A Situational Awareness Framework for Securing the Smart Grid using Monitoring Sensors and Threat Models

Anastasia Mavridou*

Institute for Information Security,
University of Tulsa,
800 S. Tucker Dr., Tulsa, OK 74104, USA
E-mail: anastasia-mavridou@utulsa.edu
*Corresponding author

Victor Zhou

Institute for Information Security,
University of Tulsa,
800 S. Tucker Dr., Tulsa, OK 74104, USA
E-mail: victor-zhou@utulsa.edu

Jerald Dawkins

True Digital Security,
5110 S Yale Ave., Suite 310, Tulsa, OK 74133, USA
E-mail: jdawkins@truedigitalsecurity.com

Mauricio Papa

Institute for Information Security,
University of Tulsa,
800 S. Tucker Dr., Tulsa, OK 74104, USA
E-mail: mauricio-papa@utulsa.edu

Abstract: Security, access control and risk mitigation in the Smart Grid are matters of great impact for this important sector of the critical infrastructure. Situational awareness requires a means of aggregating information and presenting that information in a manner conducive to assessing risk. While major components of the electric power grid were traditionally deployed in physically isolated networks, they are now utilizing IP–based, open, interconnected networks to transmit and manage the Supervisory Control and Data Acquisition (SCADA) messages. Unfortunately, SCADA protocols used for communications and the systems that implement those protocols were not originally designed with security in mind. Therefore, in order to enhance security and detect potential malicious behavior, Smart Grid operators need detailed and accurate information about the status, integrity,

configuration and network topology of SCADA devices as well as information about any threats that may impact the grid. This paper describes a comprehensive framework that provides situational awareness (SA) for SCADA devices and their operations in a Smart Grid environment. Situational awareness is achieved by processing information collected by monitoring sensors and understanding threats that may affect operations. The proposed framework employs a threat modeling methodology to support this mission.

Keywords: Cyber Security, Situational Awareness, Threat Modeling, Monitoring System, Smart Grid, SCADA

Biographical notes: Anastasia Mavridou is a graduate student in Computer Science and a graduate researcher at the Institute for Information Security (iSec) at The University of Tulsa. She holds a Dipl.-Ing degree in Electrical and Computer Engineering from the Aristotle University of Thessaloniki, Greece. Her research interests include information security, cyber-physical systems security, critical infrastructure protection and rigorous system design.

Victor Zhou is an undergraduate student majoring in Computer Science at The University of Tulsa. He is a research assistant at the Critical Infrastructure Protection lab at the Institute for Information Security (iSec). His interests include computer network security and industrial applications of computer systems.

Dr. Dawkins is CEO and Founder of True Digital Security and has extensive experience in regulatory compliance, technical risk assessments, penetration testing, vulnerability analysis, and secure coding. Dr. Dawkins has authored numerous publications on network security and attack modeling, presented at national and international conferences, and conducted security briefings for private- and public-sector organizations.

Dr. Papa is an Associate Professor of Computer Science and the Director of the Institute for Information Security (iSec) at The University of Tulsa. His main areas of interest are: process control systems security, network security and distributed systems. As an NSA Center of Excellence, iSec has the overriding goal of helping execute the national agenda for securing computer networks and information systems. Dr. Papa leads several iSec initiatives in information assurance research, education and public awareness.

1 Introduction

The reliable operation of power grids is highly dependent on industrial control systems. Meanwhile, initiatives such as modernization of power grids, increased number of corporate network interconnections, and the Smart Grid are rapidly changing the threats that industrial control systems face. Therefore, there is a growing interest in understanding the security implications SCADA environments pose so that security provisions can be developed to address not only intended

attacks to these environments but also inadvertent compromises due to equipment failures, user errors, and natural disasters.

The power grid was originally designed to use large central generation sources with predictable power flow directions using only one-way communication channels. As a result, it is already considered to be an outmoded, inefficient, vulnerable infrastructure (DoE, 2008). There have been at least five massive blackouts over the past 40 years (DoE, 2008) that illustrate some of the problems associated with the power grid. These blackouts have occurred mainly due to faults at power stations, damage to power lines, substations or other parts of the distribution system, unusually high demand and others. Also, a cyber attack may have a significant impact in the functionality of the power grid which may result in a massive blackout. In fact, the massive North East blackout of 2003 has been linked to the propagation of the MSBlaster worm (CERT, 2003) (Verton, 2003). Although electric utilities require 24x7 availability, the present power grid may not be able to recover quickly from all types of security breaches. There is a strong need to address these issues.

Therefore, the higher demand for quality and availability, penetration of renewable energy resources, increased threat of terrorist attacks and a growing need to minimize environmental impact have given birth to what is called the Smart Grid. The Smart Grid is expected to deliver electricity from multiple suppliers to end consumers using two-way communications, involve multiple distributed intelligent entities and include large-scale real-time data collection capabilities (NETL, 2009). This large-scale data collection capability and fusion of the monitored processes of the Smart Grid can be used to provide situational awareness (SA), a capability that has been identified by the National Institute of Standards and Technology (NIST) as a high priority. In particular, NIST states that "the goals of situational awareness are to understand and ultimately optimize the management of power-network components, behavior, and performance, as well as to anticipate, prevent, or respond to problems before disruptions can arise" (NIST, 2010).

In order to achieve such a lofty goal, two approaches must be undertaken, a top-down and a bottom-up approach. A top-down strategy provides the analytical rigor necessary to interpret and understand threats. While a bottom-up information processing approach offers technical detail used to feed analysis efforts. This paper describes a SA architecture intended to provide Smart Grid operators with both a top-down and a bottom-up approach to evaluating their systems. The paper builds on previous work described in (Mavridou et al., 2012). Threat modeling is leveraged in order to access and characterize the systems and threats involved. In addition, an architecture is proposed to provide a detailed view of the network topology along with information about the configuration, status, critical states and traffic of SCADA devices.

2 Smart Grid Architecture

Once electricity is generated, whether by burning fossil fuels, by harvesting wind, solar, geothermal and hydro energy, or by nuclear fussion, it is generally sent through high-voltage transmission lines to step down transmission substations where it is transformed into a lower voltage and sent through lower-voltage distribution lines to end consumers. Operators manage electric power flow using

6 Conclusions

The proposed framework provides a robust and sophisticated environment for situational awareness. This is achieved by the use of both monitoring services and threat models that can be tuned for a specific environment, i.e. SCADA systems in the Smart Grid. Monitoring services, responsible for reporting raw data to a central location, are the "eyes" of the system and provide basic sensory-information. On the other hand, threat modeling is the enabling mechanism to evaluate possible system vulnerabilities. Together they provide the necessary constructs to understand, at an abstract level, the security posture of such systems, the operational risks and possible mitigation strategies. In addition, in cases where regulations dictate what is being done to secure the environment, i.e. NERC-CIP reliability standards, the framework has already shown value in auditing and compliance efforts.

7 Acknowledgments

This material is based on research sponsored by DARPA under agreement number FA8750-09-1-0208. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

References

Anonymous, (2011) 'Penetration Testing Execution Standard (PTES)', Available from www.pentest-standard.org/index.php/Main_Page [Accessed 1 July 2011].

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., Ning, P., Ou, X., Song, D., Strater, L., Swarup, V., Tadda, G., Wang, C., Yen, J., (2010) 'Cyber SA: Situational Awareness for Cyber Defense', *Springer*.

Brundage, M., Mavridou, A., Johnson, J., Hawrylak, P.J., and Papa, M., (2012) 'Distributed Monitoring: A Framework for Securing Data Acquisition', Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection: Approaches for Threat Protection, *IGI Global*.

CERT, (2003) 'Advisory CA-2003-20 W32/Blaster Worm', Carnegie Mellon University's Computer Emergency Response Team, Available from http://www.cert.org/advisories/CA-2003-20.html [Accessed 25 April 2011].

Curtis, K., (2005) 'A DNP3 Protocol Primer (Revision A)', Available from www.dnp.org/About/DNP3%20Primer%20Rev%20A.pdf [Accessed 25 April 2011].

DoE (2008) 'The Smart Grid: An Introduction', U.S. Department of Energy, Available from http://www.oe.energy.gov/1165.htm. [Accessed 25 April 2011].

DoE, (2009) 'Study of Security Attributes of Smart Grid Systems Current Cyber Security Issues', U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

Dykstra, T., Fuller, E., Hoagberg, M. P., Miles, G., and Rogers, R., (2004) 'Security Assessment: Case Studies for Implementing NSA IAM', Available from www.isecom.org/osstmm/ [Accessed 1 July 2011].

EPRI, (2008) 'DNP Security Development, Evaluation and Testing Project Opportunity', Electric Power Research Institute.

FERC, (2009) 'Smart Grid Policy', Federal Energy Regulatory Commission Available from http://www.ferc.gov/whats-new/comm-meet/2009/071609/E-3.pdf [Accessed 1 August 2011].

FERC, (2011) Federal Energy Regulatory Commission, Available from http://www.ferc.gov/about/ferc-does.asp [Accessed 1 October 2011].

GAO, (2011) 'ELECTRICITY GRID MODERNIZATION: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed', U.S. Government Accountability Office.

Mavridou, A., and Papa, M., (2012) 'A situational awareness architecture for the smart grid', Global Security, Safety and Sustainability & e-Democracy, *Springer*.

Microsoft, (2005) 'The STRIDE Threat Model', Available from http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx [Accessed 1 October 2011].

NCS, (2004) 'Supervisory Control and Data Acquisition (SCADA) Systems', National Communications System, *Technical Information Bulletin NCS TIB 04-1.*

NERC, (2010) 'Reliability Standards for the Bulk Electric Systems of North America', North American Electric Reliability Corporation, Available from http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf. [Accessed 1 October 2011].

NERC, (2011) North American Electric Reliability Corporation, Available from http://www.nerc.com [Accessed 1 October 2011].

NETL, (2007) 'The NETL Modern Grid Initiative Powering our 21st-Century Economy: MODERN GRID BENEFITS', National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

NETL, (2008) 'Advanced Metering Infrastructure', National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

NETL, (2009) 'The NETL Modern Grid Initiative Powering our 21st-Century Economy: A COMPENDIUM OF SMART GRID TECHNOLOGIES', National Energy Technology Laboratory for the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

NETL, (2011) National Energy Technology Laboratory, Available from http://www.netl.doe.gov/about/ [Accessed 1 October 2011].

NIST, (2010) 'NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0', National Institute of Standards and Technology, *NIST Special Publication 1108*.

NIST, (2010) 'NISTIR 7628, Guidelines for Smart Grid Cyber Security', National Institute of Standards and Technology.

OpenVAS, (2011) Available from http://www.openvas.org/ [Accessed 1 October 2011].

OSVDB, (2011) The Open Source Vulnerability Database, Available from http://osvdb.org/ [Accessed 1 October 2011].

President Obama, (2009) 'Remarks by the President on Securing our Nation's Cyber Infrastructure', Available from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ [Accessed 25 April 2011].

Snyder, W., and Swiderski, F., (2004) 'Threat Modeling', *Microsoft Press*.

Verton, D., (2003) 'Blaster Worm Linked to Severity of Blackout', *Computerworld*.