

Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia

Marshall D. Abrams, The MITRE Corporation
Joe Weiss, Applied Control Solutions, LLC

Annual Computer Security Applications
Conference

December 2008



NIST Industrial Control System (ICS) Cyber Security Project

- **Objective: to improve the cyber security of federally owned/operated ICS**
- **ICS pervasive throughout all critical infrastructures**
- **Improve the security of public and private sector ICS**
 - **Work with voluntary industry standards groups (e.g., The Instrumentation, Systems, and Automation Society – ISA)**
 - **Assist in ICS cyber security standards and guideline development**
 - **Foster ICS cyber security standards convergence**
 - **Raise the level of ICS security through R&D and testing**
- **Purpose of case studies is to focus in on factors otherwise overlooked, not to ascribe any blame**

NIST Cyber Security Strategic Vision

- **Promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act (FISMA)**
- **Build a solid foundation of information security across one of the largest information technology infrastructures in the world based on comprehensive security standards and technical guidance.**
- **Institutionalize a comprehensive Risk Management Framework that promotes flexible, cost-effective information security programs for federal agencies.**
- **Establish a fundamental level of “security due diligence” for federal agencies and their contractors based on minimum security requirements and security controls.**

The Current Landscape

- Public and private sector enterprises today are **highly dependent** on information systems to carry out their missions and business functions.
- Developments in ICS have seen these traditionally closed systems become open and internet-connected, thus putting the national services critical **infrastructure at risk**.
- To achieve mission and business success, enterprise information systems must be **dependable** in the face of serious cyber threats.
- To achieve information system dependability, the systems must be appropriately **protected**.

The Threat Situation

- **ICS are becoming more open making them vulnerable to intentional and unintentional cyber threats**
- **Effects of errors and omissions increasingly catastrophic**
- **Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated**
- **Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with intentions of compromising information systems**
- **Significant exfiltration of critical and sensitive information and implantation of malicious software occurring on a regular basis**
- **Largely untutored work force with little interest in IT security**
- **ICS community diverse using different protocols (many archaic)**

NIST ICS Project Deliverables

- Support public & private sectors, and standards organizations that want to use NIST Standards & Guidelines for ICS
- Evolve SP 800-53 *Recommended Security Controls for Federal Information Systems* to better address ICS
 - Revision 2 published December 2007
 - Revision 3 first public draft scheduled for (end of) December 2008
- Develop SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*
 - Second draft September 2007
 - Final in 2009

Case Study Overview

- **Examine actual control system cyber event**
 - **Resulted in significant environmental and economic damage**
 - **Malicious attack by knowledgeable insider, who had been a trusted contractor employee**
 - **Timelines, control system response, and control system policies**
- **Identify operating policies and procedures that were missing or had readily identifiable cyber security vulnerabilities**
- **Identify NIST SP 800-53 management, operational, and technical safeguards or countermeasures that, if implemented, could have prevented or ameliorated the event**

Attack Synopsis

- **Vitek Boden worked for Hunter Watertech, an Australian firm that installed SCADA radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia (a rural area of great natural beauty and a tourist destination)**
 - **Applied for a job with the Maroochy Shire Council**
 - **Walked away from a “strained relationship” with Hunter Watertech**
 - **The Council decided not to hire him**
 - **Boden decided to get even with both the Council and his former employer**
- **On at least 46 occasions issued radio commands to the sewage equipment**
 - **Caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel**
 - **Marine life died, the creek water turned black and the stench was unbearable for residents**

Time Line

- **1997-December 1999 – Boden employed by Hunter Watertech**
- **December 3, 1999 – Boden resigns from Hunter Watertech**
- **Early December 1999 – Boden seeks City Council employment**
- **Early January 2000 – Boden turned down**
- **February 9-April 23, 2000 – SCADA system experiences series of faults**
- **March 16, 2000 – Hunter Watertech investigator tried to troubleshoot system**
- **April 19, 2000 – Log indicates system program had been run at least 31 times**
- **April 23, 2000 – Boden disabled alarms at four pumping stations using the identification of pumping station 4.**
- **April 23, 2000 – Boden pulled over by police with computer equipment in car**
- **October 31, 2001 – Boden convicted in trial – sentenced to 2 years**
- **March 21, 2002 – Appeal rejected**

Evidence Found in Boden's Vehicle

■ Laptop

- Reloaded February 28, 2000
- Software used in the sewerage system (re)installed February 29
 - Run at least 31 times prior to April 19
 - Last run on April 23

■ Motorola M120 two-way radio same type used in the Council's system

- Tuned into the frequencies of the repeater stations
- Serial numbers matched delivery docket provided by the supplier of the radios to Hunter Watertech

■ PDS Compact 500 computer control device

- Address set to spoof pumping station
- Serial number identified it as a device which should have been in the possession of Hunter Watertech

Observations (1/2)

- **Boden was an insider who was never an employee of the organization he attacked**
 - Employee of contractor that supplied IT/control system technology
 - With his knowledge he was the “ultimate insider”
- **Contractor’s responsibilities unstated or inadequate**
 - Management, technical and operational cyber security controls
 - Personnel security controls
 - Background investigations
 - Protection from disgruntled employees
- **As a skillful adversary, Boden was able to disguise his actions**
 - A number of anomalous events occurred before recognition that the incidents were intentional
 - Extensive digital forensics were required to determine that a deliberate attack was underway
- **No existing cyber security policies or procedures**
- **No cyber security defenses**

Observations (2/2)

- **Difficult to differentiate attacks from malfunctions**
- **When/why is it important to determine whether intentional attack, or unintentional flaw or error?**
- **Difficult to protect against insider attacks**
- **Radio communications commonly used in SCADA systems are often insecure or improperly configured**
- **SCADA devices and software should be secured to the extent possible using physical and logical controls**
- **Security controls often not implemented or used properly**
- **Generally SCADA systems lack adequate logging mechanisms for forensic purposes**
- **Also recommended**
 - **Anti-virus** • **Firewall protection** • **Appropriate use of encryption**
 - **Upgrade-able SCADA systems (from a security perspective)**
 - **Proper staff training** • **Security auditing and control.**

SP 800-53 Security Control Classes, Families, and Identifiers

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

SP 800-53 Pervasive Cyber Security Prophylactic Controls

PROBLEM	CONTROL FAMILY
Policy and Procedures	The first control in every control family addresses policy and procedure.
Personnel Security	Personnel Security (PS)
Hardware & Software	System and Services Acquisition (SA)
Awareness and Training	Awareness and Training (AT)
Audit	Audit and Accountability (AU)
Contingency Planning	Contingency Planning (CP)
Incident Response	Incident Response (IR)
Cryptographic Protection	System and Communications Protection (SC)

SP 800-53 Controls for Malicious Activities

MALICIOUS ACTIVITY	CONTROL FAMILY
Issuing radio commands	Access Control (AC) Identification and Authentication (IA)
Falsifying network address	Access Control (AC)
Sending false data and instructions	System and Information Integrity (SI)
Disabling alarms	

Access Control (AC)

- A combination of access controls would have alleviated or prevented the attack
- Tightly coupled with Identification and Authentication

<u>AC-1</u>	<u>Access Control Policy and Procedures</u>	AC-11	Session Lock
<u>AC-2</u>	<u>Account Management</u>	AC-12	Session Termination
<u>AC-3</u>	<u>Access Enforcement</u>	<u>AC-13</u>	<u>Supervision and Review— Access Control</u>
<u>AC-4</u>	<u>Information Flow Enforcement</u>	AC-14	Permitted Actions without Identification or Authentication
AC-5	Separation of Duties	AC-15	Automated Marking
<u>AC-6</u>	<u>Least Privilege</u>	AC-16	Automated Labeling
<u>AC-7</u>	<u>Unsuccessful Login Attempts</u>	<u>AC-17</u>	<u>Remote Access</u>
AC-8	System Use Notification	<u>AC-18</u>	<u>Wireless Access Restrictions</u>
AC-9	Previous Logon Notification	<u>AC-19</u>	<u>Access Control for Portable and Devices</u>
AC-10	Concurrent Session Control	AC-20	Use of External Information Systems

Learning From the 2000 Maroochy Shire Cyber Attack

- **Public record of an intentional, targeted attack by a knowledgeable person on an industrial control system teaches us to consider:**
 - **Critical physical, administrative, and supply chain vulnerabilities**
 - **Vulnerabilities coming from suppliers or others outside the organization**
 - **Contractor and sub-contractor personnel as a potential attack source**
- **Need to be concerned with both inside & outside attack**
- **Difficulty in identifying a control system cyber incident as a malicious attack and retaking control of a “hijacked” system**
- **A determined, knowledgeable adversary could potentially defeat most controls**
- **Structured defense-in-depth security is best**

Additional Information

■ Authors

- Marshall Abrams <abrams@mitre.org>
- Joe Weiss <joe.weiss@realtimeacs.com>

■ Incident

- See references in paper

■ Case Study

- <http://csrc.nist.gov/sec-cert/ics/papers.html>

■ NIST Industrial Control System Security Project

- <http://csrc.nist.gov/sec-cert/ics/index.html>

■ NIST Project Managers

- Stu Katzke <stuart.katzke@nist.gov>
- Keith Stouffer <keith.stouffer@nist.gov>