Chapter 17
Distributed Monitoring:
A Framework for Securing Data Acquisition

Matthew Brundage
The University of Tulsa, USA

James Johnson
The University of Tulsa, USA

Anastasia Mavridou
The University of Tulsa, USA

Peter J. Hawrylak
The University of Tulsa, USA

Mauricio Papa
The University of Tulsa, USA

ABSTRACT

SCADA systems monitor and control many critical installations around the world, interpreting information gathered from a multitude of resources to drive physical processes to a desired state. In order for the system to react correctly, the data it collects from sensors must be reliable, accurate, and timely, regardless of distance and environmental conditions. This chapter presents a framework for secure data acquisition in SCADA systems using a distributed monitoring solution. An overview of the framework is followed by a detailed description of a monitoring system designed specifically to improve the security posture and act as a first step towards more intelligent tools and operations. The architecture of the Smart Grid is used to analyze and evaluate benefits that the proposed monitoring system can provide. Finally, the effects and use of Radio Frequency Identification (RFID) and ZigBee as data acquisition platforms are discussed in the context of the proposed solution.

INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems (NCS, 2004) form the backbone of industries in the areas of electric power, oil and gas, water, and rail transportation. They have been identified by the EU Commission and the U.S. Department of Homeland Security as a core component of most critical infrastructures (Brunner, & Suter, 2008). SCADA systems provide real-time centralized monitoring and control of industrial processes through a combined use of data acquisition and transmission systems and Human-Machine Interfaces (HMIs). In the past, SCADA systems were considered to be secure due to the use of proprietary equipment and software as well as the limited network connectivity and isolation of these systems. However, during

DOI: 10.4018/978-1-4666-5942-1.ch017

Copyright © 2014, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

recent years, continued SCADA modernization and increased interconnection have resulted in a transition from closed, isolated networks to open, IP-based networks. Therefore SCADA systems are now considered to be part of the cyber infrastructure (DHS & DoE, 2007). The increased interconnection has made SCADA systems more vulnerable to attacks and has introduced new security risks. As a result, there is a pressing need to mitigate these risks.

Currently, in industry, there are several SCADA protocols in use. In the electric sector, the most popular are the International Electrotechnical Commission (IEC) 60870-5-101 (IEC, 2003), commonly referred to as 101, and the Distributed Network Protocol version 3 (DNP3) (Curtis, 2005). IEC is also developing 61850 to provide guidelines for the secure automation and operation of electrical substations. Security in SCADA implementations is a major concern because many SCADA protocols in use today are still operating in unauthenticated clear text. While there is a significant effort to enhance SCADA protocols with security functionality, for example the DNP3 SA (secure authentication) (Gilchrist, 2008), the majority of systems in the industry sector still use clear text. As a result, in order to enhance the security of SCADA systems and detect any suspicious behavior, SCADA communication networks need to be monitored to provide operators with accurate and timely information about the network devices and their interactions. In particular, a distributed monitoring system will be able to verify that the incoming information is accurate, as well as provide a foundation to support development of more powerful tools such as intrusion detection systems and packet filtering components.

This chapter uses the Smart Grid domain and relevant components in the energy sector to illustrate security concerns in SCADA systems. Although utilities in the electric sector require 24x7 availability, they may not be able to recover quickly and efficiently from all security breaches. Thus, a cyber-attack in this sector can have destructive results. Such an attack on SCADA systems located in the power grid can have a significant impact in the functionality of the grid. In fact, the massive North East Blackout has been linked to the propagation of the MSBlaster worm in 2003 (Verton, 2003; CERT, 2003). Also, the recently discovered W32.Stuxnet rootkit (Falliere, Murchu, & Chie, 2011) is an example of malware targeting Industrial Control Systems (ICS). Falliere (2010) notes that, "Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems."

In particular, this chapter contributes a recommended security practice of a monitoring structure for the purpose of improving SCADA security. The proposed distributed monitoring system addresses the important issue of secure data acquisition. This will provide system operators with the information needed for (i) a more intelligent response to incoming information and (ii) increased awareness of possible malicious activity in an environment outside of the control of the SCADA system. The Smart Grid is used as a case study to demonstrate the benefits such a distributed monitoring system could provide.

BACKGROUND

SCADA systems and their communications are currently at a critical point in time, as cyber-attacks become more common and these systems are becoming increasingly interconnected (Craig, Mortensen & Dagle, 2008). A brief overview of the security risks, standards, encryption and authentication, and functionality of the systems will be given.

SCADA Systems

SCADA systems (NCS, 2004) are used to monitor and control critical infrastructures such as energy,

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/distributed-monitoring/107735

Related Content

Educational and Cultural Identities in Virtual Social Networks
Wajeeh Daher (2012). *International Journal of Cyber Ethics in Education (pp. 57-70).*
www.irma-international.org/article/educational-and-cultural-identities-in-virtual-social-networks/90237

Online Knowledge Sharing
Will W.K. Ma (2012). *Encyclopedia of Cyber Behavior (pp. 394-402).*
www.irma-international.org/chapter/online-knowledge-sharing/64770

Teachers' Certification on Basic Computer Skills
Christos X. Christakoudis, George S. Androulakisand Charalampos Zagouras (2012). *International Journal of Cyber Ethics in Education (pp. 12-23).*
www.irma-international.org/article/teachers-certification-basic-computer-skills/74786

Telepresence, Flow, and Behaviour in the Virtual Retail Environment
Saïd Ettis (2014). *User Behavior in Ubiquitous Online Environments (pp. 173-195).*
www.irma-international.org/chapter/telepresence-flow-and-behaviour-in-the-virtual-retail-environment/81174

Integrating Smartphone Talking Applications, Trust, Switching Cost and Customer Switching Behaviour in the Mobile Phone Market: The Case of Egypt
Ali Abdelkader (2019). *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications (pp. 285-303).*
www.irma-international.org/chapter/integrating-smartphone-talking-applications-trust-switching-cost-and-customer-switching-behaviour-in-the-mobile-phone-market/220947