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

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

August 2008

MITRE

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.
- NIST standards and guidelines are voluntarily used by the private sector

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**
- **Develop SP 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security***
  - **Second draft September 2007**
  - **Final in 2008**

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)

Security Policy and Procedures

- SP 800-53 policy and procedure controls
  - The first control in every control family is policy and procedure
  - The organization develops, disseminates, and periodically reviews/updates:
    - a formal, documented, <*family*> policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance
    - formal, documented procedures to facilitate the implementation of the <*family*> policy and associated <*family*> controls.

Personnel Security (PS)

- **No personnel security requirements on contractor**

PS-1	Personnel Security Policy and Procedures	PS-5	Personnel Transfer
PS-2	Position Categorization	PS-6	Access Agreements
PS-3	Personnel Screening	PS-7	Third-Party Personnel Security
PS-4	Personnel Termination	PS-8	Personnel Sanctions

- **PS-7 identifies need for contractual obligations**
- **Other controls candidates for inclusion**
  - **Key personnel clause**
  - **Sometime contractors treated same as employees**
  - **Example: PS-4 exit interview might have identified potential malicious action**

Controls that would have helped are underlined

System and Services Acquisition (SA)

- **Contractor supplied hardware & software**
- **No indication that any System and Services Acquisition family (SA) controls were in contract**

SA-1	System and Services Acquisition Policy and Procedures	SA-7	User Installed Software
SA-2	Allocation of Resources	SA-8	Security Engineering Principles
SA-3	Life Cycle Support	SA-9	External Information System Services
SA-4	Acquisitions	SA-10	Developer Configuration Management
SA-5	Information System Documentation	SA-11	Developer Security Testing
SA-6	Software Usage Restrictions		

- **Example SA-11 required tests for resistance to penetration**

Awareness and Training (AT)

- **No security training had been provided to staff**

AT-1	Security Awareness and Training Policy and Procedures	AT-4	Security Training Records
AT-2	Security Awareness	AT-5	Contacts with Security Groups and Associations
AT-3	Security Training		

- **People are one of the weakest links in cyber security**
- **Robust awareness and training program is paramount to ensuring that people understand cyber security responsibilities, organizational policies, and how to properly use and protect the resources entrusted to them**
- **All individuals should receive specialized training focused on their responsibilities and the application rules**

Audit (AU)

- System lacked sufficient audit capability
- Audit supports other control families such as incident response, access control, and flaw remediation.

AU-1	Audit and Accountability Policy and Procedures	AU-7	Audit Reduction and Report Generation
AU-2	Auditable Events	AU-8	Time Stamps
AU-3	Content of Audit Records	AU-9	Protection of Audit Information
AU-4	Audit Storage Capacity	AU-10	Non-repudiation
AU-5	Response to Audit Processing Failures	AU-11	Audit Record Retention
AU-6	Audit Monitoring, Analysis, and Reporting		

- Recording and analyzing remote access might have led to quicker determination of malicious activity

Contingency Planning (CP)

- All the analysis indicates that there were no plans to deal with an emergency or system disruption

CP-1	Contingency Planning Policy and Procedures	CP-6	Alternate Storage Site
CP-2	Contingency Plan	CP-7	Alternate Processing Site
CP-3	Contingency Training	CP-8	Telecommunications Services
CP-4	Contingency Plan Testing and Exercises	CP-9	Information System Backup
CP-5	Contingency Plan Update	CP-10	Information System Recovery and Reconstitution

- Existing plans for dealing with natural disasters and equipment breakdowns should be augmented for deliberate attacks, physical and cyber

Incident Response (IR)

- Response to the sewerage discharge was ad hoc
  - Considerable time elapsed during troubleshooting before malicious intent was considered

IR-1	Incident Response Policy and Procedures	IR-5	Incident Monitoring
IR-2	Incident Response Training	IR-6	Incident Reporting
IR-3	Incident Response Testing and Exercises	IR-7	Incident Response Assistance
IR-4	Incident Handling		

- All incident response controls contribute to
  - Rapidly detecting incidents
  - Minimizing loss and destruction
  - Mitigating the weaknesses that were exploited
  - Restoring services
  - Apprehending malefactors

System and Communications Protection (SC)

- Cryptographic protection recommended
  - Supports identification and authentication (I&A)

SC-1	System and Communications Protection Policy and Procedures	SC-13	Use of Cryptography
SC-9	Transmission Confidentiality	SC-17	Public Key Infrastructure Certificates

- Recent U.S. government policy
- *Protection of Sensitive Agency Information*, OMB M-06-16, June 23, 2006, specifies
  - Full disk encryption
  - Two factor authentication

Other SC controls not relevant to cryptography

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

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

Access Control Examples

- Radio access (AC-18) limited to
  - Specific hardware devices
  - Authorized persons and processes
- Authorization & credentials require management (AC-2)
- Authorized persons granted only those privileges necessary to do their job (AC-6)
- Audit log review uncover unexpected access (AC-13)

Identification & Authentication (IA)

- **Physical possession of radio and computer should not have been sufficient**

IA-1	Identification and Authentication Policy and Procedures	IA-5	Authenticator Management
IA-2	User Identification and Authentication	IA-6	Authenticator Feedback
IA-3	Device Identification and Authentication	IA-7	Cryptographic Module Authentication
IA-4	Identifier Management		

- **Techniques for hardware (radio) I&A**
  - **Shared known information (e.g., Media Access Control (MAC))**
  - **Organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP))**

System & Information Integrity (SI)

- Unauthorized activity could have been detected

SI-1	System and Information Integrity Policy and Procedures	SI-7	Software and Information Integrity
SI-2	Flaw Remediation	SI-8	Spam Protection
SI-3	Malicious Code Protection	SI-9	Information Input Restrictions
SI-4	Information System Monitoring Tools and Techniques	SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-5	Security Alerts and Advisories	SI-11	Error Handling
SI-6	Security Functionality Verification	SI-12	Information Output Handling and Retention

- Commands that led to dumping raw sewerage
  - Detected
  - Validated

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>