Thanks to the designed pauses built into the simulated attack for safety reasons, it took about three minutes to complete the destruction. The destruction could have been much quicker if attacks were launched without the added delays. Obviously, the standard safety devices did not respond fast enough to prevent the damage.

The subsequent analysis recommended stronger passwords, tighter access control, modification of the digital relay firmware and other protective mechanisms and procedures. In short, a similar attack can cause significant damage to generators, motors, pumps and substations.

III. SECURE SYSTEM DESIGN

Secure system design should consider the system in its entirety, including people, process and the equipment. Security should be integrated right from the beginning of the system development, if possible. Both human factors and technical factors should be considered.

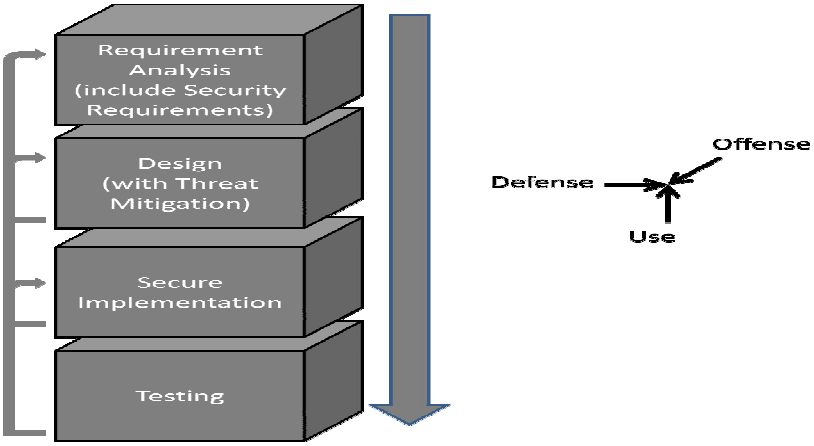

Fig. 1 Secure System Development Cube Lifecycle

Fig 1 shows the Secure Software Development Cube Cycle. This is similar to the conventional software development lifecycle but combines the iterative design for usable security [4]. At each stage, security is given emphasis by analyzing it from ***Defense***, ***Use and Offense*** perspectives[1]. The ***Defense*** analyzes what protection mechanisms must be included from an administrator's point of view; ***Use*** focuses on how the system is going to be used (including the usability of the security functions) from the users' perspective; ***Offense*** focuses on how the system could be attacked from an adversary's viewpoint.

For example, during the requirement analysis phase a system designer normally would sit with the user and develop specifications. A good analyst asks questions to find out how the system is going to be used. Since the primary task of the user is not security, in our experience, security issues do not often come up. So the analyst has to specifically ask questions to assess the security requirements. Even when an analyst meticulously does this, the discovery is often limited to ***Defense*** viewpoint. However, a potential intruder into the system often has a different perspective. For example, say, for a business, the system availability for use is more important than enforcing password quality. However, for a particular cyber criminal, breaking into an account having an easy password will provide insider access in order to attempt privilege escalation. So it makes sense to analyze the system from the ***Offense*** perspective as well.

The perspectives may be switched as necessary. For instance, a particular security feature may be hard to use. If that is the case the system designer should consider usable security aspects. Also, it pays to analyze the effectiveness of a security feature from human factor perspective. The system design should include threat modelling and mitigation [5]. The perspective switching may be done in all stages - for instance, testing can be done with users for ensuring usability

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 5, December 2014

and usable security. Experts can test the safeguards to ensure they work as expected. And a red team can be deployed to test the system from the ***Offense*** viewpoint. Also, at any stage in the cube cycle, we can go back to any of the previous stages as needed. For example, during testing, if we find that the system is not working as expected, we may revisit the design or even go back to the requirement analysis.

IV. APPLYING SECURE CUBE LIFECYCLE

Stuxnet: Clearly, the ***Defense*** viewpoint influenced the decision of keeping the SCADA network air gapped. The hope was that air gap would protect the system from outside attacks, but it just provided a false sense of security. However, if designers had viewed from the ***Use*** viewpoint, they could have concluded that employees might use their flash drive for transferring files and installing programs and therefore the system was vulnerable to malware. Such an analysis would have resulted in having additional safeguards. Looking from ***Offense*** viewpoint, someone could have tried to penetrate the system using malware as that was a common method of attack. Stuxnet employed root kits, again a very common tool used by hackers.

Project Aurora: one recommendation came out of the project is to install automatic out-of-sync detectors with every relay in order to block its closure if the frequency, phase or voltage is not within tolerable range. While this safeguard may prevent generator damages in the case of an attack, when viewed from ***Offense*** perspective, we realize that this does not prevent a generator from going out of service. If a sufficient number of power generators are affected, that can result in cascaded tripping and widespread power outage. The fundamental issue is that power grid communication protocols are not designed with security in mind. Department of Homeland Security (DHS) suggested a number of mitigations including simple (non-programmable) protection mechanisms and standalone alarms that are not accessible from the network. While these may be effective in the interim, better long term strategy should be to design secure control systems. Analysis from ***Use*** perspective would show that for control systems protected by password or PIN, the security depends on users choosing adequately strong passwords. If system requires complex passwords, users may tend to forget them. So they may compromise security by writing them down (although writing down a complex password and keeping them in a safe place is much better than setting a weak password). As the result, the system may require better authentication mechanisms that are simultaneously usable and secure.

V. CONCLUSIONS

Lessons from "Stuxnet" and "Aurora Project" emphasize the need for significant improvement in ICS security. From our experience of developing secure software, we think that a similar approach may be extended to the development of secure control systems. The method should consider the system as a whole and include equipment, personnel and processes. For security to be effective, both technical and human factors should be considered. The security should be introduced as early as possible into the system design and development. A Secure System Development Cube Cycle may be considered for improving ICS security.

ACKNOWLEDGMENT

The author acknowledges Susan S. Mathai for her suggestions and constructive feedback.

REFERENCES

[1] B. George, M. Klems, and A. Valeva, *A method for incorporating usable security into computer security courses*, SIGCSE 2013.
[2] R. Langner, *Stuxnet: Dissecting a Cyberwarfare Weapon*, IEEE Jl of Security and Privacy, 9(3), May 2011.
[3] C. Liu, A. Stefanov, J. Hong,, P. Panciatici., *Intruders in the Grid*, IEEE Power and Energy Magazine, 10(1),Jan -Feb 2012.
[4] B. D. Payne and W. K. Edwards, *A Brief Introduction to Usable Security*, IEEE Internet Computing, 12(3),May -June 2008.
[5] F. Swiderski, *Threat Modeling*,.Microsoft Press, 2004.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 5, December 2014

BIOGRAPHY

Dr Binto George is a Professor in School of Computer Sciences at Western Illinois University, USA. He is also the founder and president of CSTRNEDS LLP. Dr George completed his Ph.D. from Indian Institute of Science, Bangalore. He has also worked as an Assistant Research Professor at Rutgers University.

Dr George has several publications in the area of secure real-time transaction processing, secure buffer management, database security and usable security. He was the principal investigator of National Science Foundation (NSF) funded project on incorporating Usable Security into Computer Science curriculum. Dr. George has been working closely with many organizations that promote cyber security and national infrastructure security. Dr. George is a member of the IEEE Computer Science Society and a professional member of the Association for Computing Machinery (ACM).