

Cyber Incidents Involving Control Systems

Robert J. Turk

October 2005



The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-05-00671

Cyber Incidents Involving Control Systems

Robert J. Turk

October 2005

**US-CERT Control Systems Security Center
Idaho Falls, Idaho 83415**

**Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**

US-CERT Control Systems Security Center

Cyber Incidents Involving Control Systems

INL/EXT-05-00671

October 12, 2005

Approved by:



Robert J. Turk
Author/Systems Engineer



Date



George A. Beitel
Consulting Engineer/Scientist
SCADA/Power Systems



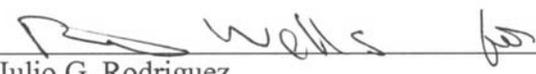
Date



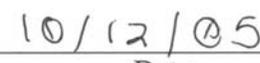
Fred C. Cowart
Program Manger of CSSC
US-CERT Control Systems Security Center



Date



Julio G. Rodriguez
Program Area Lead
SCADA/Power Systems



Date



EXECUTIVE SUMMARY

The Analysis Function of the US-CERT Control Systems Security Center (CSSC) at the Idaho National Laboratory (INL) has prepared this report to document *cyber security incidents*^a for use by the CSSC. The description and analysis of incidents reported herein support three CSSC tasks: establishing a business case; increasing security awareness and private and corporate participation related to enhanced cyber security of control systems; and providing informational material to support model development and prioritize activities for CSSC.

The stated mission of CSSC is to reduce vulnerability of critical infrastructure to cyber *attack* on control systems. As stated in the Incident Management Tool Requirements (August 2005) “Vulnerability reduction is promoted by risk analysis that tracks actual risk, emphasizes high risk, determines risk reduction as a function of countermeasures, tracks increase of risk due to external influence, and measures success of the vulnerability reduction program.”

Process control and Supervisory Control and Data Acquisition (SCADA) systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wreaked so much havoc on corporate information systems. New research indicates this confidence is misplaced—the move to open standards such as Ethernet, Transmission Control Protocol/Internet Protocol, and Web technologies is allowing hackers to take advantage of the control industry’s unawareness. Much of the available information about cyber incidents represents a characterization as opposed to an analysis of events. The lack of good analyses reflects an overall weakness in reporting requirements as well as the fact that to date there have been very few serious cyber attacks on control systems. Most companies prefer not to share cyber attack incident data because of potential financial repercussions. Uniform reporting requirements will do much to make this information available to Department of Homeland Security (DHS) and others who require it.

This report summarizes the rise in frequency of cyber attacks, describes the perpetrators, and identifies the means of attack. This type of analysis, when used in conjunction with vulnerability analyses, can be used to support a proactive approach to prevent cyber attacks. CSSC will use this document to evolve a standardized approach to incident reporting and analysis. This document will be updated as needed to record additional event analyses and insights regarding incident reporting.

This report represents 120 *cyber security incidents* documented in a number of sources, including: the British Columbia Institute of Technology (BCIT) Industrial Security Incident Database, the 2003 CSI/FBI Computer Crime and Security Survey, the KEMA, Inc., Database, Lawrence Livermore National Laboratory, the Energy Incident Database, the INL Cyber Incident Database, and other open-source data. The National Memorial Institute for the Prevention of Terrorism (MIPT) database was also interrogated but, interestingly, failed to yield any cyber attack incidents.

a. Italicized terms are defined in the Glossary in Appendix A.

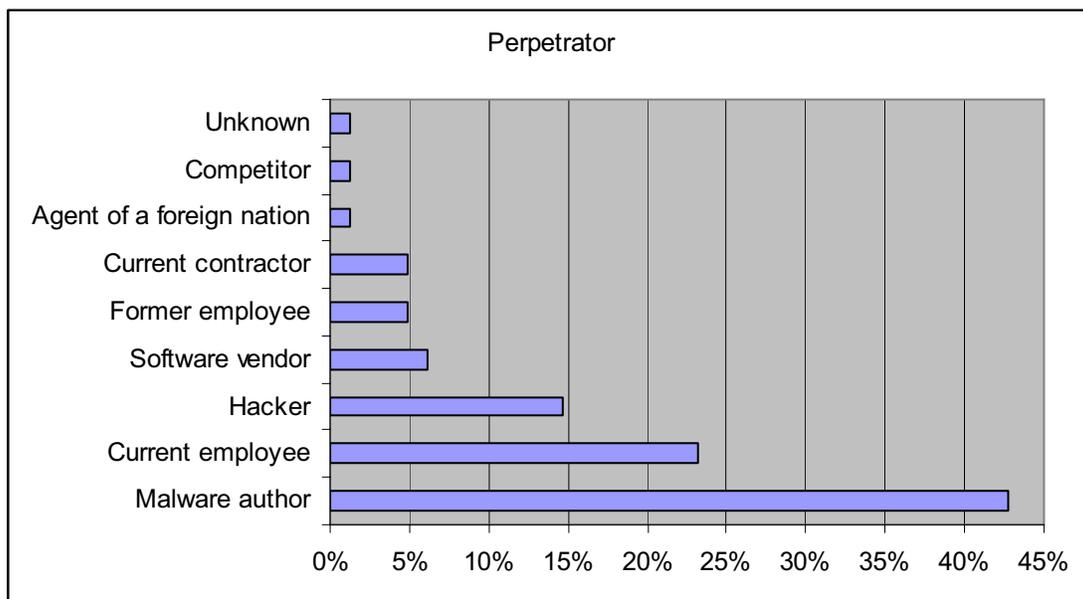
The results of this evaluation indicate that historical evidence provides insight into control system related incidents or failures; however, that the limited available information provides little support to future risk estimates. The documented case history shows that activity has increased significantly since 1988. The majority of incidents come from the Internet by way of opportunistic *viruses*, *Trojans*, and *worms*, but a surprisingly large number are directed acts of sabotage. A substantial number of confirmed, unconfirmed, and potential events that directly or potentially impact control systems worldwide are also identified. Twelve selected cyber incidents are presented at the end of this report as examples of the documented case studies (see Appendix B).

Summary of Cyber Security Incidents

One hundred and twenty cyber security incidents considered for this report were evaluated for type, origin, perpetrator, and motivation. The following list presents the analysis results representing the highest percentage entry in each area:

- 42% of all incidences were conducted by means of *mobile malware*
- 61% of the perpetrators originated from external sources
- 43% of perpetrators backgrounds were *malware authors*
- 43% had a motivational intention of malware infection.

An example of additional detail regarding perpetrators accumulated across all 120 incidents is presented in the following chart.



As depicted, and at this time, the combination of insiders such as contractors, former employees, and current employees are responsible for less incidents than the malware authors

who write *spyware*. Trojans and viruses generally use evolved methods to send exploit code across the internet or other networks.

Assessing the consequences of industrial cyber attacks is not simply a case of assigning a financial value to an incident. Although there are obvious direct impacts that may be easily quantifiable financially (e.g., loss of production or damage to the plant), other consequences may be less obvious. For most companies, the impact on reputation, subsequently reflected in loss of stock value, is probably far more significant than the mere cost of a production outage. The impacts of health, safety, or environmental incidents could be highly detrimental to a company's brand image. Even impacts such as minor regulatory contraventions may in turn affect a company's reputation, thereby threatening their license to operate.

For most of the reported incidents, the contributors have been unable (or unwilling) to provide a financial measure of the impact of the industrial cyber attack. In fact, only 30% have provided such an estimate. However, even though the sample data is not large, it does seem significant that nearly 50% of reported incidents, where a financial impact estimate was given, led to sizeable financial losses (<\$1M).

Forty-one percent reported loss of production while 29% reported a loss of ability to view or control the plant. Fortunately, human impacts have been small, with only one unconfirmed report of loss of life. Overall, the reported incidents clearly show that the most likely consequences of industrial cyber attacks to date are loss of the ability to view and-or control the process or system, causing an increased reliance on emergency and safety systems.

Traditional safety systems are independent of the main control system and generally considered highly reliable. However, the design trend is to base emergency systems on standard cyber technologies; thus, mirroring main control systems, even if not directly connected, this configuration increases the potential risk of common mode failure of both the main control system and its safety systems. Consequently, in the future, the systemic risks of cyber attack need to be considered in the design of not just the control systems, but also the safety systems.

The cyber incidents reviewed to date suggest that the threat to national infrastructure is real, and that our national ability to anticipate, predict, and prepare against cyber attack will benefit greatly from national efforts to produce a more methodical approach to incident reporting and analysis. In some regard, review of the available incidents suggests trends similar to what is being experienced in the information technology world.

The effort to evolve enhanced reporting and analysis methods needs to be a joint industry and government venture. Until such time as a formalized incident reporting structure and analysis paradigm can be finalized, a combination of the current U.S. Computer Emergency Response Team incident reporting requirements, in conjunction with other approaches such as those contained in the MIPT and BCIT, should be considered as an interim means of collecting and analyzing incident data.

ACKNOWLEDGMENTS

Much of the data in this report was provided by British Columbia Institute of Technology, Lawrence Livermore National Laboratory, and KEMA, Inc. under contract to the US-CERT Control Systems Security Center program.

CONTENTS

EXECUTIVE SUMMARY	iii
ACKNOWLEDGMENTS	vii
CONTENTS.....	ix
ACRONYMS.....	xi
INTRODUCTION	1
CYBER INCIDENT IDENTIFICATION	2
Database Searches	2
CERT Coordination Center.....	3
Memorial Institute for the Prevention of Terrorism Database	4
Energy Incident Database.....	5
SANS and CSI.....	6
Informal Process Control System Cyber Impact Database	6
Industrial Security Incident Database.....	7
Database Search Results.....	7
CYBER INCIDENT ANALYSIS RESULTS	8
Incident Type.....	8
Perpetrator Origins	8
Perpetrator Background.....	8
Motivational Intent of Attackers	9
Summary of Cyber Incidents.....	10
ADDITIONAL FINDINGS	11
Lack of Awareness	11
Shortage of Good Analyses.....	12
Fear of Financial Repercussions	13
RISKS AND RISK MITIGATION	14
Cyber Incident Risks	14
Mitigating Risks and Losses	14
Human Factors	15
Human Reliability and Human Factors as Crosscutting Issues.....	15
Human Reliability Analysis and Control Systems.....	16
DOCUMENT MAINTENANCE.....	19
SUMMARY	20

REFERENCES	22
Appendix A – Glossary.....	23
Appendix B – Selected Cyber Case Studies	29
1. Hackers Crash Controller via Web Service – ISID #38.....	31
2. Slammer Infected Laptop Shuts Down DCS – ISID #41	33
3. Two Viruses Cause Near Miss – ISID #66	33
4. Nachi Worm on Advanced Process Control Servers – ISID #51	33
5. Reverse Osmosis System PLC Attacked – ISID #29.....	31
6. Navy Radar Shuts Down SCADA Systems – ISID #37	32
7. Backdoor Trojan Attack on Manufacturing Lab – ISID #75	34
8. The Salt River Project Hack – ISID #1	31
9. European Distribution SCADA – KEMA #1	35
10. European Hydro – KEMA #2.....	35
11. Siberian Gas Pipeline Explosion.....	32
12. Educational Case Study – LLNL #1	36

FIGURES

1. Cyber incidents detected and reported to CERT®/CC by third parties within the U.S.....	4
2. Pie chart illustrating the percent of incident types.....	8
3. Pie chart illustrating the percentage of perpetrator origins.....	8
4. Bar chart illustrating the percentage of perpetrator backgrounds.....	9
5. Bar chart illustrating the motivational intent of attackers.....	9

TABLES

1. Control system-related terms in the MIPT database.....	5
2. Events in the Energy Incident Database by type.....	6

ACRONYMS

BCIT	British Columbia Institute of Technology
CERT®/CC	CERT Coordination Center
CSI/FBI	Crime Screen Investigation/Federal Bureau of Investigation
CSSC	US-CERT Control Systems Security Center
DHS	U.S. Department of Homeland Security
HRA	human reliability analysis
INL	Idaho National Laboratory
ISID	Industrial Security Incident Database
IT	information technology
LLNL	Lawrence Livermore National Laboratory
MIPT	National Memorial Institute for the Prevention of Terrorism
PCS	process control system
PLCs	programmable logic controllers
SANS	SysAdmin, Audit, Network (Institute)
SCADA	Supervisory Control and Data Acquisition
TCP/IP	Transmission Control Protocol/Internet Protocol
US-CERT	U.S. Computer Emergency Response Team

Cyber Incident Report for the US-CERT Control Systems Security Center

INTRODUCTION

This cyber incident report was prepared for the US-CERT Control Systems Security Center (CSSC) at the Idaho National Laboratory (INL). It will be used by CSSC as input to establishing a business case for increasing awareness and security within private and corporate entities and encourage their participation in developing a more methodical approach to cyber incident reporting and analysis. U.S. Computer Emergency Response Team (US-CERT) will use this document to evolve a standardized approach to incident reporting and analysis. Uniform reporting requirements will do much to make this information available to Department of Homeland Security (DHS) staff that can then use this data to support and update the US-CERT national control system security strategy. When combined with vulnerability analyses, the strategy can then be used by DHS staff and industry to support a proactive approach to preventing cyber attacks.

CYBER INCIDENT IDENTIFICATION

A substantial number of confirmed, unconfirmed, and potential cyber incidents that directly or potentially impact control systems have been documented worldwide. As confirmed in this section, case histories show that cyber attacks have increased significantly since 1988. The majority of attacks come from the Internet by way of opportunistic *viruses*, *Trojans*, and *worms*, but a surprisingly large number are directed acts of sabotage.

Database Searches

In theory, control system security can be quantified in part by analyzing the past history of malicious attacks directed toward control systems. To this end, the following sources were evaluated:

- US-CERT Coordination Center (CERT®/CC)^b
- Industrial Security Incident Database (ISID; British Columbia Institute of Technology [BCIT] proprietary)
- Energy Incident Database
- National Memorial Institute for the Prevention of Terrorism (MIPT) <http://www.mipt.org>
- Process Control Cyber Security Forum <http://www.pcscs.org/>
- National Counterintelligence Center <http://www.nacic.gov/>
- Embedded systems failures
<http://www.theinternetfoundation.org/Notes/Y2K/EmbeddedFailures.htm>
- Supervisory Control and Data Acquisition (SCADA) discussion list
<http://lists.iinet.net.au/cgi-bin/mailman/listinfo/scada>
- SysAdmin, Audit, Network (SANS) Institute <http://www.sans.org/>
- *2003 CSI/FBI Computer Crime and Security Survey*
- Kema, Inc.
- Lawrence Livermore National Laboratory (LLNL)
- Idaho National Laboratory (INL).

These historical repositories were searched for evidence of terrorist attacks on control systems, including process control systems (PCSSs), SCADA systems, and control systems. Approximately 450 physical attacks have been reported in the energy sector related to control systems, although few of these were consciously directed as attacks against a control system. Neither the MIPT nor CERT®/CC uses the labels “Process Control System,” “Control System,”

b. CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark office. Copyright 2005 Carnegie Mellon University.

“SCADA,” or variants thereof. One reason for this may be that, historically, so few incidents specifically involving a control system have occurred that the term was never used as a keyword in databases or reporting systems. Also, the existence of autonomous control systems in the past has prevented a convenient target for terrorist attack. Another reason could be that the required technical sophistication to carry out a cyber attack against a control system is much greater than other more accessible targets. However, considering the evolution of the Internet and pervasiveness of computers, history and voluntary reporting are not good indicators at this time. This study is also consistent with an observation made in the Process Control Systems Cyber Security Website, which quotes Pete Simpson from a March 12, 2003, article in Computer Weekly 360:

“The U.S. Department of Energy and several private security companies have demonstrated the ability to obtain unauthorized access to control systems. There have been many electronic impacts of control systems. Most have been unintentional, though there have been some intentional cases. None of these incidents have been identified by CERT, SANS, or CSI as they do not have the expertise or contacts to obtain this information.” (<http://www.pcscs.org/news.php>)

The result of this database repository evaluation, provided in the following subsections, indicates that historical evidence provides insight into control system related incidents or failures; however, that the information provides little support to future risk estimates.

CERT Coordination Center

Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our infrastructures have increased. From 1995 to 2003, the United States CERT®/CC, the first computer security incident emergency response team, reported that security vulnerabilities resulting from software flaws increased from hundreds per year to more than 4,000 per year. Along with these increasing vulnerabilities, the number of computer security incidents reported to the CERT®/CC has risen dramatically from 9,859 in 1999 to 82,409 in 2002 and 137,529 in 2003. Although cyber incidents now exceed 100,000 per year, only a few damaging attacks on control systems have been documented, and of the 320,000 records, CERT®/CC reports only 13,000 vulnerabilities through 2003. It is difficult to say how conservative these numbers are however, because some attacks are not detected and some users, to protect their reputation or to avoid encouraging hackers, do not report incidents.

The following tables provide a breakdown of incidents by year from 1988 to 2003.

1988–1989

Year	1988	1989
Incidents	6	132

1990–1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000–2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

Total incidents reported (1988–2003) = **319,992**

Figure 1 shows the cyber incidents detected and reported by third parties within the United States.

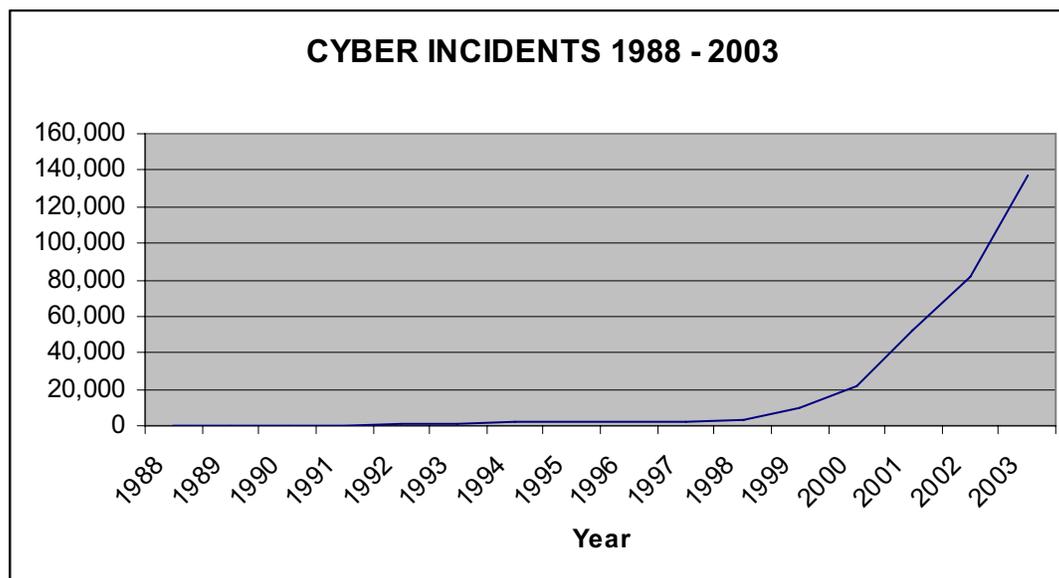


Figure 1. Cyber incidents detected and reported to CERT®/CC by third parties within the U.S.

Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, the number of incidents reported is no longer published.

The database used by CERT®/CC to track these incidents is operated out of the Carnegie-Mellon Institute. Although it contains a record of close to 320,000 cyber attacks (through 2003), essentially all apply to business information; no records of “process control systems” are mentioned.

Memorial Institute for the Prevention of Terrorism Database

The MIPT (www.mipt.org) carries a RAND-produced database on terrorism events. This database includes only those events that meet the definition of terrorism set forth by the United States Federal Government in 22 U.S.C. § 2656f(d) (U.S. Code 2003). A total of 16,224 incidents were recorded in the database between 1968 and May 2004.

The MIPT database was searched for a variety of key words that would likely identify PCS or control system attacks, as shown in Table 1. In the database, attacks are categorized by weapon, but the word cyber is never used to describe a weapon.

Table 1. Control system-related terms in the MIPT database.

Search Term	Number of Hits
Process	62
Control	248
Process control	3
Remote	129
Remote control	95
Computer	23
PCS	0
SCADA	0
Cyber	0

Although “control” and “remote” appeared frequently, in no case were there references to control systems as used in this document. Review of three events using the term “process control” showed that the term was not related to “process control” as used in this document. The word control is generally associated with control of an object or a controlled explosion, as in “remote controlled” explosion, or such as physically taking control of a plane. The word remote is associated with either carrying out an act remotely or using a remote-control device that is part of a weapon used in a terrorist act. The word computer is associated with physical destruction of computers, theft of computers, or computer companies. There was no incident in the database involving the use of a computer as a vector to damage a facility or infrastructure or an attack on a business, industrial, or infrastructure computer. There were no instances of the use of the word “cyber.”

Energy Incident Database

The Energy Incident Database is a proprietary database owned and maintained since 1974. Currently, the DOE Office of Intelligence must approve any release of information from this database for use by anyone other than themselves. The Energy Incident Database has records of approximately 200,000 incidents of all kinds, but is limited to incidents involving sub-national actors. A search of all incidents even remotely associated or potentially associated with control systems was conducted, including electrical control panels, switch gear, computers, control rooms, and so on. The search covered incidents associated with electrical power, oil and gas, coal, railroads, and seaports.

The search identified 409 worldwide incidents between 1967 and May 2004. Most (98%) of these incidences involved physical attacks on a building, fenced area, or other structure that may have had a control system associated with it, but the attack was not focused on the control system (explosives tossed into a substation, rifle shots into switch gear, electrical switches thrown, and so on). Table 2 indicates the distribution of the 409 events by type—less than half involve sabotage or terrorism. Many of the recorded events were in foreign countries. Only nine incidents were identified as specifically relating to control rooms or SCADA systems involving computers and/or cyber attack. These incidents are identified by type and number of events in Table 2.

Table 2. Events in the Energy Incident Database by type.

Category	No. of Events
Sabotage/terrorism	185
Disgruntled or striking employees	119
Vandalism/nuisance	57
Test and maintenance error	22
Fraud	12
Manager/operator decision	4
Equipment failure	3
Military take-over	6
Unknown	1
Total	409

SANS and CSI

The SANS Institute tracks computer-related incidents similar to the Crime Screen Investigation/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey. SANS is a leader in information technology (IT) security education and reports findings consistent with CSI/FBI surveys. The CSI/FBI 2003 Survey contains the same relevant information reported by SANS and, as such, was selected for review. No incidents related to PCS/SCADA were reported.

Informal Process Control System Cyber Impact Database

KEMA, Inc., has maintained an informal, but verified, database of cyber impacts on process control systems. They have recorded more than 60 real-world cases where control systems have been impacted by electronic means. These events have occurred in electric power control systems for transmission, distribution, generation (including fossil, gas turbine, and nuclear, where three plants experienced denial of service events), as well as control systems for water, oil and gas, chemicals, paper, and agribusinesses.

Some of these events have resulted in damage. Confirmed damage from cyber intrusions have included intentionally opening valves resulting in discharge of millions of liters of sewage, opening breaker switches, tampering with boiler control settings resulting in shutdown of utility boilers, shutdown of combustion turbine power plants, and shutdown of industrial facilities.

Industrial Security Incident Database

The ISID operated by the BCIT has been tracking cyber attacks on industrial control systems. The Industrial Security Incident Database contains 100 incidents over the past 20 years.

Information Sharing Websites

The following Web sites, documents, and discussion lists were searched by LLNL and INL for control-system-related cyber attacks, but none were identified.

- Process Control Cyber Security Forum <http://www.pcses.org/>
- National Counter Intelligence Center <http://www.nacic.gov/>
- Embedded Systems Failures
<http://www.theinternetfoundation.org/Notes/Y2K/EmbeddedFailures.htm>
- SCADA discussion list <http://lists.iinet.net.au/cgi-bin/mailman/listinfo/scada>.

Database Search Results

The database search activity identified 120 cyber incidents that the CSSC team could analyze. These incidents are located in the BCIT ISID, KEMA Inc. database, LLNL, Energy Incident Database, INL cyber incident database, and in other open-source data (e.g., general internet searches, emails, etc.). Identifying and analyzing these reported incidents was a key activity in preparing this analysis.

CYBER INCIDENT ANALYSIS RESULTS

This section summarizes the results of the analysis conducted on 120 cyber incidents located in the various databases described above. Analysis data is presented based on incident type, origin, perpetrator, and motivation of the attacker.

Incident Type

In an effort to obtain an accurate breakdown of the type of incident, the incidences were categorized as *audit or pen test*, *misconfiguration*, *hack*, or *mobile malware*. Figure 2 displays the analysis results for the incident types considered in this study. Analysis results show that 42% of incidences were due to mobile malware, 28% to hack, 26% to misconfiguration, and 3% to audit or pen test types. As depicted, mobile malware poses the largest activity risk.

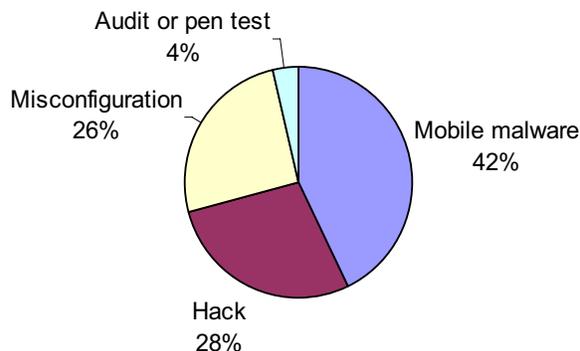


Figure 2. Pie chart illustrating the percent of incident types.

Perpetrator Origins

In an effort to obtain an accurate breakdown of the perpetrators origin, the incidents were identified as external, internal, and unknown. Figure 3 displays the analysis results for the origin of perpetrators considered in this study. Analysis results show that 61% of perpetrators originated outside or external to the organization, 38% were internal, and the other 1% was unknown. As depicted, external perpetrators pose the greatest risk.

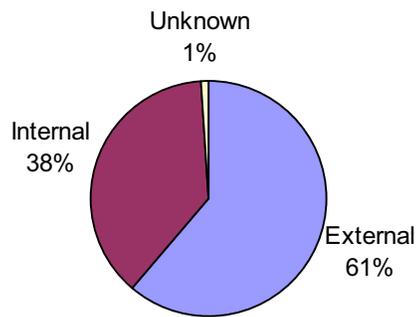


Figure 3. Pie chart illustrating the percentage of perpetrator origins.

Perpetrator Background

In an effort to obtain an accurate breakdown of the perpetrators background, the incidents were categorized as *malware authors*, current employees, hackers, software vendors, former employees, current contractors, agents of foreign nations, competitors, and unknowns.

Figure 4 displays the analysis results for perpetrator backgrounds considered in this study. Analysis results show that 43% of perpetrators were malware authors, 23% were current employees, 15% were hackers, 6% were software vendors, 5% were former employees, 5% were current contractors, and 4% were agents of a foreign nations, competitors, and unknowns, equally divided with 1%. As depicted, insiders such as contractors, former employees, and current employees pose less of a threat than malware authors who write *spyware*.

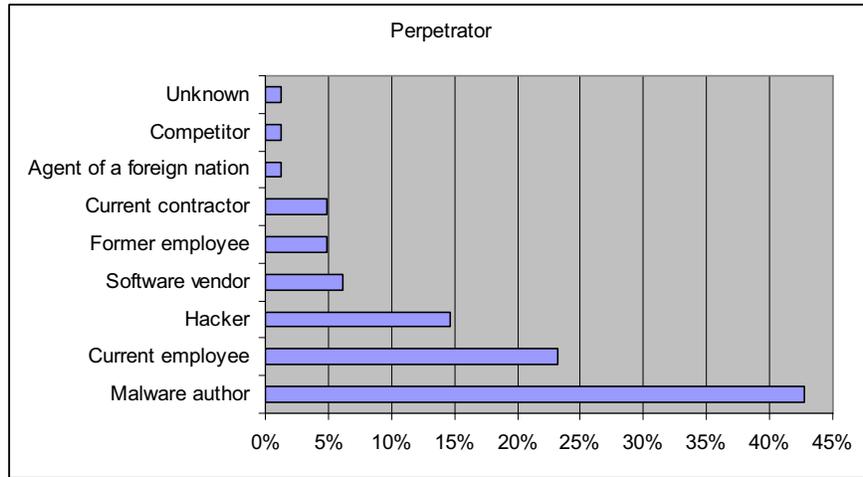


Figure 4. Bar chart illustrating the percentage of perpetrator backgrounds.

Motivational Intent of Attackers

In an effort to obtain an accurate breakdown of the perpetrators motivational intent, the incidents were categorized as infecting malware, a result of user or administrator error, curiosity, personal, software error, audit or pen test, financial gain, information or electronic warfare, unknown and hacktivism.

Figure 5 displays the analysis results based on the motivational intent of attackers considered in this study. Analysis results show that the motivational intent of 43% of attackers was to infect malware, 20% the result of user or administrator error, 12% curiosity (malicious or otherwise), 10% personal, 6% software error, 4% audit or pen-test, 2% financial gain, 1% information or electronic warfare, 1% unknown, and 1% hacktivism. As depicted, the most common intent of the attacker was to infect malware.

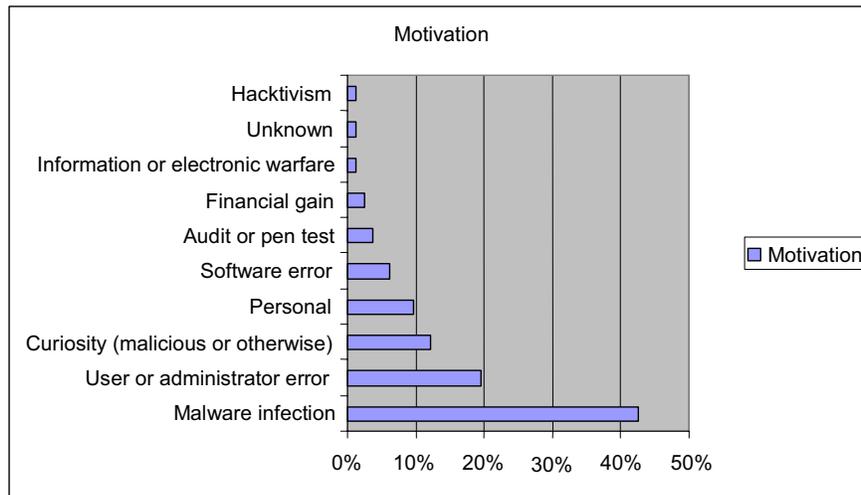


Figure 5. Bar chart illustrating the motivational intent of attackers.

Summary of Cyber Incidents

The following list summarizes the analysis results of all cyber incidents considered for this report based on type, origin, perpetrator, and motivation of the attacker; the list gives the highest percentage entry in each area:

- 42% of all incidences were conducted by means of mobile malware
- 61% of the perpetrators originated from external sources
- 43% of perpetrators backgrounds were malware authors
- 43% had a motivational intention of malware infection.

Further analysis suggests that a large percentage of incidents reported were due to a disgruntled employee who caused physical damage to the system.

ADDITIONAL FINDINGS

In the process of identifying and analyzing *cyber security incidents*—particularly as they relate to *attacks* on PCSs, SCADA systems, and control systems—the CSSC 2004 identified certain issues and concerns dealing with obstacles, risks and potential costs that felt needed to be addressed in order to increase industry awareness and security, and to reduce costs in private and corporate sectors of the nation. Our research confirms this notion. In their research they identified three main obstacles that are keeping private and corporate sectors from improving security measures:

- Lack of awareness
- Shortage of good analyses to draw from
- Fear of financial repercussions.

Lack of Awareness

Process control and SCADA systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wreaked so much havoc on corporate information systems. Recent research indicates this confidence is misplaced; the move to open standards such as Ethernet, Transmission Control Protocol/Internet Protocol (TCP/IP), and Web technologies is allowing *hackers* to take advantage of the control industry's unawareness. This can be seen in the following examples of cyber incidents that have occurred in the recent past:

- In August 2003, a *worm* infected the communication system of the U.S. railway company CSX Transportation. The dispatching and signaling systems were affected and all passenger and freight traffic, including morning commuter traffic in the Washington, D.C. area, had to be stopped for about 12 hours.¹
- In January 2003, the “Slammer” *worm* disabled the computerized safety monitoring system at the Davis-Besse nuclear power plant in Ohio, which was shut down for repair at that time. The responsible managers considered the plant “secure,” as its outside network connection was protected by a firewall. The worm entered the plant network via a contractor's infected computer that was connected via telephone dial-up directly to the plant network, thus bypassing the firewall.^{2,3}
- In March 2000, a former consultant to waste water plant in Maroochy Shire, Queensland, Australia, accessed the control system of the plant and released up to 1 million liters of sewage into the surrounding waterways.⁴
- The Internet Engineering Lab of the British Columbia Institute of Technology has set up an industrial control system security incident tracking database, which, in the spring of 2004, contained approximately 41 entries with a number of additional investigations pending.⁵

These examples show that security vulnerabilities in industrial automation and communication systems are open to attack and pose a risk of financial damage for plant owners, as well as harm to humans and the environment. Industrial communication systems share some security-relevant characteristics with information and communication systems in the office and Internet domain, but they also exhibit major differences, which create both obstacles and advantages. For example, they have different protocols on communication links, different layers of security password protection, and different means of isolation for safety systems.

In another example, from December 2002 to January 2003, a *hacker* or group of hackers gained *unauthorized access* to a modular hybrid controller resulting in a *denial of service* and loss of equipment control. There were two phases to the attack. First, hackers opened connections, sent unknown messages, and left without closing the connection. After repeated attacks, all connections were consumed resulting in a denial of service to legitimate users on the Ethernet port. Second, hackers sent a Web page to the controller containing Java script and the text: “Hello! Welcome to <http://worm.com> Hacked by Chinese.” This exposed a bug in the TCP/IP stack causing the controller to reset, forcing all outputs to their off state. Two controller vendor engineers worked full-time on the problem for three to four weeks each. Network activity was captured with a network analyzer. Once the causes were identified, the fixes were relatively easy. First, the controller’s software was modified to properly close all timeout connections. Second, the vendor of the TCP/IP stack software used in the controller was informed and provided a fix for the stack.

This incident clearly demonstrates Web services being deployed directly on industrial controllers. Common practice is to include access to Web based services on most remote terminal units, programmable logic controllers (PLCs), and distributed collector systems sold today. According to a major manufacturer of PLCs,^c the vast majority of their products are ordered with Web services enabled, particularly on their premium brands. However, a study by the same company’s marketing team indicated that only 13% of the users of this PLC actually configured and used the Web services. The remaining customers left the Web servers in the PLCs active with default passwords deployed.

Shortage of Good Analyses

Much of the available information about cyber incidents represents a characterization as opposed to an analysis of events. This shortage of good analyses particularly in the area of human-systems interaction reflects an overall weakness in the availability of detailed data. Available data, in turn, reflect current reporting requirements. This obstacle has made it difficult for CSSC to obtain meaningful historical data related to *cyber security incidents* that can be used to support trending, quantification, and development of means to reduce the relative risk associated with cyber attacks.

c. The name of this vendor is withheld by request.

Fear of Financial Repercussions

Often, companies are not forthcoming about cyber attacks because of potential financial repercussions. This keeps them from reporting incidents that occur because they believe consumer confidence will decrease with each cyber-incident occurrence. Consequently, the confidential nature of cyber incidents makes it difficult to collect data and project future losses.

Our study showed that cyber incidents within the business community are extensive and costly, with U.S. companies currently reporting unauthorized system access. Financial losses from these cyber incidents appear to be shared equally among denial of service, theft of private information, virus distribution, and other attacks. Some measures of the annual global financial impact of *virus attacks* alone, when taken over the period from 1995 to 2003, indicate a twenty to forty-fold increase.⁶

The annual cost in losses from major attacks has increased sharply since the mid-1990s. The estimates from sources are varied but in all cases report attacks in the billions of dollars. The worldwide financial impact of viruses in 2003 was estimated to be almost \$18 billion.⁶ Based on global losses of this magnitude, the Institute for Catastrophic Loss Reduction estimates that computer viruses cost between \$1 and \$2 billion in 2003. Ernst & Young's 2003 *Global Information Security Survey*⁷ reports that hackers, worms, and other high-tech interference caused \$11.1 billion in damages in 2002, more than a twenty-fold increase since 1995.

RISKS AND RISK MITIGATION

Cyber Incident Risks

As confirmed in a recent survey, there are currently three main categories of significant cyber incident risks that affect companies: viruses, denial of services, and theft of proprietary information. These kind of cyber incidents accounted for 81% of losses experienced by industry within the United States in 2002.

A cyber incident that occurred in February 2000 demonstrates the extreme risks that cyber crimes pose to companies worldwide. This incident was caused by a 15-year old Montreal computer hacker who was responsible for 58 attacks and security breaches of Internet sites in Canada, the United States, Denmark, and Korea. Known as “Mafiaboy,” he launched a denial-of-service attack that overloaded targeted Web sites with so much data that it completely shut each one down. Users were unable to gain access to these Web addresses for several hours.

Companies affected by Mafiaboy included Yahoo!, eBay, Amazon, CNN, and the Microsoft network. By the nature of their business of Internet-related customers these companies serve requires them to be Internet-accessible at all times to conduct their business. His denial-of-service attack disrupted Internet service periods ranging from 1 hour to more than 3 hours.

Many companies accept a certain level of risk by relying primarily on the Internet for revenue. While many of these companies experience denial-of-service attacks, such strikes are often not reported to the police; instead, they are referred to as “glitches” so as not to deter customers from using their services in the future because of concern over security issues.

Mafiaboy’s attacks on the Internet sites of Yahoo! and eBay resulted in a decrease in their stock values of between 17 and 23% in the weeks following the attack. Market reactions such as this demonstrate why companies are reluctant to disclose cyber attacks.

Mitigating Risks and Losses

As stated above, the objective of this report is to support DHS staff and industry in developing a proactive approach to preventing cyber attacks. Part of such an approach logically includes preventing or mitigating risks by exposing the needs and presenting solutions that can be used in developing a more methodical approach to incident reporting and analysis. These efforts will strengthen long-term abilities to anticipate, predict, and prepare against cyber attacks, not only in the United States, but also throughout the world. This report will increase awareness among industry leaders, recognizing that the full participation of such leaders will be critical in mitigating risks and minimizing losses.

Many industry leaders are aware of these risks and have taken important initial steps to safeguard their assets, including prescriptive security rules and training of personnel to instill new practices and modify hardware and software used in business systems and plant floor controls. Some sector leaders are very active in securing their control systems, many others do

not see a compelling business case for investing in upgrades prior to normal changes driven by obsolete systems; thus, control system security is far from universal. Based on diminishing awareness, industry can therefore be categorized as follows:

1. Those who are aware and actively protecting their own systems, but know that the supply and distribution networks or infrastructure they rely on are susceptible to malicious attack.
2. Those who have current management support, but are doubtful of the needed long-term commitment for complete establishment and maintenance of their security needs.
3. Those aware of problems or potential problems, but cannot convince management that the risk warrants investment in upgrades.
4. Those who believe they are adequately aware, but think the risks to their systems are insignificant or that their relative obscurity produces security.
5. Those who are unaware to the risks associated with being connected to the Internet and using telecommunications and wireless communications.

Human Factors

The discipline of human factors generally refers to designing for human use.⁸ It has also come to mean the study of human capabilities and limitations, including human system interaction and design for reliable performance. Within the context of incident analysis, it represents the human aspect of the common vulnerabilities in control systems and the ability of the human to assist in mitigating damaging consequences. Although many incidents are the result of malware and malware attack several incidents are a direct result of human error, user or administrator error or curiosity. These incidents are identified in Database Search Results section of this document.

Human Reliability and Human Factors as Crosscutting Issues

The purpose of *human reliability analysis* (HRA) is to account for the human contribution to system risk. Within the context of control systems, human-influence extends to systems including administrative and financial systems as well as to the design, selection, and testing of physical systems. It also encompasses human response to and mitigation of cyber attack.

There are typically three aspects to HRA: error identification, modeling, and quantification. Formal methods of HRA categorize errors according to a general human performance model.⁹ Human behavior has nominal error rates for routine actions and cognitively engaging tasks. These error rates apply to the failure of achieving desirable actions. HRA also helps to identify and quantify the risk contribution of undesirable actions. Thus, error rates are associated with both protecting and defending through the process of detection, diagnosis, and taking corrective actions, as well as activities maliciously undertaken to undermine a control system. The error rate is increased by clearly understood factors such as training, experience, workload, and stress. For example, a lack of training and experience coupled with high workload due to either the fast pace of events or the sheer number of things to be considered in conjunction with mental stress can greatly increase the human error probability. These same factors may also

contribute positively by decreasing the nominal error rate. Extensive training and experience coupled with good ergonomics, adequate systems feedback, good procedures, low workload, and a low level of stress will generally result in a decrease in the human error probability.

As part of an overall control system risk model, calculating the human error probability makes it possible to model the overlap of the failure of human protective measures and the successful disruption of a control system by adversaries. Understanding this vulnerability space allows owners and operators to focus efforts in the design of secure systems, which can be made more secure by putting in place mechanisms to maximize human performance on the protective side, while simultaneously putting in place barriers to minimize offensive human actions. For example, forcing password changes on a regular basis acts as a way to increase system operator awareness of security, while effectively putting a roadblock in place to intrusion by unauthorized personnel.

Culture, including organizational culture, shapes human performance and human error. This is true for cyber attackers and system defenders. Culture is comprised of values, attitudes, and beliefs that have been shaped by a group of individuals over a period of time. Culture acts as a filter that influences perception, cognition, and action. Within control systems, there are attitudes and beliefs held by personnel that are unique to individual infrastructures and organizations that, in turn, can help to condition human-system response, even to the extent of doing things contrary to our intentions. For example, the culture of the professional hacker working for a nation state, versus a malware author frequenting a zero day room for inspiration may be quite different. The former may wish to extract information from the systems without attribution, the latter may wish to disable a system and do so as publicly as possible.

Predicting human performance and human reliability in response to a control system attack includes understanding important aspects of human-machine interaction. Influencing factors include the quality, clarity, and timeliness of the information that is present; staffing levels and staff skill levels; reporting requirements; an organizational culture that reinforces questioning attitudes; and the additional influences that can affect human response such as training, experience, workload, stress, complexity, and the quality of procedures. Pre-event, human errors in system-design, maintenance, and operation can also serve to make errors in response to the control system attack more likely.

Human Reliability Analysis and Control Systems

Human reliability and human factors in control systems are important parameters in determining the probability of success or failure for those actions and decisions assumed by designers and facility operators. Human factors insights can be used to assist in building physical and cyber defenses, and in detecting and diagnosing attacks. Proper attention to human factors can help to ensure that personnel follow appropriate procedures to restore systems and functionality, and alert the appropriate authorities. Knowledge of human factors and human reliability concepts can be used to strengthen the design of cyber security training and awareness, and ensure getting systems back online with the least amount of damage to property and human life. Currently, reporting requirements associated with events do not provide all the information

necessary to develop the proper sensitivity to human factor issues. Further, to get truly meaningful information people will have to feel free from retribution when reporting what has occurred during events.

Some proactive actions can be taken immediately to enhance the current state of human performance in response to events. This could entail organizations recognizing that their unencrypted financial transactions are at risk to rogue monitoring and taking appropriate defensive actions, such as using encryption, implementing intrusion detection systems, and instituting an effective encryption and password policy. In food processing, it could mean that people have sufficient awareness of a terrorist threat to control systems and accordingly decide to isolate the control system from the Internet and set up additional means of preventing attack, such as two-person rules (shown as Separation of Duties) for changing temperature set points. Management and industry bear the responsibility to set up the appropriate infrastructure requirements.

A review of Sandia findings in May 2003¹⁰ provides ample evidence of the role of human factors across four out of the following five major control system vulnerability groupings: control system data, security administration, architecture, networks, and platforms.

The first notable failure is in control system data. They indicate that failure to assign sensitivity levels for control system data is an overarching challenge that has led to fundamental problems in assessing whether the security of associated databases is appropriate. The other categories demonstrate additional problems. For example, 100% of the vulnerabilities in control system administration involve human factors or human error as is manifest in policy decisions regarding control systems, problems in procedure design or implementation, lack of formal security training, and lack of formal configuration management. Only control system architecture vulnerability is not ordinarily associated with human factors. Fifty percent of the common vulnerabilities in control system networks and 44% of the vulnerabilities in control system platforms involve human factors. Finally, the findings list miscellaneous cultural factors such as having blind faith in the ability of control system links to faithfully transmit data. These cultural human factors represent shortcomings in training and sensitivity related to control system security.

The current generation of reporting systems is weak in terms of reporting the human aspect of preparation and response to cyber attack. This is true do to aspects of trust as well as financial considerations and public perception. Once these are dealt with more successfully than presently is the case specific human factors information in a number of areas needs to be developed. Some of the more important for reporting include the following: number, level and skill of personnel responding to the attack; better characterization of perpetrator parameters, whether or not security procedures are implemented and enforced, identification of successful and unsuccessful actions, whether security checks proved effective, etc. Research can be focused on the design of these reporting requirements from a human factors perspective.

The decisions and actions that people take determine much of control system response to cyber attack. Although generic awareness is useful, potential success of these actions are context specific to infrastructure and to application. The only way to increase our knowledge of what

works and doesn't work is through the collection and analysis of event-based data. Industry groups are developing standards for the protection of control systems across infrastructures. This needs to be informed by the analysis of cyber events that can form a basis for next generation reporting requirements. This information has to be made available in such a way that sectors can properly employ control system standards and share their success without placing proprietary and trade information at risk or creating additional vulnerabilities.

DOCUMENT MAINTENANCE

This document will be updated as requested and as pertinent information becomes available. Cyber incidences that occur during the year will be identified, compiled, and documented in future revisions via a process similar to that followed in this analysis. Comments received on this report, independent of origin but including members of the control system community, the public, the General Accounting Office, and DHS, will also be incorporated. These comments will be analyzed and evaluated with a recommendation for incorporation into future risk analysis and modeling efforts, where appropriate.

SUMMARY

The incidents reviewed to date suggest that the risk to national infrastructure is real but very low at present. Even so, the number per year is increasing, and the trends appear similar to what is being experienced in the IT world. Although the reported number of incidences is low, discussions with industry experts suggest that the actual number of incidents is at least a factor of 10 higher, but these incidents are not reported beyond the companies which have experienced them. Furthermore, the economic losses from cyber attack on control systems remains low, rarely exceeding \$1 million.

The significant discrepancy between the control system experience and the IT experience (tens versus hundreds of thousands of incidents per year) is because terrorists have not yet found control system attacks a useful tool. In fact, the MIPT database of international terrorism has yet to record a single incident of cyber attack on a critical infrastructure control system that results in significant damage. There are a number of factors believed to cause this, including:

- The still prevalent use of “legacy” control systems with their own proprietary software and information exchange protocols;
- In the IT world the data being sought, such as personal identification numbers, has immediate value in financial theft or scams whereas in control systems the data is of no real value without understanding the process;
- High hazard processes being controlled by electronic control systems typically have redundant, non-cyber safety systems;
- Taking advantage of hacking into a control system requires detailed technical knowledge of the process to cause significant damage; and
- Terrorists, domestic or foreign can achieve greater immediate bang for the buck with fire, crashes, or explosives.

The above observation is similar to that by Gabriel Weimann.¹¹ These observations are also consistent with the fact that the most prevalent incident is related to a current or former employee.

Even though the incident rate is too low to allow statistically valid trend analysis, it does appear that the incident rate is rising exponentially. As the hacker and terrorist community increases in size and becomes more skilled, and as other avenues of terrorist attack are increasingly closed, it is reasonable to expect that significant cyber attacks will become more a inviting attack opportunity. Other appealing features of cyber attacks are the low investment cost, the potential for greater attack frequencies, and the ability to remotely conduct attacks and the lack of attribution (almost automatic anonymity). Though it may take terrorists a year to plan and execute a plane crash or a 40-ton explosive attack, the ease of conducting cyber attacks can increase the attack rate from a few per year across the nation to greater than 1×10^{10} per year, depending on the expertise, resources, and motivation of potential attack agents.

The higher the degree of interconnectivity and communication among cyber systems, the greater is the opportunity for talented people to breach the security systems and maliciously manipulate information or control system functions. We also anticipate this interconnectivity and communication capability to increase in control systems, at least for the foreseeable future. While access to information available to operators and executives (or denial of access to this information to those who legitimately need it (a denial-of-service attack) may cost industry money or result in embarrassment, the manipulation of system functions using this information can have more far-reaching consequences. An individual gaining unauthorized access to systems could potentially act as an operator and affect systems in ways that injure people, damage facilities, and shut down segments of the infrastructure, with the potential of cascading into regional and even national disasters. Currently, we are not collecting data in such a way that it would provide DHS and industry the technical basis for characterizing and quantifying the human-system response to attack. To do so would allow us to identify and correct vulnerabilities thus making the perpetrator's job more difficult.

Finally, the most immediate need in the arena of incident tracking is a more effective way of reporting all, or all significant and most other cyber attacks on control systems. This enhanced reporting system needs to be a joint venture between industry and government. The CSSC has tasks planned for FY 2006 that will go a long way towards achieving that goal.

REFERENCES

1. CSX Transportation, “Computer virus strikes CSX transportation computers—Freight and commuter service affected (press release),” Aug 2003.
2. K. Poulsen. (2003, Aug.) Slammer worm crashed Ohio nuke plant net. [Online]. Available: <http://www.securityfocus.com/news/6767>.
3. U.S. Nuclear Regulatory Commission. (2003) NRC Information Notice 2003-14. [Online]. Available: <http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf>
4. T. Smith. (2001, Oct.) Hacker jailed for revenge sewage attacks. The Register [Online]. Available: <http://www.theregister.co.uk/content/4/22579.html>.
5. E. Byres and J. Lowe, “The myths and facts behind cyber security risks for industrial control systems,” presented at the VDE Kongress, Berlin, Germany, 2004.
6. Computer Economics. (2004). *Virus Attack Costs on the Rise – 2004 Update*. California: Computer Economics, March 2004.
7. Ernst & Young’s 2003 *Global Information Security Survey*
8. U.S. Department of Homeland Security, Presidential Decision Directive 63, PDD-63, May 1998, <http://www.fedcirc.gov/library/legislation/presDecDirective63.html>.
9. Information Sharing and Analysis Centers (ISACs), <http://www.dhs.gov/dhspublic/display?theme=73&content=1375&print=true>.
10. J. Stamp, J. Dillinger, and W. Young, *Common Vulnerabilities in Critical Infrastructure Control Systems*, SAND2003-1772C, Sandia National Laboratory, May 2003.
11. Gabriel Weimann, “Cyberterrorism How Real Is the Threat?” <http://www.usip.org/pubs/specialreports/sr119.pdf>.

Appendix A
Glossary

Appendix A

Glossary

- audit or pen test.* A intentional intrusion into a computer system to assess security vulnerabilities and identify potential opportunities to penetrate the system (e.g., security codes, firewalls, passwords, etc.)
- attack.* An intentional violation of a security objective. Attacks may either be initiated by persons outside the plant or by insiders. We distinguish between *targeted* and *untargeted attacks*.
- cyber security incident.* Any adverse event that threatens the confidentiality, integrity or accessibility of an agency's information resources. Includes but are not limited to: attempts (either failed or successful) to gain *unauthorized access* to a system or its data; disruption or *denial of service*; unauthorized use of a system for the transmission, processing or storage of data; changes to system hardware, firmware or software without the agency's knowledge, instruction or consent; attempts to cause failures in critical infrastructure services or loss of critical supervisory control and data acquisition (SCADA) systems; attempts to cause failures that may cause loss of life or significant impact on the health or economic security of the agency and/or State; probing of any nature that an agency or other authorized entity has not approved in advance for system security testing purposes.¹
- denial of service (DoS).* Attacks that adversely affect or degrade access to critical servers or attempted attacks, particularly if they are persistent or significant such as those aimed specifically at an agency's routers or critical servers. DOS is an attack where the goal of the attacker is to decrease the availability of the system.
- hack.* A *targeted attack* against a specific system; because the attacker is going after a specific system, a great deal more technical expertise is required because multiple exploits are typically used and continued control of the host is desired, which means covert communication channels have to be established (typically how hacked systems are identified) and must be good enough to bypass multiple detection mechanisms.
- hacker.* A person who deliberately targets a system, with a specific network or group of networks for a particular reason; a good hacker is much better technically than a virus/worm writer (mobile *malware*); hackers require enough technical expertise to be able to modify existing exploits, develop custom code specific to the target environment, etc. during an attack.
- human reliability analysis (HRA).* HRA is the probabilistic calculation of "...unwanted actions or inactions that arise from problems in sequencing, timing, knowledge, human-system interface, procedures, or work processes that result in deviations from standards or norms that place people, equipment, or systems at risk."²
- malware authors.* A person whom writes programs to obtain information from identified sources. Good malware writers can get paid extremely well, better even than white hat security experts for writing good code; professionals who depend on their reputation for high-quality, technically innovative code.

malware or spyware. Malware are programs, certain types of which are illegal, that gather information for a variety of purposes but are not considered ethical by most people. This includes information gathering for marketing, spam mailing, harvesting information for identity theft or other financial crimes, and turning vulnerable personal computers into drones in botnets that are rented out to people who need lots of bandwidth. Spyware is non-mobile malware and is some of the best-written code in industry; untargeted attacks.

misconfiguration. Incident wherein a user has misconfigured a computer system by omitting required passwords, network firewalls, etc. to inadvertently create a vulnerability.

mobile malware. Worms and viruses—the form of attack most people are familiar with; generally untargeted; their purpose is to spread as rapidly as possible; may include a backdoor for use as in a botnet later, but generally the backdoors are detected by anti-virus software and removed. Generally takes advantage of one known exploit to infect a host; one or two means of propagating and one or two backdoors for later use by the writer.

Spyware. See *malware*, above.

targeted attack. An attack intended to harm a specific communication system or type of system, such as for purposes of industrial espionage, warfare, or terrorism. Targeted attacks are typically preceded by a phase of gathering information about the target, such as using online and offline available references, as well as dedicated tools for discovering vulnerable systems on a network.³

Trojan. A virus where the malicious functionality is hidden behind functionality that is desired and used by the user. Trojans are typically employed to circumvent confidentiality or access control objectives.

unauthorized access. An attempt to gain access to someone else electronic domain, control system, computer, etc. Successful unauthorized access to agency systems can result in Website defacements, unauthorized root/administrator access, etc. Persistent unsuccessful attempts can cause a system to lock out accounts due to brute force password attacks, response problems because an automated script keeps probing a Web server, etc.

Untargeted attack. An attack that victimizes any vulnerable system discovered.

virus attack. An attack with a virus that manipulates a legitimate user to bypass authentication and access control mechanisms in order to execute the *malicious code* injected by the attacker. In practice, virus attacks are often untargeted and spread among vulnerable systems and users. Virus attacks often directly or indirectly decrease the availability of infected systems by consuming excessive amounts of processing power or network bandwidth.

worm. A malicious code whose propagation mechanisms rely on automatic exploration and exploitation of vulnerabilities in the targeted system, without involvement of any user. Worm infections are untargeted and usually create availability problems for the affected systems or even the Internet as a whole.⁴ In addition, the worm may carry malicious code to launch a distributed, targeted attack from all the infected hosts.

References

1. ITRMC Guideline 510 – Cyber Security Incident Reporting Template can be found at <http://www2.state.id.us/itrmc/plan&policies/guidelines.htm#510>
2. Gertman, D. I., and H. S. Blackman, Human Reliability and Safety Analysis Data Handbook, John Wiley, New York, 1994.
3. “The Electronic Attack Threat to Supervisory Control and Data Acquisition (SCADA) Control & Automation Systems,” National Infrastructure Security Coordination Centre (NISCC), UK, July 12, 2003.
4. FX and Kimo “Attacking Networked Embedded Systems” CanSecWest Conference, Vancouver, May 2003 VDE Congress, Berlin, October 2004, Page 5 of 5.

Appendix B
Selected Cyber Case Studies

Appendix B

Selected Cyber Case Studies

Twelve of the 120 incidents reviewed under this task are presented here as case studies.

1. The Salt River Project Hack – ISID No. 1

Between July 8th and August 31st, 1994, Lane Jarrett Davis gained unauthorized access to the Salt River Project (SRP) computer network via a dialup modem so he could have access to billing information. He installed a back door into the system giving him access at a later time. At the time, SRP's water SCADA system operated a 131-mile canal system, which was used to deliver water to customers in the Phoenix metropolitan area. Mr. Davis had at least one 5-hour session on mission critical systems which controlled the canals. Data vulnerable during the intrusions included water and power monitoring and delivery, financial, and customer and personal information. Data taken and/or altered included login and password files, computer system log files, and "root" privileges. Furthermore, a Doppler-radar research project between the SRP and National Weather Service's National Severe Storms Lab was also accessed. SRP estimated losses at \$40,000, not including lost productivity due to the compromise.

Mr. Davis was a member of a group that met regularly to share information on computer hacking and telephone fraud. In one instance he reprogrammed a PBX (telephone switch) to allow a previously inactive extension to receive incoming calls, obtain a dial tone, and make outgoing calls at the expense of the victim. A search to arrest produced numerous items including burglary tools, and a "Red Box" (a device that emulates the tones produced by coins inserted into a pay phone). He was actively involved in hacking into many other business and government systems including: U.S. West, Motorola, Arizona State University, AT&T, Glendale Community College, Evergreen Communications, U.S. Geographical Survey at Northern Arizona University, and the Internal Revenue Service Bulletin Board System.

This hack is often linked to an attack on the Roosevelt Dam and has become technological myth which regularly resurfaces. Quoting a statement made before the U.S. House of Representatives, "a juvenile hacker gained unauthorized access to the companies controlling the operations of the Roosevelt Dam in Arizona." At the time of this incident, Mr. Davis was 27 years old and there was no connection between the SRP and Roosevelt Dam.

One final note, the reward for his activities were bragging rights and the intellectual challenge. At the time of the incident, Mr. Davis was a programmer and software developer for Unique Software. He left in February 1996 for a better job prospect at Quest USA where he worked as a network and software developer until their going out of business. He was employed with Genuity, a large Internet Service Provider, at the time of his sentencing in 1997 and reported that he comes and goes as he pleases and makes his own schedules. Mr. Davis has an associate's degree in computer science and believed that he had the right to pursue his intellectual freedom through his hacking activities.

2. Reverse Osmosis System PLC Attacked – ISID No. 29

A programmable logic controller (PLC) used to control a reverse-osmosis water purification system at a semiconductor manufacturer was shutdown when an individual or group gained unauthorized access through the Internet. Due to its location in the plant, the PLC had been connected to a non-process control network that allowed Internet traffic. There was no impact on production as there were sufficient backup water supplies.

3. Siberian Gas Pipeline Explosion – ISID No. 32

A Russian Gas Pipeline was disrupted causing an undisclosed dollar amount of damage created by an explosion with the power of a three kiloton nuclear weapon. Gas supplies were disrupted and consequential foreign currency earnings. An external-Agency of Foreign States, hired engineering firms to design defects into the technologies and products perpetrating the controls utilizing software that included a Trojan Horse that caused a major explosion of the Trans-Siberian pipeline in June of 1982. The Trojan ran during a pressure test on the pipeline but doubled the usual causing the explosion.

4. Navy Radar Shuts Down SCADA Systems – ISID No. 37

During a military exercise a naval radar system caused severe electromagnetic interference with the SCADA system of a nearby water authority and gas and electric company. Both the water authority and gas and electric company were unable to remotely actuate critical valve openings and closings, and technicians had to be dispatched to effected remote locations to manually open and close water and gas valves as a result. In both cases, the points of intrusion were wireless networks. Although this incident was accidental, it effectively resulted in a denial-of-service.

This incident illustrates the susceptibility of wireless networks to an external attack and the paramount importance that data integrity represents to operational SCADA systems. The financial impact of this incident is unknown; however, it is clear that there was loss of staff time and equipment control.

5. Hackers Crash Controller via Web Service – ISID No. 38

From December 2002 to January 2003, a hacker or group of hackers gained unauthorized access to a modular hybrid controller resulting in a denial of service and loss of equipment control.

There were two things happening at the same time. First, hackers were opening connections, sending unknown messages and then leaving without closing the connection. After repeated attacks, all connections were consumed resulting in a denial of service to legitimate users on the Ethernet port. Second, hackers sent a Web page to the controller containing Java script and the text: “Hello! Welcome to <http://worm.com> Hacked by Chinese.” This exposed a bug in the TCP/IP stack causing the controller to reset forcing all outputs to their off state.

Two controller vendor engineers worked full-time on the problem for three to four weeks each. Network activity was captured with a network analyzer and once the causes were identified, the fixes were relatively easy. First, the controller's software was modified to properly close all timeout connections. Second, the vendor of the TCP/IP stack software used in the controller was informed and provided a fix for the stack.

This incident clearly shows the risk of Web services being deployed directly on industrial controllers, a common practice on most remote terminal units (RTUs), programmable logic controllers (PLCs), and distributed collector systems (DCSs) sold today. According to a major manufacture of PLCs,^d the vast majority of their products are ordered with Web services enabled, particularly on their premium brands. However, a study by the same companies marketing team indicated that only 13% of the users of these PLCs actually configured and used the Web services. The remaining customers left the Web servers in the PLCs active with default passwords deployed.

6. Slammer Infected Laptop Shuts Down DCS – ISID No. 41

In May 2003, a corporate employee installed software on a laptop, unaware that it included an unpatched version of Microsoft SQL. Sometime later, the user connected the laptop to the Internet (in violation of company policy) to access email via an Internet service provider. The SQL-slammer worm infected the Internet connected machine. The user then brought the infected machine into the office and connected to the network, causing a small outbreak of the SQL-slammer worm within the corporate network and process network.

A data acquisition server without a firewall, a control system, and a development control system became infected with the worm and had to be removed from the control network to prevent further infection. There was no significant impact to production, but some history data was lost during server down-time and had to be manually created.

7. Nachi Worm on Advanced Process Control Servers – ISID No. 51

In December 2003, eight advanced process control servers in a petrochemical company were affected by the Nachi virus, resulting in a loss of production for about 5 hours. The advanced process control servers running Windows 2000 had to be disconnected from the network until the virus could be removed from the machines.

8. Two Viruses Cause Near Miss – ISID No. 66

A major petroleum company experienced a serious near miss when two worms—the nb_worm and SQL-slammer—affected many of the servers on their process control network. The impact of this incident included server and communications failures throughout the system from the wells and manifolds to the floating production offshore platform. The process control system was kept functional during the entire process of identifying and resolving the problem.

d. The name of this vendor is withheld by request.

The perpetrator and point-of-entry are unknown. The financial impact was estimated to be between \$10,000 and \$100,000, and there was a significant loss of staff time

9. Backdoor Trojan Attack on Manufacturing Lab – ISID No. 75

This incident describes a complex and wide-reaching malware-based attack against the manufacturing lab systems of a major electronics manufacturer. The lab was a large integrated test and development facility with a significant number of Windows servers and development machines spread over several building sites. The attack was a back-door Trojan, which was at that time, a new and unknown variant. It is unknown whether this was a directed attack or not, and the intent of the attack is unknown.

Initially, it appeared that only one server had been infected and then cleaned automatically by its antivirus software. Inspection of the antivirus logs on this server indicated that the virus had been deleted. Unfortunately, later investigation proved that the virus had created a file named administrator.txt which contained a list of IP addresses for all the lab machines, along with all of the account names for each machine recorded, and the password for that account. Many of the accounts that were recorded were local administrator accounts with blank passwords or passwords consisting of the phrase “password.” The virus had configured an ftp server and was sending this information to an unknown location. The server was disconnected and the administrator.txt file was printed.

Another server was experiencing similar problems and a decision was made to disconnect this server from the network as it most likely had a virus, but the users refused, as they couldn't spare the down time. Consequently management was asked to disconnect the infected lab machines which would result in decreased production and therefore cost money. In a few short hours, at least half of the lab machines were discovered to be infected and were disconnected from the network, resulting in production stoppages.

From here, the issue was escalated and corporate entities were contacted to share information. The corporate network and desktop support vendors were informed of the situation and a call was made to the organization's network security. A representative at the anti-virus software vendor was also contacted. The problem was considered contained by the end of the day but not solved. Almost a week went by and there was a desperate need for an immediate solution. The engineers decided to invoke the equivalent of a mutiny by reconfiguring the test beds with the machines hooked to hubs and switches for connectivity. There was no access to DNS servers, no communication process and no documentation for changing the many embedded passwords. There was no official fix yet available and some valuable resources were not properly backed up. Ultimately, users were helped with work-arounds until the network and all related resources were up and running. All-in-all, about 3 weeks of development time and countless other related hours were lost, although the actual number is unknown.

10. European Distribution SCADA – KEMA No. 1

A European utility connected their distribution SCADA system to the corporate network. They did not deploy the Microsoft security patch for Welchia nor upgrade their anti-virus software before the virus hit. In addition, the CISCO router had older software that did not include Quality-of-Service nor rate limiting applications. The distribution SCADA utilized shared corporate routers for communications. The virus entered through the corporate network and created a synflood attack on the router. This created a shutdown of 30–40% of all communication traffic from the distribution SCADA to the Control Center. Because there was no loss of power, the event was not noticeable to the outside world. If there was a loss of power while the SCADA communications were impacted, it could have had serious impacts on utility operations and customer response. The attack was initially construed as a hardware problem for the first 24 hours until a senior IT security officer identified the problem as a virus.

Even though there was no loss of power, the utility expended approximately 40 man-weeks (4 calendar weeks) cleaning-up the event. The utility lost significant distribution SCADA capability for three days (many distribution substations were not visible to the control center). Since there was no loss of power, there was no requirement for disclosure and the utility did not disclose this event.

11. European Hydro – KEMA No. 2

A European utility with significant hydro resources encountered an event while attempting to reduce power from high power (approximately 70%) to zero in rapid manner during a safety analysis test. The hydro control system motor control utilized a Profibus network. When the request for load reduction was received at the motor, the set point appeared to be outside the accepted range. Consequently, the motor controller substituted the set point with a value from a local register within the motor.

This misconfiguration created a conflict in valve operation where some valves were maintaining a high power operation and high water flow while others were attempting to reduce water flow.

The result of the set point mismatch was that valves were slammed shut as a result of the force of the water flowing into the turbine. Instead of a slow and controlled shutdown of the water flow the flow was reduced over 70% within a second creating a vacuum bubble within the turbine.

There was no physical damage to the power plant. But as a result of the problems 4 other plants using the same Profibus-motor control network were shutdown for about two weeks.

It took almost a week before the software was released but only a couple of minutes to find what were wrong with it. Installation of the new software took about a week.

12. Educational Case Study – LLNL No. 1

The attached case study, *Backdoors and Holes in Network Perimeters*, was prepared by Lawrence Livermore National Laboratory (LLNL) for CSSC. This is a fictionalized case based on several actual cyber attack incidents, recreated specifically to educate owners of similar systems on potential cyber attacks and means of enhancing cyber security to minimize the probability of attack in the future. The incidents were fictionalized to provide anonymity to those critical infrastructure facilities, which were impacted by cyber attack.



US-CERT Control Systems Security Center

A Department of Homeland Security program to secure national infrastructures

Case Study Series: Vol 1.1

Backdoors and Holes in Network Perimeters

A Case Study for Improving Your Control System Security

Troy Nash
Vulnerability & Risk Assessment Program (VRAP)
Lawrence Livermore National Laboratory
UCRL-MI-215398

August 2005

Backdoors and Holes in Network Perimeters

A Case Study for Improving Your Control System Security

Contents

Introduction... 1

Background... 1

Overview

Architecture

Threat

Example Attack Sequences

Discussion... 4

Conclusion... 7

Sponsor:

U.S. Dept. of Homeland Security
Control System Security Center



Developed by:

University of California



Note: This case study is fictional with composite elements from real-world examples and open source information. The goal of this series is to provide a neutral platform for the discussion of critical infrastructure security issues across a variety of sectors.

Introduction

The Supervisory Control and Data Acquisition (SCADA) system of a natural gas utility was compromised resulting in a reduction of operation. The breach was discovered when operator interfaces became unresponsive and the system was no longer acquiring data. As a result, the system was disconnected from the network and a combination of manual operation overrides and limited fail-over to a backup server went into effect until the environment could be restored. Technicians troubleshooting the incident identified the deletion of several core application files on the primary control server as the source of the problem.

Background

Overview

The SCADA system is operated by a natural gas company serving customers (residential, industrial, and some commercial) in several communities spread across a geographically diverse region. The company handles all aspects of distribution, storage, transportation, and customer service (installation, billing, meter reading) of the natural gas which it purchases from interstate suppliers. The primary purpose of the system is to monitor and control pressure, volume, temperature, and general operating status of the various pipeline facilities, including underground storage reservoirs and unmanned compressor stations at locations throughout the service area.

Architecture

Figure 1 illustrates the network environment at a conceptual level, including the following core elements:

DMZ – A less restrictive network used for public access services like Web and FTP. In this case, the target company hosts a website for Internet presence, customer

service, as well as providing some system data to industrial clients. Other systems provide applications for the company's operations. All of the hosts on the DMZ are on a separate subnet (with public, Internet-addressable IP addresses) behind the primary firewall.

Business LAN – The network used for the conduct of business operations, including Internet access, Intranet services (web, electronic mail, file sharing, printing, databases), and other application infrastructure for common business functions such as finances, human resources, market monitoring and operations, the employee desktop environment, and facility operations.

Operations LAN – The primary network where the SCADA system resides. Includes components such as the servers, operator workstations, historical archiver, alarm management, and data control (gateways, concentrators, multiplexers).

Remote Stations – The infrastructure located at the specific control point (e.g., compressor station). This is where the monitoring and control equipment resides, including the sensors and actuators (meters, valves, pressure controller, odorant injection) for the specific mechanism being monitored/controlled.

In addition, the following attributes of the overall environment are worth noting:

- The communications infrastructure is Ethernet and TCP/IP-based using a combination of leased-lines and microwave radio as the transmission medium between remote sites.
- The SCADA utilizes Unix-based systems, while all other systems (desktops, laptops, business servers) in the environment are Windows-based.

1

- There is a firewall and intrusion detection at the Internet perimeter between the Business LAN and the Internet. However, there are no intrusion sensors on the Operation LAN itself. Additionally, scanning activity from the Internet is ignored (no critical alerts are generated, no action is taken).
- The system includes several gas applications for analysis, data warehousing, and customer use, some of which are interconnected to systems external to the Operations LAN, but with very little security segmentation or compartmentalization between systems and networks in general.
- 802.11b wireless is used at the remote compressor stations. This allows field technicians easy access to the control network for diagnostics and maintenance purposes using their portable laptops.

Threat

Threat is defined for this case study as: *a source of danger (whether intentional, accidental, or natural) with the capability to cause harm, damage, or other operational impact to an asset (persons, property, data) by exploiting vulnerability.* Threats are dynamic, can change with time and opportunity, and are influenced by both internal and external events.

Specific threats may include an earthquake, a harmful biological agent, or an individual intent on disrupting operations. In this case, the threat is construed to be a human adversary such as a terrorist, hacker, activist, or disgruntled employee. In the following discussion, the threat will be referred to as the *adversary*.

The adversary in this case chooses to utilize a remote, cyber-based attack that does not require physical access to control system resources. While the attack described here is the deletion of files leading to a denial of service, other potential scenarios are possible, including more covert tactics such as capturing and exfiltrating data or controlling set points and operational parameters of

the SCADA system itself. The attack does not necessarily have to be isolated to the specific SCADA system but could be used in support of a coordinated "swarming" attack¹ using multiple exploits (both physical and cyber) in order to maximize the impact of the attack and further complicate recovery and response efforts.

Example Attack Sequences

In the case of our target company, we will focus on two attack sequences for achieving compromise of the environment. The first represents a *backdoor* that completely circumvents perimeter defenses while the second involves a *hole* that penetrates through perimeter defenses.

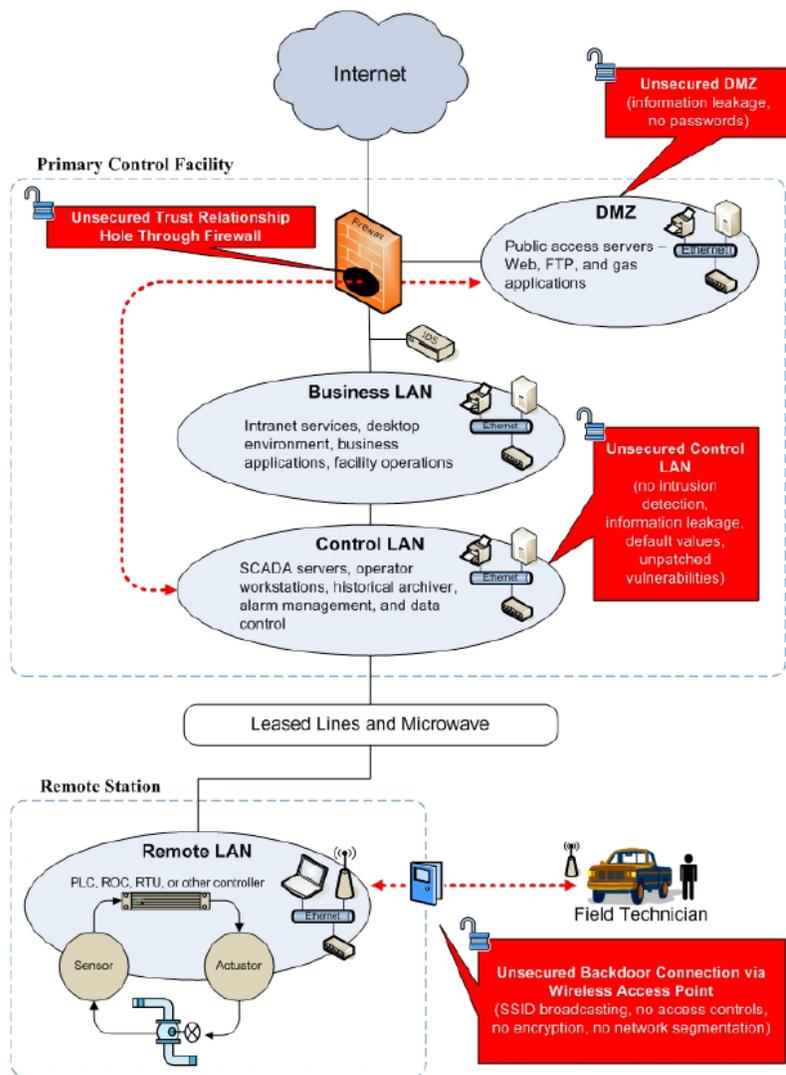


Figure 1

Attack Sequence #1 – Infiltration through the Wireless Access Point

STEP 1	The adversary becomes aware of the wireless access point at the remote facility (through reconnaissance, social engineering, insider knowledge, or wardriving). From a parked vehicle outside the property fence line, the adversary uses a standard mobile rig (laptop, 802.11 wireless network interface card, range-extending antenna, and discovery software) to determine the specifics of the wireless network. Signal strength, WEP usage, and the MAC address and SSID used by the wireless access point are obtained in a matter of seconds.
STEP 2	Using the SSID, the adversary attempts to gain access onto the wireless network. Since there are no security measures (authentication, access control, or encryption) in place, the adversary is able to associate with the access point unchallenged. Additionally, a Dynamic Host Configuration Protocol (DHCP) server is active on the network, assigning a dynamic IP address to the adversary's laptop, and thereby completing the connection to the wireless network.
STEP 3	Once connected, the adversary is able to probe the network and its systems. First, host discovery techniques are used to discover active systems on the network. Where possible, the specific network infrastructure (the switches, routers, and firewalls) is identified as well.
STEP 4	For those systems that are found to be live, a fast port scan is conducted to discover what ports they have open, as well as identify the operating system and applications in use. The adversary focuses on a small subset of ports that are typically associated with common exploits or specific control system environments such as port 21(FTP), 23(Telnet), 25(SMTP), 80(HTTP), 102(ICCP), 161(SNMP), 502(Modbus TCP), 1433/1434(MSSQL), and 20000(DNP).
STEP 5	SNMP (Simple Network Management Protocol) is found to be running on several systems. Using a SNMP utility and the default community string "public", the adversary connects to the open SNMP port and retrieves system information. The <code>system.sysDescr.0</code> field for one of the hosts is SCADA-01 . The vendor and version of the operating system is determined as well.
STEP 6	SCADA-01 is moved to the top of the adversary's list of potential target systems. Further probing identifies a vendor specific vulnerability in the operating system. An exploit is acquired from a well known hacker site and then attempted with success. The attacker gains root privileges and a command shell on the system then proceeds to recon the system for several hours before deleting the files which cause the denial of service.

Attack Sequence #2 – Infiltration through the DMZ

STEP 1	From a remote system on the Internet, the adversary performs reconnaissance of the company using keywords and custom searches to identify information that can be used to support the attack. In one document retrieved from the company's website, the adversary finds the hostname and IP address of the SCADA system. The adversary cannot connect directly to the system remotely because a firewall is blocking access from hosts on the Internet.
STEP 2	The adversary then proceeds to identify all of the public IP address ranges associated with the target company using the <i>American Registry for Internet Numbers</i> (www.arin.net) and then begins to perform various scans against those addresses to identify open ports and potential vulnerabilities.
STEP 3	A Windows system is discovered on the perimeter that has TCP port 139 (NetBIOS Session Service) open, used for connecting to file shares. Access to the port is not blocked by a firewall. Additionally, system accounts are not using strong passwords (a null administrator password can be used to remotely map the system drive). Once connected, the adversary is able to read, write, and delete files on the primary file system.
STEP 4	Before attempting to attack the SCADA system the adversary first recons the compromised box. The backup SAM file is acquired (to run a password cracker on) and the system (logs, caches, histories, bookmarks, scripts, batch files, archives, trash bin, etc.) is searched for information that can be used to propagate the current compromise to other systems on the network. It is discovered that the host uses SSH (Secure Shell) to connect to the SCADA server.
STEP 5	The adversary can successfully ping the SCADA system (using the IP address obtained from the document found on the Web in Step 1) from the compromised host. While the firewall is providing limited protection to hosts on the DMZ it is not blocking the DMZ network from making connections to systems on its trusted interface. In other words, a <i>trust relationship</i> exists between the hosts on the DMZ and hosts on the protected network. With an available access pathway, all that is required to attack the SCADA is more interactive control and a vulnerability. Virus protection software on the Windows machine prevents the uploading of known Trojans onto the system, but it does not prevent the installation of a remote access tool. The adversary escalates their control of the system by installing <i>rconsole</i> , giving them more freedom and options to remotely use the resources of the compromised host (or install their own) as if they were running the tools locally at that system.
STEP 6	From the compromised host, the adversary identifies that the SCADA system is using a vulnerable version of SSH. An exploit is crafted and then attempted with success. The attacker gains root privileges and a command shell on the system then proceeds to recon the system for several hours before deleting the files which cause the denial of service.

Discussion

Beyond the specific system vulnerabilities that allowed for a compromise of the SCADA host, four general observations can be made with respect to vulnerabilities in the overall environment that contributed to the success of the attack.

OBSERVATION #1:

Perimeter security is incomplete.

Modern process control environments face significant security challenges. SCADA or other DCS (Distributed Control Systems) that operate in these environments are distributed by nature and are not concentrated in a single area that is easy to delineate and defend.

The boundaries (both physical and logical) of these systems vary. Some are localized to a specific facility, while others span large geographical regions with multiple, interconnected sites. Given the dispersed environment, the perimeter—the outermost edges, border, interfaces, interconnections—that surrounds the control system is somewhat blurred and difficult to manage from a security viewpoint. This is especially true of the cyber components of the control system, as opposed to the physical apparatus which is easier to visualize and protect — it's a piece of hardware inside a room, within a building, behind a fence, on private property, and so on. But the cyber perimeter is less tangible, and unsecured backdoors and other holes in the network perimeter are not uncommon.

Consider the wireless access point. While the physical hardware may be locked inside a secure building, the network perimeter is not just the remote station anymore, but everything within wireless range of the access point, including the hosts that connect to it. Even though access from the Internet may be heavily monitored and guarded, this connection circumvents those security controls — it's the unlocked backdoor that puts the control system at risk as long as pathways such as these remain unsecured.

RECOMMENDATIONS

1. **Know your perimeter** – What is the boundary of your *network* perimeter? Is it simply the border gateway that separates your control system from other external networks? Is it at the firewall? What about a modem that connects directly to the SCADA system or the field technician's laptop that gets connected to both the control network and untrusted networks (e.g., at home, hotel, or airport)? To better understand your network perimeter, consider the following:
 - Take a complete inventory of all access points, remote connections, and other ways onto your networks. Consider all relevant mediums (satellite, microwave, radio, telecommunications, wireless 802.11, Bluetooth) and locations (remote stations, vendors, customers), not just the Ethernet pathway from the Internet.
 - Develop and maintain network or system-level diagrams that inventory and illustrate these connections and the security controls that are in place.
 - Develop a process for periodically verifying and modifying the inventory as the perimeter expands or shrinks.
2. **Defend your perimeter** – Appropriate security controls should be added to all entry points onto your network, not just the Internet connection. In this specific case, security should be added to the wireless network connection (see sidebar for suggestions) and the trust relationship on the DMZ should be broken.
3. **Test your perimeter** – Table-top review, assessments, wardialing, wardriving, scanning, and penetration testing will help identify backdoors and holes, as well as uncover potential vulnerabilities in perimeter defenses.

Tips for Improving Wireless Access Point (AP) Security

Change default parameters on your AP such as the administrator password and the SSID used for the network. Changes should be performed periodically, not just the first time the device is deployed.

Turn off SSID broadcasting on all non-public APs or single AP environments that have a pre-defined set of users.

Control access to the network. At a minimum, enable MAC address filtering and use WEP encryption keys to control access to the network. For a more secure approach, consider a dedicated authentication server.

Set up the AP on its own dedicated subnet. Establish separation and security controls between the wireless subnet and the wired network(s) that it connects to using a firewall or Access Control Lists (ACLs) on the router.

Use encryption for communications. Enable WEP (preferably with TKIP or other similar enhancement). Use the largest encryption key possible and change the key frequently (if applicable). Dynamic or session-based WEP keys offer the best protection. In addition, use higher-level encryption mechanisms like VPN, SSH, and SSL for connections between hosts.

Know your network. Maintain inventories and diagrams of systems and devices on your wireless local area network (WLAN). Enable logging on systems and devices and check logs regularly. Consider deploying a wireless intrusion detection system on the WLAN.

Conduct periodic assessments. Establish a practice of testing existing wireless environments to discover new vulnerabilities and rogue devices as well as to verify that the security posture is maintained over time.

IMPORTANT: Simple security measures (like disabling SSID broadcasting, enabling WEP, or using MAC address filtering) in and of themselves will not provide adequate security against a determined adversary. However, when used in combination as reinforcing layers in a "defense-in-depth" strategy, a more comprehensive security posture is established, raising the level of sophistication and effort required for a successful attack and increasing the opportunity to detect that attack.

**OBSERVATION #2:
Intrusion detection coverage is limited.**

While the infiltration is seamless in both attack sequences (the attacker looks like an ordinary user, accessing system resources by ordinary means), the network reconnaissance and subsequent exploit is very **loud**, generating suspicious traffic on the network, both outside the perimeter and on the interior networks. However, this is not discovered in either scenario because there are no intrusion sensors on the control system network and traffic from the host on the DMZ is given a regrettable pass because of the trust relationship.

RECOMMENDATIONS

1. **Verify intrusion detection coverage** – Consider all the potential access points to each of your networks, whether they are from the Internet, a remote station, or an Ethernet jack in a public lobby or conference room. Consider key choke points and mission-critical systems. These all become potential candidates for intrusion sensors and should be considered in the overall deployment of an intrusion detection system.
2. **Develop an intrusion detection capability** – Beyond hardware/software controls, establish a capability (people + tools + process) to monitor and react to suspected network and system-level intrusions, as well as to maintain and tune the specific detection rulesets and logging requirements for your organization.
3. **Evaluate the detection capability** – Perform regular tests at all perimeter entry points, key choke points, and from random systems on the networks. Confirm that intrusion detection is working as expected – i.e., suspicious activity (like scanning) and relevant exploit signatures are flagged and the appropriate response (email or page, for example) is generated and routed correctly.

4. **Report suspicious activity** – Communicate with Internet Service Providers (ISPs) regarding IP addresses within their range that are being used to conduct scans against your networks and notify law enforcement of exploit attempts. Also, consider reporting incident activity to external organizations (e.g., DShield.org or US-CERT) that track such information. Forming cooperative partnerships in an effort to share information (best practices, lessons learned) and identify trends and common issues is another effective strategy. While this will not stop an adversary, it will foster an image that your organization takes violations against your security seriously and are willing to act on them.

**OBSERVATION #3:
Nonexistent and default passwords were in use in the environment on both mission-critical and perimeter systems.**

The use of passwords for authentication (and subsequent access to systems) is a potential area of vulnerability in every security environment. The security issues relating to password authentication (i.e., the use of weak, default, or non-existent passwords) has consistently remained among SANS *Most Critical Internet Security Vulnerabilities*² since the inception of the list. The creation, distribution, usage, revocation, and other aspects of managing and protecting the keys to our network systems is an unending challenge, with many opportunities for failure.

On a control system network, the problem is exacerbated due to its mission-critical nature and the requirement for real-time operation. Operators need instant access to systems (getting locked out for mistyping a password in a crisis situation is not tolerable) and passwords often go unchanged simply because technicians do not want to risk bringing down a system that is stable. As such, shared, default, weak, or blank

passwords are not uncommon in these environments. In this case, the use of nonexistent and default passwords contributed to the success of the attack sequences described here. Specifically, the following observations are worth noting:

1. There was no password required for access to the wireless network.
2. There was no password required to access the file share on the perimeter system.
3. The SCADA server used the default SNMP community string (the protocol password) “public”.

In each case, a stronger password would not have adversely affected the operation of the environment, while significantly improving security.

RECOMMENDATIONS

1. **Change default and non-existent passwords** – This requires a comprehensive look at all of the default and non-existent passwords used in the environment, including:
 - User accounts (administrator, root, service, temporary, guest)
 - Application passwords (SCADA, FTP, SNMP, database, web, mail, file shares)
 - Scripts & source code (Web-applications, utilities, plug-ins)
 - Network devices (access points, routers, switches, printers, firewalls)
 - Control equipment (RTUs, PLCs, IEDs, ROCs)
2. **Develop and implement policy and procedures** – Establish the minimum requirements for creating strong passwords, such as: length, aging, reuse, character set to be used, as well as general principles—the password shouldn’t be found in a dictionary (English or foreign) or utilize personal information (such as name, birth date, or SSN).

The policy should also handle changing passwords after suspected compromise or when an untrusted user such as a vendor or technician is allowed temporary access to mission critical systems and devices. Finally, educate users regarding the policy and best practices for the security and overall usage of passwords.

2. **Assess the environment** – Periodically audit the passwords used in the environment to ensure that they meet policy requirements. At a minimum, systematically check mission-critical systems on a regular schedule.
3. **Wrap additional layers of security around the exceptions** – If a system absolutely must have a weak, blank, default, or shared password then it becomes important to add additional layers of security around that system. For example:
 - Deny remote login (only allow physical login at console/device).
 - Use a firewall or access control list to restrict network access to a given system. In other words, the user must use System X to remotely connect to System Y (the one with the weak, default, or nonexistent password). No other system is allowed access to System Y, regardless if the password is known or not.
 - Use more robust system event logging. Determine what the normal behavior is and is not and then flag those events that are suspicious – in order to identify brute-force guessing at login prompts, access to password files, and unusual command or data patterns.
4. **Consider alternative methods of authentication** – Where applicable, two-factor authentication (using smartcards, tokens, or bio-

metrics) should be considered as alternatives to using simple passwords by themselves. The advantage of two-factor authentication is that in order to access the system the user must provide something they have (smartcard, token, or fingerprint) and something they know (a PIN or Password). An adversary must acquire (or circumvent) both for the attack to succeed.

OBSERVATION #4: Sources of information leakage were present in the environment.

Unless the adversary is an insider or has otherwise acquired insider knowledge (through social engineering, coercion, blackmail, or bribery) the specifics of the network and systems prior to the attack are unknown. In the early stages of a cyber attack, the adversary operates somewhat blindly and must first discover the information, targets, and vulnerabilities necessary to execute the attack. In other words, adversaries do not magically know where your SCADA system is or what systems are vulnerable. They must discover this information through various techniques of scanning, probing, information searches, etc.

As we observed in both attack sequences, the adversary needed to gain knowledge in order to successfully attack the target. For example:

- The existence of the wireless network
- The SSID of the wireless network
- Live systems, open ports, potential vulnerabilities
- Version, brand, or type information of systems and devices
- The IP address, host name, or MAC address of target systems

If the SCADA system did not contain a descriptive name, or if its IP address was unknown, what system would the adversary attack? All of them? Or randomly, in hopes of identifying the

SCADA? The adversary's work is made much easier if information leakage exists, since they may not have the capability to profile a system across a network of hosts to adequately determine if a particular one is a SCADA system or not. Packet capture and analysis or social engineering are valid secondary options, but they involve more time and resources.

The less information you give to the adversary the harder their job becomes and the more likely you will discover their attack. In this case, the attacks succeeded because the adversary was able to easily acquire the information necessary. Finding ways to control and minimize information leakage without affecting operations is the challenge.

RECOMMENDATIONS

1. **Practice good Operations Security (OPSEC)** – OPSEC is a process that attempts to deny the adversary information that could be leveraged to improve the opportunity, success, and impact of an attack. Some recommendations for improving OPSEC in this case would be:
 - Not using descriptive names for mission-critical systems. While it may be more convenient for managing those systems, using names like SCADA or FIREWALL or DNS make those systems prime targets in keyword searches and network discovery.
 - Minimize the amount of information regarding vendors, versions, configurations, and applications that you provide (in banners, diagrams, documents, presentations, fact sheets, annual reports, etc.), especially if those resources are accessible via the network. Identify, track, and protect those sources that do contain such information.
 - Develop a review and release process for all information that is accessible via the Web

including webpages, documents, pictures, and other media files.

2. **Make use of obfuscation techniques where possible** – Default banners provide the adversary with information (type, version) about the applications in use on a given system. Vulnerability and port scanners often base their findings on the information returned from a standard query. This information can be used for attack planning and exploitation. Modifying these can trick the adversary (or automated tool) into launching the wrong attack as well as increase the opportunity for discovery. Similarly, default installations (directory structures, ports used, or other patterns) can reveal information. Renaming directories (e.g., using "/apps" instead of "/cgi-bin") and using different ports for special services (e.g., using port "9999" instead of a default "8080" for a given admin web service) are examples of obfuscation techniques that can frustrate the adversary's efforts.

Conclusion

Figure 2 illustrates some of the primary recommendations from this document, applied to the environment presented in Figure 1. Primary recommended mitigations included:

- reinforcing all perimeter access points
- improving intrusion detection coverage
- hardening password usage
- minimizing information leakage

These will serve as starting points for a more comprehensive, multi-layer security posture.

While the presence of vulnerabilities on the SCADA server did introduce risk, no single vulnerability was the ultimate cause of the compromise and subsequent denial of service presented in this case study. There were several factors that contributed to the opportunity and success of the attack. The consideration of these factors, as well as the recommendations provided in this document, can help to improve the overall security posture of control system environments across a variety of sectors that face similar issues.

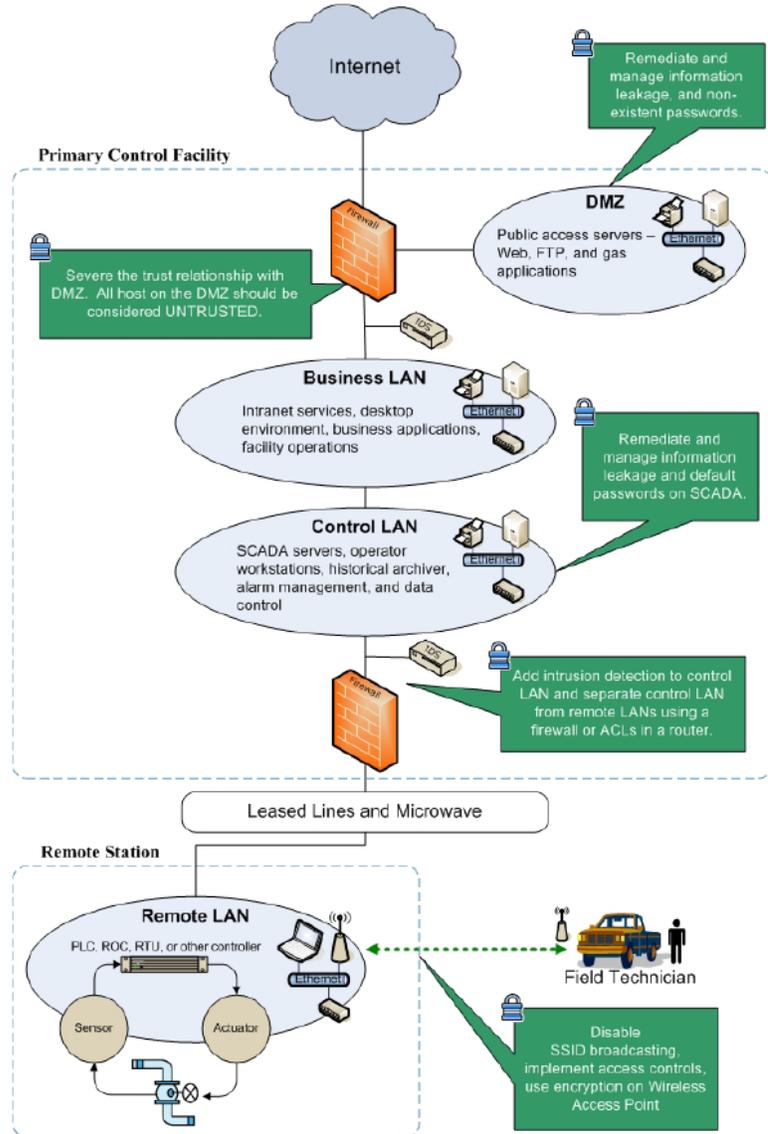


Figure 2

References

- [1] *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption*, a whitepaper developed by the National Infrastructure Protection Center (NIPC), July 2002.
- [2] *The SANS Top 20 Internet Security Vulnerabilities*, Version 5.0 October 8, 2004 Copyright (C) 2001-2004, SANS Institute, <http://www.sans.org/top20/>