PREVENTION AND PREPARDENESS FOR CYBER SECURITY ATTACKS AND INCIDENTS AGAINST ICS/SCADA

Tiffani A Shields

Saint Leo University

Abstract

More often than not control and security overlap, resulting in the two sides disagreeing and left unaware of each other's objective to ask pertinent questions. Therefore, as of late the goal is how to successfully deploy an ICS/SCADA system and enhance security while simultaneously providing a reliable platform for process control and automation. Historically, cyber security was not needed and now increased power makes systems more efficient, but also more vulnerable. So how does an organization sustain peak production and strengthen security? Recent ICS/SCADA incidents emphasize the importance of good governance and regulator of ICS infrastructures. Of late there have been several cyber incidents impacting confidentiality, integrity, and availability of systems either intentionally or unintentionally. About a year ago, a Trend Micro Sr. Threat Researcher embarked on a venture to deploy an internet facing ICS/SCADA honey pot to assess who is attacking the devices and why. During the examination, it was noted 16 different countries attempted a malicious or inadvertent attack citing an overall attack listing of 74 of which 63 were non-critical and 11 critical. Consequently, a few thing to keep in mind is to perform pen testing incident responses as much as possible, perform specialized vulnerability assessments, control contractors (if contractors/vendors have a back door then someone else potentially does too), and perform basic security controls. While the honeypot assessment is one of many recent incidents, others to consider are Stuxnet worm attack, Shamoon virus, Aurora vulnerability, turbine control attack, and most recently the assassination of Iran's cyber warfare commander.

Introduction

We've become conditioned to trust the applications or operating systems that we run in our servers, desktop, and even cell phones. As vulnerabilities surface software companies are responsible for releasing a fix or patch for it. As time-consuming as the process can be, patches and updates are key in maintaining the security of the system. However, the process of dealing with legacy SCADA systems and other Industrial Control Systems require more sophisticated measures to protect against vulnerabilities.

Ultimately, SCADA systems were designed to monitor the process without considering external security threats. "Many of the critical components that operate today do so in a context that's completely different from the one they have been designed for" (Paganini, 2013). As most SCADA systems are paramount to the World's critical natural infrastructures, such as water, power, and transportation using modern technology is a must.

What is SCADA?

Before jumping right into SCADA systems vulnerabilities, a clear understanding of what a SCADA system does will be helpful. SCADA systems can affect everything from the heat in your home to your bank account. It's not a specific piece of equipment or technology, but rather relies on data collected from the system to control that system. For example, let's say the current procedure for monitoring the city water system requires an employee to walk through and to monitor each element of the water system. Ultimately the employee, is responsible for checking water levels and ensuring distribution lines are properly working. Fast forward to the integration of a SCADA system, the central monitoring and control of water is completed via a single host hereby replacing the employee walk-through. With the use of the SCADA system the host is supervised by a human operator that oversees the process, receive alerts, and exercise control.

SCADA Vulnerabilities

Organizations as a whole have a critical role in bridging the gap between automation and IT Security. Although similar in function, SCADA and IT Security, remain unparalleled, as they often are unaware of the other's objective and lack asking the pertinent questions. The priority of IT Security is confidentiality, integrity, and availability. On the other hand, the focal point of SCADA systems is maintaining the "reliability" of data without affecting productivity. As the two remain at odds, successfully deploying enhanced security while simultaneously providing a reliable platform for automation leaves gapping security holes.

More than ever SCADA systems now run Ethernet-like networking and are now more vulnerable to attacks at the same time they've become more valuable to operations. As SCADA systems have gained popularity in monitoring and control of water, oil, utility grids, pipelines, and many other critical infrastructure systems, SCADA systems were never designed to be secure from network intrusion. Patches may not take place for an extended period if vendors are not updating as they should or if the vendor still exist. So if a bug is exposed in a legacy SCADA system, it's likely to be vulnerable to a network attack because they may require new hardware just to upgrade as a patch may not suffice.

For SCADA systems, security has been a supplement to the architecture instead of being built around the product from the ground up. Security has been seen more as a hindrance while SCADA systems were built to be easy for the operators, so security wasn't a priority. Many security vulnerabilities exist because people think it will not happen to them. A few classic vulnerabilities are insiders, disgruntled employees, competitor, organized crime, and many others.

SCADA Attacks

The first attack against a Critical Infrastructure using a computer virus was called Stuxnet (Kroft, 2012, para. 3). Stuxnet was a well written bug containing tens of thousands of lines of code designed to attack an Iranian nuclear facility. Kim Zetter from Wired states, "An early version of the attack weapon manipulated valves on the centrifuges to increase the pressure inside them and damage the devices as well as the enrichment process" (Zetter, 2014, para 4). As a computer virus has been typically known to steal and/or corrupt information on your computer. The Stuxnet virus was designed to physically destroy equipment from a single host.

There is also the Aurora, the simulated cyber-attack demonstrating the takedown of an electrical power grid. In a CNN interview, U.S Cyber Consequence Unit, Scott Borg explains the impact of the loss of power to only a third of the country for three months. "It's equivalent to 40 to 50 large hurricanes striking all at once. Its greater economic damage than any modern economy has ever suffered. Greater than the Great Depression" (Edwards & Rhyne, 2007, para. 8).

Recommended Strategies

Defending against SCADA vulnerabilities has been an uphill battle. However, there are many necessary procedures in avoiding attacks. For instance, constant monitoring of remote access will aid in a more secure SCADA system. Disabling Internet access to trusted resources and ensure the trusted resources have the latest patches. Perform pen testing incident response as much as possible to keep abreast of possible loopholes. Control contractors' access to avoid system access by unknown personnel. In addition to, performing essential security controls such as network segmentation, two-factor authentications, patch your stuff, lockdown external media, manage vulnerabilities, and classify data/assets.

Conclusion

As you can see, SCADA systems are becoming increasingly complex, due to the integration of modern components with legacy systems, varied vendors, department cohesion, and security awareness. The methodology of SCADA systems must change to coincide with security requirements to minimize the surface attack and exposure to cyber threats. It is “must” that security becomes a priority in all SCADA projects to protect our critical infrastructures. With continued persistence and the utilization of secure computing tactics, we become one step closer to keeping the enemy out.

References

Brown, J. (n.d.). Exploiting SCADA Systems. Retrieved from http://defcon.org/images/defcon-18/dc-18-presentations/JBrown/DEFCON-18-Brown-SC ADA.pdf

Edwards, D., & Rhyne, J. (2007, September 27). The Raw Story |US power grid could be seized by hackers. Retrieved from http://rawstory.com/news/2007/Study_U.S._power_grid_could_be_0927.html

Kroft, S. (2012, June 4). Stuxnet: Computer worm opens new era of warfare. Retrieved from http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/

Paganini, P. (2013, December 6). Improving SCADA System Security - InfoSec Institute. Retrieved from http://resources.infosecinstitute.com/improving-scada-system-security/

Robles, R., & Choi, M. (2009, June 1). Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems. Retrieved from http://www.sersc.org/journals/IJGDC/vol2_no2/3.pdf

Wilhoit, K. (2013, January 1). Who’s Really Attacking Your ICS Equipment? Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-whos-really-attacking-your-ics-equipment.pdf

Zetter, K. (14, November 1). An Unprecedented Look at Stuxnet, the World's First Digital Weapon | WIRED. Retrieved from http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/