SCADA Threats in the Modern Airport

John McCarthy, ServiceTec, Cranfield University, Cranfield, England
William Mahoney, University of Nebraska Omaha, Omaha, NE, USA

ABSTRACT

Critical infrastructures are ubiquitous in the modern world and include electrical power systems, water, gas, and other utilities, as well as trains and transportation systems including airports. This work is concerned with Supervisory Control and Data Acquisition (SCADA) systems that are at the heart of distributed critical infrastructures within airports. Modern airports are highly competitive cost driven operations that offer a range of public and private services. Many airport systems such as car parking and building control systems are SCADA controlled. This is achieved with sensors and controllers monitored over a large, geographically disperse area. To increase efficiency and to achieve cost savings, SCADA systems are now being connected to information technology system networks using TCP/IP. The merging of SCADA systems into the main IT network backbone is presenting new security problems for IT security managers. Historically, proprietary solutions, closed systems, ad-hoc design and implementation, and long system life cycles have led to significant challenges in assessing the true security posture of SCADA systems. To address this, this work seeks how SCADA systems are being integrated into the IT network within a modern airport. From this new standpoint we will be able to identify ways in which SCADA may be vulnerable to malicious attack via the IT network. The results of this work could offer solutions to increase security within airports.

Keywords: Airport Terminals, Control Systems, Distributed Security, Information Technology (IT) Networks, Supervisory Control and Data Acquisition (SCADA)

INTRODUCTION

Supervisory Control and Data Acquisition (SCADA) systems act as the hidden computer equipment behind large infrastructures that are essential to maintaining the quality of our life. These infrastructures include electrical power grids, water purification and delivery, gas, and other utilities, as well as trains and transportation systems. Legacy SCADA systems, planned and implemented possibly decades ago, were either not designed to be secure, or were designed with “security through obscurity”. In the design and analysis of these systems, features such as physical isolation and technical uniqueness greatly reduced the possibility of cyber attacks. But this is no longer true with newly designed SCADA systems, and it is no longer as true with legacy systems that might now be connected to corporate networks.

DOI: 10.4018/ijcwt.2013100104
With long product lifecycles, SCADA systems often become a quilt work of different hardware, operating systems, applications, and software. Meanwhile, due to the continuous availability requirements of such arrangements, operating system and software updates are often not applied. Over time the system components may no longer even be supported for updates, leading to potential vulnerabilities that can be exploited at the component level. At the network level, vulnerabilities are inadvertent, due to the usual misconfigured firewall or router, but also via deliberate interconnections between a SCADA network and the company or utility IT structure. While the replacement of older devices with new devices solves the problem of the lack of software updates, newer devices allow low cost Internet Protocol (IP) based communications, nullifying the uniqueness that once provided some of the security.

Due to the nature of the computing equipment—often legacy software/hardware—as well as the criticality of the services which these systems control, some SCADA systems are coming under increasing regulatory oversight. In the United States, the International Electrotechnical Commission (IEC) standard 61850 [IEC10] is one such standard; the NERC (North American Electric Reliability Corporation) also produces standards in this area (NERC, 2012). Nearly 1,700 of the 3,200 power utilities in the United States have some type of SCADA system in place, and it is estimated that one quarter of these utilities have no separation between the corporate network and the system control network (Lemos, 2009). Special publications from NIST 800-82 (NIST, 2008) are designed for securing SCADA systems. NIST 800-53 guidelines (NIST, 2007) have been extended to include SCADA related improvements in the specification of its controls, along with a wide discussion of control system vulnerabilities. The 800-53 standards now include a description of their applicability to control systems and their vulnerabilities. Other SCADA implementations are coming under greater regulation as well. For example the petroleum and gas refining systems are subject to regulatory issues, and are now asked to secure pipeline and other infrastructure in their API 1164 standard (API, 2009).

But these regulations have not entered much of the transportation sector. An obvious distributed system using SCADA would be the railroad industry. However, an equally, if not more important transportation system which relies on SCADA is the world’s airports. In particular, airport SCADA systems control a wide variety of terminal facilities and are not currently scrutinized with respect to regulatory standards. This paper is concerned with an examination of the deployment of SCADA systems in a major airport.

The paper is organized as follows: the following section provides a brief set of examples of SCADA security issues to demonstrate the severity of the problem. We use section three to relate the SCADA threat to the modern airport industry. The authors recently visited a major North American airport facility and have comments regarding the visit in section four. Suggestions for increased security are offered in section five, and our conclusions follow.

**SCADA THREATS AND BREACHES**

There are many examples of SCADA systems gone awry that will illustrate the severity of the problem, as well as demonstrate the wide variety of critical infrastructure devices controlled by these types of systems. Among the SCADA critical infrastructure failures which are often cited, include the following.

A water treatment plant near Harrisburg, PA was attacked in 2006. The hacker planted malicious software into the control systems and could potentially have altered or stopped the operation of the treatment plant (ABC, 2006). The water treatment facility in Queensland’s Maroochy Shire was accessed by a disgruntled past employee named Vitek Boden, who used a wireless connection into the pumping and valve system to route millions of gallons of untreated sewage into a creek adjacent to a hotel (Wyld, 2004). Another often cited example is the train...
Related Content

Understanding Optimal Investment in Cyber Terrorism: A Decision Theoretic Approach
[www.igi-global.com/article/understanding-optimal-investment-cyber-terrorism/64311?camid=4v1a](www.igi-global.com/article/understanding-optimal-investment-cyber-terrorism/64311?camid=4v1a)

Formulating the Building Blocks for National Cyberpower
[www.igi-global.com/article/formulating-the-building-blocks-for-national-cyberpower/185601?camid=4v1a](www.igi-global.com/article/formulating-the-building-blocks-for-national-cyberpower/185601?camid=4v1a)
Cyber Espionage and Illegitimate Information Retrieval
www.igi-global.com/article/cyber-espionage-and-illegitimate-information-retrieval/152232?camid=4v1a

A Supplementary Intervention to Deradicalisation: CBT-Based Online Forum
www.igi-global.com/chapter/a-supplementary-intervention-to-deradicalisation/213318?camid=4v1a