ASA

Annie Searle & Associates LLC

Research Note

Protecting Critical Infrastructure

By Andrew H. R. Hansen

Keywords: Critical Infrastructure, Shodan, smart grid, risk management, industrial control systems, SCADA, cyber threats

Abstract – The critical infrastructure of the United States are essential to the nation's security, public health and safety, economic vitality, and way of life. Advances in technology have made the eighteen critical infrastructures more efficient, but have also introduced new threats. Shodan is a tool that exposes potential weaknesses by identifying Internet facing industrial control system devices. Smart grid has the capability to provide more efficient energy consumption, but existing threats have security experts concerned. Risk managers should assess the ways compromises to critical infrastructure would impact their organizations and take appropriate measures to mitigate identified threats.

Introduction

The critical infrastructures of the United States have developed a highly complex and co-dependent relationship. Protecting and ensuring the continuity of these critical infrastructures is "essential to the nation's security, public health and safety, economic vitality, and way of life."[1] The rapid technological advances of the previous two decades have resulted in improved efficiency and increased performance of several critical infrastructure sectors, but weaknesses in these systems are "among the country's greatest threats to national security."[2] This research note will introduce the critical infrastructure sectors, discuss an emerging hacking resource, analyze specific challenges facing the smart grid, and conclude with recommendations organizations can take to help ensure their systems are protected.

Critical Infrastructure

Critical infrastructure are the "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."[3] The Homeland Security Presidential Directive 7 established United States policy for enhancing critical infrastructure protection, and "for each sector, designated a federal Sector-Specific

Agency (SSA) to lead protection and resilience-building programs and activities."[4] Through this directive and other legislative efforts spanning more than a decade, the following eighteen[5] infrastructure sectors have been identified as critical:

- Food and Agriculture
- Commercial Facilities
- Dams
- Energy
- Information Technology
- Postal and Shipping
- Banking and Finance
- Communications
- Defense and Industrial Base
- Government Facilities
- National Monuments and Icons
- Transportation Systems
- Chemical
- Critical manufacturing
- Emergency Services
- Healthcare and Public Health
- Nuclear Reactors, Materials and Waste
- Water

Protection of these infrastructures has been deemed especially important as attacks "could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident."[6] Many of these sectors are governed by industrial control systems, which is a high-level term that encompasses "supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configuration such as skid-mounted Programmable Logic Controllers (PLC)."[7]

Industrial control systems were initially isolated systems, running specialized proprietary hardware and software.[8] However, recent years has seen widely available, low-cost Internet Protocol (IP) devices replacing these proprietary solutions. Because industries like electric, water and wastewater, oil and natural gas, transportation, chemical and many others typically utilize industrial control systems, this shift away from proprietary technology to common IP technology could increase the possibility of cyber security vulnerabilities and incidents.[9]

Shodan

Sentient Hyper-Optimized Data Access Network, or Shodan, has been referred to as the Google for hackers, and is "essentially a search engine for servers, routers, load balances and computers."[10] The database developed by Shodan was built by indexing metadata in the headers contained in the hardware broadcasts to other devices.[11] Shodan provides the ability to find devices based on "city, country, latitude/longitude, hostname, operating system and IP,"[12] which means that, "not only can it identify a Solaris server, it can in many cases identify a Solaris server located in Pakistan that remains vulnerable to a known exploit."[13] With a tool like Shodan, the resources necessary to locate and identify Internet-facing SCADA systems has been greatly

reduced, a concerning fact that has not escaped the attention of security experts.

In October, 2010, following several reports from multiple independent security researchers, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an alert specifically addressing Shodan's ability to expose control system vulnerabilities. The ICS-CERT alert identified systems spanning several critical infrastructures, specifically mentioning the increased risk of account brute force attacks as some of the systems "continue to use default user names and passwords and/or common vendor accounts for remote access to these systems."[14] More alarming, many of these default credentials can easily be found online.[15] As discussed in a previous research note, the Stuxnet worm that reportedly burrowed into SCADA systems controlling Iranian nuclear power plants is a good example of the kinds of infrastructure attacks a resource like Shodan can help facilitate.

Although the compromising of any of the critical infrastructures would result in cascading and far reaching consequences, according to former CIA Director John Woosley, "One of (the greatest threats) is the vulnerability of our electricity grid to hackers and to physical attack on things like transformers… All of the 17 other (critical infrastructures)

depend on the electrical grid."[16] The following section will discuss some of the challenging security issues facing the electrical grid as it transitions to a "smart grid."

Smart Grid

Smart grid is a reference to the computerization of the existing power grid and will add "monitoring, analysis, control, and communication capabilities to the national electrical delivery system to maximize the throughput of the system while reducing the energy consumption."[17] The two-way digital devices will empower utilities to maximize efficiency by better controlling power distribution and allow homeowners and businesses to use electricity as economically as possible.[18] With $3.4 billion in stimulus funds being injected into smart grid technologies, an estimated 60 million American households and businesses are projected to deploy the technology in 2012 alone.[19] This will very likely result in more efficient energy consumption, but with "multiple credible threats" to the smart grid already in existence, many security experts feel the transition is premature.[20]

According to security experts, some of the meters and other points on the smart grid are susceptible to known attacks. In fact, professional security firm IOActive "determined that an attacker with $500 of equipment and materials and a background in electronics and

software engineering could 'take command and control of the [advanced meter infrastructure] allowing for the en masse manipulation of service to homes and businesses.'" Once a hacker was in the system, they could potentially "gain control of thousands, even millions, of meters and shut them off simultaneously."[21] In addition, a hacker may also be able to dramatically alter the demand for power, which would disrupt the load balance on the local power grid, and result in a blackout.[22]

Extended loss of power can have enormous consequences on the economy. On August 14, 2003 a power surge affected the transmission grid resulting in a blackout along the border of the United States and Canada leaving more than 50 million people without power.[23] The majority of areas impacted had power fully restored within two days, but part of Ontario experienced rolling blackouts for more than a week.[24] Most figures estimate the cost of the blackout to be around $6 billion, including costs like lost income to workers, extra costs to government agencies (due to overtime and emergency service costs), costs associated with lost or spoiled commodities, and costs associated with other industry specific losses (ie delays in shipping impacting supply chains).[25]

Since the 2003 blackout, the utility industry has made great improvements to its ability to detect and isolate outages and is projecting that some elements of new smart grid technology will enhance that capability.[26] Representatives from the industry seem to be aware of the potential problems, and claim to have no intention of putting an unsafe grid online.[27] But as the smart grid continues to develop, risk managers should exercise caution and ensure potential threats have been appropriately remedied.

Recommendations

In terms of responding to Shodan and other resources like it, the ICS-CERT alert recommended the following[28] actions:

- Placing all control systems assets behind firewalls, separated from the business network
- Deploying secure remote access methods such as Virtual Private Networks (VPNs) for remote access
- Removing, disabling, or renaming any default system accounts (where possible)
- Implementing account lockout policies to reduce the risk from brute forcing attempts
- Implementing policies requiring the use of strong passwords
- Monitoring the creation of administrator level accounts by third-party vendors

ICS-CERT also recommended control system owners and operators to audit their control systems for the use of default

administrator level user names and passwords – regardless of whether or not the system is connected to the Internet.[29] Risk managers should constantly be researching tools like Shodan, and if appropriate, using the services to identify weaknesses in their own systems.

Risk managers should also ensure that disaster recovery and business continuity plans specifically address responding to a loss of power. Should an organization ever lose access to power from the grid, alternative power sources like generators can ensure critical systems and functions can continue to operate as expected without interruption. Servicing the standby generators and conducting regular tests will further enable an organization to respond effectively should a man-made or natural disaster strike. Installing surge protectors, protective software, and backing up data are all additional ways organizations can protect their systems and ensure damage from lost data and productivity is kept to a minimum.

Conclusion

At a recent cyber security conference, Director of the Federal Bureau of Investigation (FBI) Robert S. Mueller, said, "Terrorism remains the FBI's top priority. But in the not too distant future, we anticipate that the cyber threat will pose the number one threat to our country."[30] As critical infrastructures continue to be influenced by

advances in technology, opportunities for exploitation will also rise. It is clear that even basic compromises to critical infrastructures would have far reaching, detrimental consequences. Risk managers should constantly be mindful of the ways new devices can introduce new risk, and be confident in the security features before introducing the device into work processes.

This research note specifically brought to light potential concerns challenging energy – a critical infrastructure that if compromised will affect every other sector. As the threat of state sponsored attacks increases, risk managers should take the time to research the other critical infrastructures, and understand how compromises in each infrastructure could potentially impact their organization and prepare and implement appropriate remediation plans.

References

[1] "Critical Infrastructure." *Homeland Security.* n. dat. Web. 5 June 2012. <http://www.dhs.gov/files/programs/gc_1189168948944.shtm>
[2] Ferran, Lee and Jason Ryan. "DHS Deploys Special Teams to Battle Hackers in Cyber War for Infrastructure." *ABC News.* 4 Aug. 2010. Web. 5 June 2012. <http://www.theintelshop.com/2010/08/dhs-takes-steps-to-correct.html>
[3] Critical Infrastructure. n. pag.
[4] Critical Infrastructure. n. pag.
[5] Critical Infrastructure. n. pag.
[6] Critical Infrastructure. n. pag.
[7] Falco, Joe, Karen Scarfone, and Keith Stouffer. "Guide to Industrial Control Systems (ICS) Security." *National Institute of Standards and Technology.* June 2011. p. 1. Web. 6 June 2012. <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
[8] Falco. p. 1.
[9] Falco. p. 1.
[10] Naraine, Ryan. "Shodan Search Exposes Insecure SCADA Systems." *Zdnet.com.* 2 Nov. 2010. Web. 6 June 2012. <http://www.zdnet.com/blog/security/shodan-search-exposes-insecure-scada-systems/7611>
[11] Goodin, Dan. "Hackers tap SCADA Vuln Search Engine." *The Register.* 2 Nov. 2010. Web. 6 June 2012.<http://www.theregister.co.uk/2010/11/02/scada_search_engine_warning/>
[12] "Shodan Finds Computers." *Shodan.com.* n. pag. Web. 6 June 2012. <http://www.shodanhq.com/help/tour>
[13] Goodin, n. pag.
[14] "Industrial Control Systems Cyber Emergency Response Team." *Homeland Security.* n. dat. Web. 6 June 2012. <http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Fact_Sheet_02c.pdf>
[15] Industrial Control, n. pag.
[16] Ferran, n. pag.
[17] "What is Smart Grid and why is it Important." *Nema.com.* n. dat. Web. 6 June 2012. <http://www.nema.org/gov/energy/smartgrid/whatIsSmartGrid.cfm>
[18] What is Smart Grid, n. pag.
[19] Barak, Sylvie. "National Security Threat: Hacking the Smart Grid." *EDN.com* 5 April 2012. Web 6 June 2012. <http://edn.com/electronics-news/4370539/National-security-threat-hacking-the-smart-grid>
[20] Barak, n. pag.
[21] Meserve, Jeanne. "'Smart Grid' may be Vulnerable to Hackers." *CNN Tech.* 20 Mar. 2009. Web. 7 June 2012. <http://articles.cnn.com/2009-03-20/tech/smartgrid.vulnerability_1_smart-grid-power-grid-blackout?_s=PM:TECH>
[22] Meserve, n. pag.

[23] "The Economic Impacts of the August 2003 Blackout." *Electronic Consumers Resource Council.* 9 Feb. 2004. Web. 7 June 2012. p. 1. <http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf>

[24] The Economic Impacts, p. 1.

[25] The Economic Impacts, p. 1.

[26] Meserve, n. pag.

[27] Meserve, n. pag.

[28] Goodin, n. pag.

[29] "ICS-CERT Alert." *Industrial Control Systems Cyber Emergency Response Team.* 28 Oct. 2010. Web. 7 June 2012. <http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf>

[30] "Speeches." *Federal Bureau of Investigation.* RSA Cyber Security Conference, San Francisco, CA. 1 Mar. 2012. Web. 7 June 2012. <http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>