SCADA Threats in the Modern Airport

John McCarthy
Oxford Systems
John.mccarthy@oxfordsystems.co.uk

William Mahoney
University of Nebraska at Omaha
wmahoney@unomaha.edu

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: Distributed Security, Airport Terminals, Control Systems, 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.

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 system in Poland. Four vehicles were derailed when a teenage boy hacked into the SCADA equipment controlling the track switches, using a modified television remote control (Leyden 2008).
Similarly a disruption of freight and commuter train traffic near Washington D.C. in August of 2003 was determined to be caused by the signalling systems being infected with the Sobig virus (Krutz 2006). US investigators reportedly found evidence in computer logs discovered at Afghanistan Al Qaeda camps showing that members spent time on websites offering software and programming instructions for the digital switches that run power grids (Kramarenko 2004). In March of 2007 the US Department of Homeland Security, in what was widely disseminated on various video sharing sites, demonstrated the remote destruction of a power generator. The generator was sent commands telling it to operate beyond the capabilities of the design. (Meserve 2007). A company whose software and services are used to remotely administer and monitor large sections of the energy industry has warned customers that it is investigating a sophisticated hacker attack spanning its operations in the United States, Canada and Spain. Telvent Canada Ltd. said that on Sept. 10, 2012 it learned that attackers installed malicious software into "OASyS SCADA", a product that helps energy firms connect to "smart grid" technologies (Krebs 2012). Faulty software caused the gates holding back the Torrens Lake, in South Australia, to open when not commanded to do so (Hale 2012). The gates remained open for two hours, completely draining the lake. Officials had purchased faulty software from Ottoway System Integration, a firm that went out of business only days after the incident. While not caused by foul play, outsiders who have remote access to these types of control systems can cause similar damage. A recent attack in 2013 saw the transport network in Israel severely disrupted after an attack on the control barriers that access a major tunnel in the city of Haifa (Security 2013).

SCADA networks are the fundamental foundations of our society and lifestyle, yet are infamously difficult to secure, due to the complexity of their architectures. We next turn to the transportation industry, specifically to SCADA systems used at airports for terminal operations.

Modern Aviation and Cyber Security

In the USA post post-9/11 environment, there are a constant variety of threats, even though many of the security recommendations provided by the National Commission on Terrorist Attacks upon the United States have been put into place. Leon Panetta, the one-time Director of the Central Intelligence Agency, testified in June 9, 2011 to the U.S. Senate. In his statement he acknowledged emerging technology threats:

> *There is no question that the whole arena of cyber attacks, developing technologies in the information area represent potential battlefronts for the future. I have often said that there is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems (Panetta 2011).*

To emphasize this, Bob Cheong, Chief Information Security Officer of the Los Angeles Airport, report that a variety of cyber-attacks in Los Angeles have occurred in the last several years: there were over 6,400 attempts to hack into a new file server two days after it was deployed; in a one-year period, nearly 59,000 Internet misuse and abuse attempts were blocked; finally, in that same one-year period, 2.9 million hacking attempts were blocked (Cheong, 2011, p. 5).

In relation to post-9/11 aviation security, the Transportation Security Administration (TSA) has placed focus on security checkpoints and finding potential threats through bomb-sniffing technology, terrorist watch lists, increased use of in-flight security officers, full-body-scanners, positive baggage matching, and hardened cockpit doors (Mann, 2011; Poole, Jr., 2008, p. 4). Interestingly according to Bruce Schneider, a security expert, these activities are not meant to actually secure travelers from would be attackers, but are put in place to instill confidence – the more visible the perceived obstruction the more confident the public can feel about flying (Mann, 2011). This opinion is shared by the authors.

Beyond physical security at airports, and with respect to Secretary of Defense Panetta's views on the emergence of cyber attacks as a primary concern, many are turning their eyes to securing the technology that is utilized during the day-to-day operations of airports. Dominic Nessi, the Deputy Executive Director and Chief Information Officer of Los Angeles World Airports, acknowledges the challenges to the information technology (IT) expert trying to secure an international airport (Nessi 2011):

> *Organizations, including airports, are rapidly trying to balance the desire for users to have mobile applications and mobile hardware with the new security risks that they bring. The bottom line is that the hardware and new application evolves faster than the preventative measures that an organization needs to take can be developed. … The makeup of an airport's system and the network total make airports a target. Because of the types of systems that we have in an airport, we're going to have a lot of exposure just by virtue of the system itself. We can mitigate most of our vulnerabilities through good cyber security measures (McAllister, 2011, p.18).*

In October of 2011, Mr. Nessi delivered an address to the Airports Council International of North America outlining the cyber security threats facing airports, the potential vectors that might be used in an attack, and tactics for securing known vulnerabilities. Amongst Nessi's

threats were several that were focused on external airport operations, such as external airport or airline websites, concession point-of-sale, credit card transaction information, and

passenger's wireless devices. However, the overall impact of cyber-attacks on systems external to airport operations is small when compared to attacks on systems required to perform internal airport operations. Nessi points out several potential targets within this realm, including: access control and perimeter intrusion systems, eEnabled aircraft systems, radar systems, wireless and wired network systems, and network-enabled baggage systems. Obviously, a variety of vulnerabilities occur within cyberspace because of humans, hardware, software, and connection points that provide access to such systems. Nessi's system of assessing threats is similar to the United States Computer Emergency Readiness Team (US-CERT) and National Institute of Standards and Technology's (NIST) cyber vulnerability assessment guidance. US-CERT has provided a "high level overview" of cyber vulnerabilities for control systems (US-CERT 2012). Within this overview, US-CERT includes the following vulnerabilities: wireless access points, network access points, unsecured SQL databases, poorly configured firewalls, interconnected peer networks with weak security, and several others.

An Examination of a Major Hub Airport in North America

Since the publication of Nessi's work there has been much discussion within the airport sector in relation to security measures. Action has been taken and one of the authors of this paper is on a panel commissioned by the Federal Aviation Agency to determine best cyber practice in airports.

However, when examining a major hub airport in North America the authors have found that the critical driver for increased security within the actual terminal building has been the implementation of Payment Card Industry (PCI) compliance regulations for secure credit card transactions. PCI has forced many airports to upgrade and improve security measures or face the loss of revenue from credit card transaction processing. Without this driver the increase in security measures would have been considerably slower.

There was also a widely held belief that the SCADA systems in the airport were isolated from the main IT backbone. Often the car parking and baggage control systems were separated from the main IT network by hardware firewalls. These firewalls were "assumed" secure by IT staff and it was often unclear who had responsibly for the managing and configuration of these firewalls. Additional services could be added to the network without all relevant IT staff being aware of the changes. There appeared to be no overarching group or committee that had a direct focus on cyber security measures despite the considerable size of the airport. Security measures were left in multiple hands and ad hoc systems were assumed isolated due to previous hardware and software configurations without ongoing checks and testing.

Since our original examination of the terminal and the networking infrastructure, the news has been that now the aviation industry, and airports in particular, are being targeted by Spear-Phishing attacks. Given our discovery concerning the lack of the overarching group we had anticipated would be in charge, this is a serious finding as there is no way to know the training or security background of the airport employees that might receive these email attacks. These emails are not targeting monetary gain but information about the computers and networks available form the point of attack (Public 2013). Specifically, Trend Micro

reports that an older malware package – Sikypot – is resurfacing and specifically targeting the aviation industry (Wilson 2013). The malware is typically delivered by the Spear Phishing email directly to persons in the civilian aviation sector and "Like most targeted attacks,

Sykipot uses malicious attachments to spread. Once Sykipot is running on the victim's machine, it establishes an SSL connection to a [command and control] server, where more malicious files are then downloaded and installed on the victim's machine. The capabilities of the Sykipot framework allow for arbitrary code and commands to be run."

The reason that Spear Phishing is successful is that it works (FireEye 2012). "Spear Phishing emails had an open rate of 70 percent, compared with an open rate of just three percent for mass spam emails. Further, 50 percent of recipients who open Spear Phishing emails also click on the enclosed links, which is 10 times the rate for mass mailings." If an airport employee on the inside of the network opens the email links the separation between the airport networks may be eliminated, or information concerning the layout of the network may be retrievable by third parties through the follow-up attacks on that person's computer. Given that the security in place in the airport which we examined is primarily due to PCI, one has to wonder how many of the airport employees and kiosk operators are checking their email on the inside of the PCI air gap.

Assuming that the network is not a target of email attacks, one key element of PCI compliance is the use of penetration testing. This helps secure systems, at least from the casual port scanner. Regarding penetration testing and internal airport operations, there are examples of airport cyber security lapses and known weaknesses. AirTight Networks, tested wireless security at fourteen airports in the United States, Canada and Asia (AirTight 2008). One of the study's findings was that "77 percent were non-hotspot (i.e. private) networks and of those, 80 percent were unsecured or using legacy WEP encryption, a fatally flawed protocol." These Wi-Fi networks encompassed ticketing systems, baggage systems, shops, and restaurants. The implications of such a breach could be that a person infiltrates these weakly secured systems and wreaks logistical havoc on an airport, potentially bringing one airport to a standstill. Sri Sundaralingham of AirTight was quoted as saying:

> *Imagine the ripple effect at an airport like Heathrow or O'Hare if someone could work their way into the baggage transiting system and reroute luggage all over the world. It could bring the system to a grinding halt with both economic and security consequences.*

Securing Critical Information Systems

Nessi's assessment settles on four components within an airport that are vulnerable to cyber attack, each "require a different approach to security: the network, the device, the application, and the back-end system". His resolutions for securing such systems is by primarily focusing on process, culture, staffing, and training. Specifically, he recommends continuous software configuration management for software and hardware, and following established updating protocols; "social engineering awareness" campaigns educating staff on proper use of software, hardware and access points and potential exploits that expose human error and provide access to unauthorized persons; and performing penetration testing by both those with internal access and by external, third-parties such as external audits by Department of Homeland Security employees or approved vendors. Finally,

Nessi is a supporter of recruiting the right security personnel and continuing their training, opting for Certified Information Systems Security Professional (CISSP) certification.

Cheong suggests it is essential that airports have a cyber security team (Cheong, 2011, p. 4). Additionally, Mirko Montanari, Roy H. Campbell, Krishna Sampigethaya and Mingyan

Li have published paper “A Security Policy Framework for eEnabled Fleets and Airports”, which was updated in 2011. Their premise is that future airports will be “highly net-centric system-of-systems with advanced networking and wireless technology to accommodate the ‘eEnabled aircraft,’ enhanced surface area operations, as well as growing business and societal demands” (p.1). The eEnabled concept essentially allows airports and airplanes to remain interconnected through a variety of key pieces of network infrastructure. This includes check-in systems, transaction devices, baggage handling, et al. become part of the eEnabled airport. It is therefore clear that the problem will become more complex as these systems integrate and evolve.

Conclusions

The challenge as always is to find “a balance between the protection capability and cost, performance, and operations considerations” (National Security Agency). This creates a challenge of balancing needs versus operational functionality. If security requirements hinder operations, then there is no true value in implementing security. However if operational functionality is not secured and vulnerabilities are exploited, operations can cease and you have another extreme situation. Balancing both requires wisdom and the correct security strategy.

With regard to securing airport networks, stopping all attacks is nearly impossible; therefore a plan should be put into place to recover from exploitations. Experts recommend having a Computer Incidence Response Team - “a carefully selected and well-trained group of people whose purpose is to promptly and correctly handle an incident so that it can be quickly contained, investigated, and recovered from” (SANS Institute, 2001, p. 2).

Modern airport security has been impacted by the horrific events of September 11, 2001. After this tragedy, aviation physical security has received much of the focus by the government, media and public, while critics would suggest that these actions don’t make us more secure, they merely make us feel safer based on our perceptions. Experts would argue that aviation security should focus holistically on real threats to civilian aviation, including cyber security. Because of the ubiquity of network-enabled airports connected both internally and externally network security is paramount to ensuring international transportation safety. A variety of strategic frameworks can be used by airport information security managers to ensure that vulnerabilities are minimized. Both CERT and NIST provide guidance on establishing importance of key assets and utilizing resources to preserve them. Both Dominic Nessi and Bob Cheong, aviation cyber security experts for LAWA lay out the security required and how to balance that security based on a specific strategic framework. Nessi focuses on securing access control and perimeter intrusion systems, eEnabled aircraft systems, radar systems, wireless and wired network systems, and network-enabled baggage systems. And Bob Cheong points out that confidentiality, integrity, availability, and non-repudiation must be considered when securing an airport’s network. The basic principles of security have not changed they simply must be integrated

into wider networks and working practices.

References

ABC (2006) “Hackers Penetrate Water System Computers”, http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html

AirTight Networks (2008, March 3). “AirTight study at worldwide airports reveals wireless security risks for travelers and airport operations”. Retrieved from http://www.airtightnetworks.com/home/news/press-releases/pr/browse/4/select_category/8/article/123/airtight-study-at-worldwide-airports-reveals-wireless-security-risks-for-travelers-and-airport-opera.html

API (2009) American Petroleum Institute, “Pipeline SCADA Security”, 2nd edition, 06/01/09.

Cheong, B. (2011, October 28). Cyber security at airports. Airports Council International – North America. Retrieved from http://aci-na.org/sites/default/files/cheong-cybersecurity-bit.pdf

FireEye (2012). Spear Phishing Attacks – Why They Are Successful and How to Stop Them. Available from www.fireeye.com.

Hale, Gregory, (2011). “A New Report Details Trends That May Lead To Improvements That Will Help To Protect A System From Attack”, Plant Engineering, at http://www.plantengineering.com/single-article/report-scada-systems-under-siege/c6b4a830db67d2fb9d329b6fd1d04d99.html

IEC (2012). IEC Standards available at http://www.iec.ch/

Kramarenko, D. (2004). “Al Qaeda in cyber space: threats of cyberterrorism”, Computer Crime Resource Center, July 27, 2004, http://www.crime-research.org/news/27.07.2004/515/

Krebs, Brian, (2012). “Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent” at http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

Krutz, R. (2004). Securing SCADA Systems, Wiley, pp 146.

Lemos, R. (2009). “U.S. makes securing SCADA systems a priority” at http://www.securityfocus.com/news/11351/1

Leyden, J. (2008). “Polish teen derails tram after hacking train network”, at http://www.theregister.co.uk/2008/01/11/tram_hack/

Mann, C. C. (2011, December 20). Smoke screening. Vanity Fair. Retrieved from http://www.vanityfair.com/culture/features/2011/12/tsa-insanity-201112

McAllister, B. (2011). How To Be Cyber Secure. Airport Business, 26(12), 18.

Meserve, J. (2007). “Sources: Staged cyber attack reveals vulnerability in power grid”, CNN, September 26, 2007, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

NERC (2012). Standard Processes Manual, at http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Nessi, D. (2011). Are you exposed? The perils of a connected world. Airports Council

International – North America. Retrieved from http://www.aci-na.org/sites/default/files/nessi-areyouexposed-bit.pdf

NIST (2007). NIST 800-53, “Recommended Security Controls for Federal Information Systems”, http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

NIST (2008). NIST SP 800-82, “Guide to Industrial Control Systems (ICS) Security”, Draft for public comment, Sep 29, 2008, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

Panetta, L., Hon. (2011). Hearing to consider the nomination of Hon. Leon E. Panetta to be Secretary of Defense. U.S. Senate, Committee on Armed Services. Retrieved from http://armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf

Poole, R. W., Jr. (2008, December 11). Toward risk-based aviation security policy. International Transport Forum. Retrieved from http://www.internationaltransportforum.org/jtrc/discussionpapers/DP200823.pdf

Public Intelligence (2013, August). At http://publicintelligence.net/fbi-apt-aviation-industry/

SANS Institute. (2001). Computer incident response team. SANS Institute. Retrieved from http://www.sans.org/reading_room/whitepapers/incident/computer-incident-response-team_641

Security Affairs (2013). http://securityaffairs.co/wordpress/19158/cyber-crime/israel-tunnel-cyber-attack.html

US-CERT (2012). Overview of cyber vulnerabilities. US-CERT (United State Computer Emergency Readiness Team). Retrieved from http://www.us-cert.gov/control_systems/csvuls.html

Wilson, Tim (2013). Sykipot Malware Now Targeting Civil Aviation Information. At http://www.darkreading.com/vulnerability/sykipot-malware-now-targeting-civil-avia/240160988

Wyld, B. (2004). “Cyberterrorism: fear factor”, http://www.crime-research.org/analytics/501/