Chapter 6

LESSONS LEARNED FROM THE MAROOCHY WATER BREACH

Jill Slay and Michael Miller

Abstract Supervisory control and data acquisition (SCADA) systems are widely used to monitor and control operations in electrical power distribution facilities, oil and gas pipelines, water distribution systems and sewage treatment plants. Technological advances over the past decade have seen these traditionally closed systems become open and Internet-connected, which puts the service infrastructures at risk. This paper examines the response to the 2000 SCADA security incident at Maroochy Water Services in Queensland, Australia. The lessons learned from this incident are useful for establishing academic and industry-based research agendas in SCADA security as well as for safeguarding critical infrastructure components.

Keywords: SCADA security, Maroochy Water Services breach

1. Introduction

Great concern has been expressed regarding the security of supervisory control and data acquisition (SCADA) systems in the light of the breach that occurred in 2000 at Maroochy Water Services in Queensland, Australia [6, 13]. This paper discusses the Maroochy Water incident and the response to the incident. Lessons learned from the incident, which have not been widely reported, are discussed in this paper. These lessons are useful for establishing academic and industry-based research agendas in SCADA security as well as for safeguarding critical infrastructure components.

2. SCADA Systems

SCADA systems are used for gathering real-time data, monitoring equipment and controlling processes in industrial facilities and public utilities, including chemical plants and refineries, electrical power generation and transmission systems, oil and gas pipelines, and water and sewage treatment plants [9]. Servers,

Slay, J. and Miller, M., 2008, in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston: Springer), pp. 73–82.

which are generally located in the main plant, communicate with sensors and control devices, which may be inside the plant or at remote locations. Sensors and control devices are placed wherever equipment needs to be monitored or controlled. A SCADA network can cover large geographical areas, especially in the case of public utilities.

A SCADA system generally has three types of components:

- **Field Devices:** These devices include sensors and controllers, e.g., remote telemetry units (RTUs) and programmable logic controllers (PLCs). Sensors collect data from various sources. Controllers perform actions (e.g. starting a pump or closing a valve) based on sensor data and control algorithms. RTUs and PLCs are small dedicated devices, which are hardened for outdoor use and industrial environments. They may be interfaced using serial connections or Ethernet. In this paper, field devices are generally referred to as PLCs. However, a field device could be a PLC, an RTU or a combination (as in some plants).

- **Servers:** Servers are responsible for collecting and analyzing various field inputs. They are responsible for raising alarms, starting and stopping processes, and implementing the logic required to automate processes.

- **Clients:** Client machines interact with servers via terminals. Clients are used to monitor the state of a SCADA network. They also have the ability to start and stop processes running within the network.

Australian SCADA systems are often very complex because of the vastness of the country and the remoteness of many of the utility plants and field stations. For example, the networked SCADA system at the ETSA electric utility company in South Australia covers more than 70,000 square miles of terrain. It incorporates 25,000 physical I/O points and in excess of 100,000 tags. The system monitors daily data for current, temperature, power variables, load shedding systems and fire alarms, reducing the response time for dealing with anomalies and faults.

3. The Maroochy Water Services Case

One of the most celebrated SCADA system breaches occurred at Maroochy Water Services on Queensland's Sunshine Coast in Australia [6, 13]. In March 2000, Maroochy Shire Council experienced problems with its new wastewater system. Communications sent by radio links to wastewater pumping stations were being lost, pumps were not working properly, and alarms put in place to alert staff to faults were not going off.

It was initially thought there were teething problems with the new system. Some time later, an engineer who was monitoring every signal passing through the system, discovered that someone was hacking into the system and deliberately causing the problems. In time, the perpetrator, Vitek Boden, a former contractor, was arrested and eventually jailed.

Mr. Boden used a laptop computer and a radio transmitter to take control of 150 sewage pumping stations. Over a three-month period, he released one million liters of untreated sewage into a stormwater drain from where it flowed to local waterways. The attack was motivated by revenge on the part of Mr. Boden after he failed to secure a job with the Maroochy Shire Council.

The Maroochy Water Services case has been cited around the world as an example of the damage that could occur if SCADA systems are not secured. The incident was mentioned in a recent report on IT security by the U.S. President's Information Technology Advisory Committee [13].

This SCADA security incident also has to be viewed in the context of Australian data on cyber crime, particularly network security breaches. Electronic attacks on 127 Australian companies surveyed in 2003 [1] resulted in increases in financial losses of 20% over 2002, bringing the average loss to approximately $116,000 per company. The survey also revealed that organizations that were part of Australia's critical information infrastructure reported greater losses (50%) compared with organizations that were not part of the infrastructure (42%). Other key findings were that more organizations experienced attacks on the confidentiality, availability and integrity of computer systems and data in 2004 than did in 2003. The percentage of organizations affected was up from 42% in 2003 to 49% of those surveyed in 2004. Most attacks were sourced externally (88%), but fewer organizations experienced external attacks than in 2003 (91%). Infections due to viruses, worms and Trojans were most common, accounting for 45% of total losses in 2004. Other prevalent forms of electronic crime were fraud, followed by abuse and misuse of computer network access or resources.

4. SCADA Security

SCADA systems are used by 270 utilities in the United States [4]. Since this amounts to roughly eighty percent of U.S. power facilities, the risk of system-wide failure and the resulting economic loss are very high. For example, during the August 25, 2003 power outage in North America, more than 100 power plants were shut down, affecting 50 million people in the U.S. and Canada. Also, it led to the closure of ten major airports and the New York City subway system. This emphasizes the need to protect SCADA systems, especially from targeted cyber attacks.

Oman and co-workers [11] stress the importance of securing SCADA systems at a time when the terrorist threat level is high. A major concern is malicious actors gaining remote access to substations at various points in power grid, and then launching large-scale attacks throughout the infrastructure. Oman and colleagues also discuss how an "open" SCADA network can be penetrated in a relatively easy manner.

SCADA security has been highlighted in a recent report by the U.S. President's Information Technology Advisory Committee [13]. The FBI has also reinforced the need to secure SCADA networks, especially as several nation states and other actors are attempting to develop information warfare capabilities.

Utilities are prime targets for attackers because shutting them down can have a large-scale societal impact. Since SCADA systems are vital to plant operations, it is crucial to secure them to the extent possible [5].

The U.S. National Communication System [9] has identified that interconnections between SCADA networks and corporate networks increases the risk and the consequences of attack. There is a false impression that a SCADA system is safe because it is in a separate closed network. As networks become interconnected for convenience and for business reasons, an attacker who enters a corporate network can tunnel into a SCADA system, and potentially target any device.

Byres [3] has emphasized that increased interconnectivity means that hacker attacks are not the only threat. In January 2003, the Slammer worm infiltrated an Ohio nuclear power plant and several other power utilities. Byres identified four relatively innocuous entry points used by the worm:

- Contractor's T1 line (affected a power plant computer)
- Virtual private network (affected a power company SCADA system)
- Laptop (affected a petroleum plant control system)
- Dial-up modem (affected a paper plant human-machine interface (HMI)).

These infiltration points demonstrate that many SCADA systems are being connected to the Internet without consideration of security. Once it is connected to a corporate network, a SCADA network becomes vulnerable to worms and viruses originating from the Internet.

The U.S. Department of Energy's Office of Energy Assurance [10] lists several strategies for improving the security of SCADA systems. It recommends the use of evaluations, audits and surveys to identify weak points, which must then be strengthened to protect against intrusions. Many security problems can be reduced, if not eliminated, using administrative approaches, e.g., developing documentation about the SCADA system, specifying policies and procedures, and conducting periodic assessments. Similar approaches have been proposed by Sandia researchers [16]. They maintain that identifying security problems and performing a risk assessment should be the first step in securing a SCADA system. Moreover, before implementing any security controls, it is important to have a clear understanding of the architecture and configuration of the SCADA system.

Riptech [14], the security services firm, which was acquired by Symantec in 2002, identified three major misconceptions about SCADA security: (i) SCADA systems reside on physically-separate, stand-alone networks; (ii) SCADA systems are protected from corporate networks using strong access controls; and (iii) SCADA systems require specialized knowledge, which makes them difficult for intruders to access and exploit. The Riptech document asserts that these statements applied when SCADA systems, with their proprietary hardware, software and protocols, were located in isolated networks. The statements do

not hold at present, especially as corporate networks are often connected to SCADA systems.

Symantec [17] has specified a network architecture that incorporates various security controls, including firewalls to protect corporate and SCADA-client terminals from attacks originating from the Internet. Of course, due to network connectivity, it is usually the case that multiple entry points exist into SCADA systems; therefore, it is important that all entering traffic be screened.

In general, there is heightened awareness about SCADA systems and the need to secure them from attacks from insiders as well as external entities. Numerous research and development efforts have been initiated on SCADA security. Comprehensive solutions are needed that can address security in SCADA systems that comprise legacy components, proprietary hardware and software, as well as commodity computing and network equipment. Because of the scale of SCADA systems, the solutions should be relatively inexpensive. Moreover, they must not adversely impact plant operations.

5. Australian Efforts

The Australian Department of Communications, Information Technology and the Arts (DCITA) [7] has launched an effort to convince senior management of the potential risks to their SCADA systems and has recommended various physical, logical and administrative controls for managing risk. DCITA has also held a series of workshops across the country targeting SCADA owners and operators as well as academic researchers to spur research and developments focused on SCADA security. The Australian government recently initiated an effort through the Attorney General's Department called the Trusted Information Sharing Network for Critical Infrastructure Protection, which has a major focus on SCADA security.

We have worked with an Australian SCADA integrator to develop a security architecture for SCADA systems with modern and legacy components [15]. The goals of the security architecture (Figure 1) are to prevent or minimize system attacks while reducing overhead that could impact control functions. The architecture is inspired by the defense-in-depth philosophy. It incorporates security mechanisms and the application of policies and procedures to create a secure SCADA environment.

Security mechanisms consume network resources and add communications overhead. Therefore, it is important to ensure that they do not affect the real-time performance of the SCADA system.

The principal security controls are implemented at the boundary of the network. The security gateway situated at the network boundary includes a firewall, intrusion detection system and anti-virus software. The three mechanisms provide distinct layers of security that screen suspicious network traffic. In particular, incoming traffic must satisfy the firewall rules, not raise any alarms in the intrusion detection system, and pass the anti-virus checker.

A demilitarized zone (DMZ) separates the SCADA system from the corporate network. Shared resources are placed in the DMZ; for example, corporate

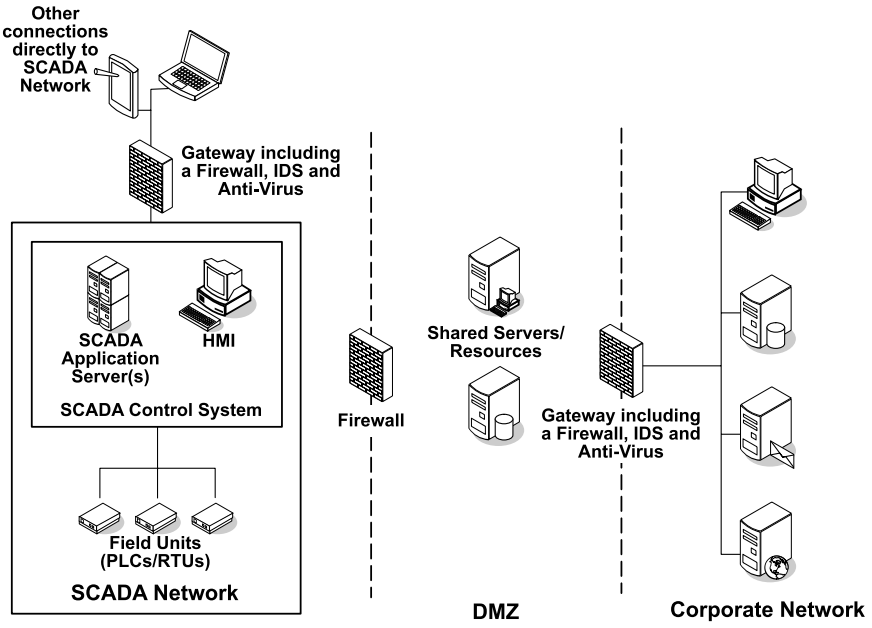

Figure 1. Proposed security architecture.

network users can obtain plant and control data by querying a DMZ historian without having to access the SCADA system.

A second firewall is located between the SCADA system and DMZ. Since entering traffic has already been screened at the gateway, this firewall can be relatively simple. However, if a corporate partner has direct access to the DMZ, then a gateway with substantial security functionality should be implemented at the boundary of the SCADA system and DMZ.

Firewalls screen all traffic entering and leaving the SCADA network, and are an inexpensive but effective security solution [2]. They eliminate direct connections from the Internet, restrict access from the corporate network, control traffic entering from wireless access points, and screen access in the case of remote connections (e.g., those used by maintenance personnel). Other important security solutions include network management and administration (e.g., managing user accounts and passwords) and addressing protocol-level vulnerabilities.

6. Lessons Learned

As we reflected on our work [15], we were challenged to consider if our solution – had it been implemented at Maroochy Water Services – would have prevented or deterred Vitek Boden from attacking the SCADA system.

Robert Stringfellow, who was the civil engineer in charge of the water supply and sewage systems at Maroochy Water Services during the time of the breach,

has presented his analysis in closed forums. The best open source discussion of Mr. Stringfellow's views is provided by Mustard [8], which we consider in our analysis.

The Maroochy SCADA system employed two monitoring stations and three radio frequencies to control the operations of 142 sewage pumping stations. The faults that occurred when the system was being investigated (prior to the discovery of the hacking attacks) included:

- Unexplained pump station alarms
- Increased radio traffic that caused communication failures
- Modified configuration settings for pump station software
- Pumps running continually or turned off unexpectedly
- Pump station lockups and pumps turned off without any alarms
- Computer communication lockups and no alarm monitoring

Stringfellow commented that at first it was easier to blame installation errors for the problems. However, upon reinstalling all the software and checking the system, he noticed that pump station settings kept changing beyond the ability of the system to do this automatically. He, therefore, concluded that an external malicious entity was responsible. With the help of advanced monitoring tools, Stringfellow determined that a hacker was using wireless equipment to access the SCADA system. At one point, Stringfellow actually "dueled" with the attacker as he was connecting to pump stations from his laptop.

Stringfellow's analysis of the incident made several important points. First, it is very difficult to protect against insider attacks. Second, radio communications commonly used in SCADA systems are generally insecure or are improperly configured. Third, SCADA devices and software should be secured to the extent possible using physical and logical controls; but it is often that case that security controls are not implemented or are not used properly. Finally, SCADA systems must record all device accesses and commands, especially those involving connections to or from remote sites; this requires fairly sophisticated logging mechanisms.

Stringfellow also recommended the use of anti-virus and firewall protection along with appropriate use of encryption. He emphasized a need for upgradeable SCADA systems (from a security perspective), proper staff training, and security auditing and control.

Our research [15] indicates that several technical solutions are already available for securing SCADA systems. The solutions vary in their coverage and may not be very robust; nevertheless, they are good starting points for implementing security in SCADA systems.

Due to their specialized architecture, protocols and security goals, it is not appropriate to simply apply IT security techniques and tools to SCADA systems. Instead, it is important to design security solutions catered specifically to

SCADA systems. For example, tools that understand SCADA protocols and are designed to operate in industrial environments would be able to identify and block suspicious traffic in a more efficient and reliable manner.

Peterson [12] discusses the need for specialized intrusion detection systems for SCADA networks. Most existing systems only pick up traditional attacks, e.g., an attacker attempting to gain control of a server by exploiting a Windows vulnerability; effective intrusion detection systems must also incorporate SCADA attack signatures. Likewise, SCADA-aware firewalls must also be developed; their specialized SCADA rule sets would greatly enhance the blocking and filtering of suspicious packets.

Peterson [12] also emphasizes the need for logging activities and events in SCADA systems. Logs can provide valuable information pertaining to attacks. This includes information about the escalation of user privileges in SCADA applications, failed login attempts, and disabled alarms and changed displays, which could fool operators into believing that a system is running normally.

In addition to investing in security techniques, mechanisms and tools, it is imperative to focus on the human aspects of SCADA security. Staff must be well-trained and should be kept abreast of the latest security practices, exploits and countermeasures. Security policies and procedures should be developed, refined periodically, and applied consistently. Only the combination of technological solutions and human best practices can ensure that SCADA systems are secure and reliable.

7. Conclusions

SCADA systems control vital assets in practically every critical infrastructure sector. Given the ubiquity of SCADA systems and their inherent vulnerabilities, strong efforts should be taken by asset owners and operators to secure SCADA systems, especially those comprising legacy components, proprietary hardware and software, and commodity computing and network equipment, which expose the entire system to external attacks. Since the Maroochy Water Services breach, numerous research and development efforts have been initiated on SCADA security. Some of the most successful efforts have involved significant collaboration between academic researchers, vendors, owners and operators, and government agencies. But these efforts should be broader and more sustained. Moreover, security solutions should be effective, reliable and economically viable, and should not adversely impact operations.

The incident at Maroochy Water Services is a prime example of the kind of attack that can be launched on SCADA systems. The incident was serious, but it was caused by a lone hacker who attacked just one system in a single infrastructure. One can only imagine – at a time when terrorist threat levels are high – how much devastation could result from large-scale coordinated attacks on SCADA systems throughout the interconnected critical infrastructure sectors.

References

[1] Australian Computer Emergency Response Team, 2004 Australian Computer Crime and Security Survey (www.auscert.org.au/render.html?it=2001), 2005.

[2] British Columbia Institute of Technology, Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, National Infrastructure Security Co-ordination Centre, London, United Kingdom, 2005.

[3] E. Byres and J. Lowe, The myths and facts behind cyber security risks for industrial control systems, presented at the *VDE Congress*, 2004.

[4] J. Fernandez and A. Fernandez, SCADA systems: Vulnerabilities and remediation, *Journal of Computing Sciences in Colleges*, vol. 20(4), pp. 160–168, 2005.

[5] General Accounting Office, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, Report to Congressional Requesters, GAO-04-354, Washington, DC, 2004.

[6] G. Hughes, The cyberspace invaders, *The Age*, June 22, 2003.

[7] IT Security Advisory Group, SCADA security: Advice for CEOs, Department of Communications, Information Technology and the Arts, Canberra, Australia (www.dcita.gov.au/communications_for_business/security/critical_infrastructure_security/key_documents), 2005.

[8] S. Mustard, Security of distributed control systems: The concern increases, *Computing and Control Engineering Journal*, vol. 16(6), pp. 19–25, 2005.

[9] National Communications System, Supervisory Control and Data Acquisition (SCADA) Systems, Technical Information Bulletin NCS TIB 04-1, Arlington, Virginia, 2004.

[10] Office of Energy Assurance, 21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, Washington, DC, 2002.

[11] P. Oman, E. Schweitzer and D. Frincke, Concerns about intrusions into remotely accessible substation controllers and SCADA systems, *Proceedings of the Twenty-Seventh Annual Western Protective Relay Conference*, 2000.

[12] D. Peterson, Intrusion detection and cyber security, *InTech*, May 2004.

[13] President's Information Technology Advisory Committee, Cyber Security: A Crisis of Prioritization, Report to the President, National Coordination Office for Information Technology Research and Development, Arlington, Virginia, 2005.

[14] Riptech, Understanding SCADA system security vulnerabilities (www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf), 2001.

[15] J. Slay and M. Miller, A security architecture for SCADA networks, *Proceedings of the Seventeenth Australasian Conference on Information Systems*, 2006.

[16] J. Stamp, P. Campbell, J. DePoy, J. Dillinger and W. Young, Sustainable security for infrastructure SCADA, Sandia National Laboratories, Albuquerque, New Mexico (www.sandia.gov/scada/documents/SustainableSecurity.pdf), 2003.

[17] Symantec, Understanding SCADA system security vulnerabilities (www4.symantec.com/Vrt/offer?a_id=20249), 2004.