A Survey of SCADA and Critical Infrastructure Incidents

Bill Miller
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 1985
bill_miller@byu.edu

Dale C. Rowe Ph.D
Brigham Young University
Information Technology Program
Provo, Utah
+1 (801) 422 6051
dale_rowe@byu.edu

ABSTRACT
In this paper, we analyze several cyber-security incidents involving critical infrastructure and SCADA systems. We classify these incidents based on Source Sector, Method of Operations, Impact, and Target Sector. Using this standardized taxonomy we can easily compare and contrast current and future SCADA incidents.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General --- Security and Protection.

General Terms
Documentation, Security.

Keywords
SCADA, Critical infrastructure, Security, Cyber security, Information assurance and security, Cyber attack, Incident response.

1. INTRODUCTION
Supervisory Control and Data Acquisition (SCADA) systems are used in many Critical Infrastructure applications. These applications are increasingly becoming the targets of cyber-attacks.

Historically, SCADA systems relied on air-gapped networks and non-standard protocols to protect them from attack. Increasingly, these networks have been connected to corporate networks and thus, the internet. There have also been advances in using standard networking protocols for communications [1].

These changes have made SCADA systems more available for attackers to target from anywhere in the world. The critical nature of these systems also makes these intriguing targets. For the first time, attacks in cyberspace can have physical manifestations in the real world. This presents a valuable and in many instances, easy to access target to those who desire to cause disruption to physical services for whatever motive. These factors have combined to increase the number of attacks against SCADA systems.

SIGITE'12, October 11–13, 2012, Calgary, Alberta, Canada.

In order to prepare to defend against future attacks against critical infrastructure, it is necessary to understand how these attacks have been carried out in the past. In this paper, we will discuss a sampling of these historical attacks and classify them by factors that allow us to analyze these attacks along with their targets and sources. This analysis will allow us to more clearly understand the nature of these attacks and how they may be carried out in the future.

2. CLASSIFICATION OF INCIDENTS
For the purposes of this paper, we use a modified version of the taxonomy presented by Kjaerland to classify attacks based on 'Source Sectors', Method of Operation (MO)', 'Impact', and 'Target Sectors' [5]. Each facet of the classification can be broken down into the terms shown in Table 1 and are subsequently explained.

Table 1: Taxonomy [5]

Source Sectors	Method of Operation(MO)	Impact	Target Sectors
Com	Misuse of Resources	Disrupt	Com
Gov	User Compromise	Distort	Gov
Edu	Root Compromise	Destruct	Intl
Intl	Social Engineering	Disclosure	
User	Virus	Death	
Unknown	Web Compromise	Unknown	
	Trojan		
	Worm		
	Recon		
	Denial of Service		
	Other Sys Failure		

2.1 Source Sectors
Source of the incident if explicitly identified (all sectors refer to US sites, except Intl.).

Com – Denotes a commercial source (including consumer products, industry, small business).

Gov – Denotes local or national government (including buildings/housing, emergency services, public benefits, social services, state and federal government, taxes, tribal governments, worker protections, environment, military).

Edu – Denotes a postsecondary school.

Intl – Denotes a Non-US entity.

User – Denotes an individual user.

Unknown – Indicates the source is not known.

2.2 Method of Operation (MO)

Method(s) used by a perpetrator to carry out an attack.

Misuse of Resources – Unauthorized use of IT resources. Ex. Storing unauthorized files on a server, using site as springboard for further unauthorized activity.

User Compromise – Perpetrator gains unauthorized use of user privileges on a host.

Root Compromise – Perpetrator gains unauthorized administrator privileges on a host.

Social Engineering – Gaining unauthorized access to privileged information through human interaction and targeting people's minds rather than their computers.

Virus – A virus is a piece of code that, when run, will attach itself to other programs, which will again run when those programs are run.

Web Compromise – Using vulnerabilities in a website to further an attack.

Trojan – A Trojan is a program that adds subversive functionality to an existing program.

Worm – A program that propagates itself by attacking other machines and copying itself to them.

Recon – Scanning/probing site to see what services are available. Determining what vulnerabilities exist that may be exploited.

Denial of Service – An exploit whose purpose is to deny somebody the use of the service: namely to crash or hang a program or the entire system.

Other Sys Failure – The incident was caused by a design failure or other unknown.

2.3 Impact

The effect of an attack.

Disrupt – Access change, removal of access to victim or to information. Manipulate permissions, e.g. Denial of Service attack or Trojan horse. 'Disrupt' would be the least invasive nature of attack.

Distort – File change, modification of information from victim. This is a change to data within files.

Destruct – File deletion, removal of information from victim. Destruct would be seen as the most invasive and malicious and may include Distort or Disrupt.

Disclosure – Unauthorized exposure of information, other than in support of one of the above. Disclose would imply disclosure of information that may lead to further compromises. Ex. Download of password file.

Death – Loss of human life.

Unknown – Insufficient information to classify.

2.4 Target Sectors

Victim of the incident (all sectors refer to US sites, except Intl.).

Com – Commercial entity (including consumer products, industry, small business).

Gov – Local or national government (including buildings/housing, emergency services, public benefits, social services, state and federal government, taxes, tribal governments, worker protections, environment, military).

Intl – A Non-US target.

3. SURVEY OF INCIDENTS

The following are an analysis of several Critical Infrastructure security failings in chronological order. For each failure a brief description and classification using the aforementioned taxonomy is provided. Note that not every failure is due to external attack (although this is true for the majority).

3.1 Siberian Pipeline Explosion (1982)

This is the first known cyber-security incident involving critical infrastructure. In 1982, intruders planted a Trojan in the SCADA system that controls the Siberian Pipeline. This caused an explosion equivalent to 3 kilotons of TNT [2].

Source Sector: Unknown

MO: Trojan

Impact: Distort

Target Sector: Intl

3.2 Chevron Emergency Alert System (1992)

A fired employee of Chevron's emergency alert network disabled the firm's alert system by hacking into computers in New York and San José, California, and reconfiguring them so they would crash. The vandalism was not discovered until an emergency arose at the Chevron refinery in Richmond, California, and the system could not be used to notify the adjacent community of the release of a noxious substance. During the ten-hour period in 1992 when the system was down, thousands of people in twenty-two states and six unspecified areas of Canada were put at risk [3].

Source Sector: User

MO: Misuse of Resources, User Compromise

Impact: Disrupt

Target Sector: Com

3.3 Salt River Project (1994)

Between July 8th and August 31st, 1994, an attacker gained unauthorized access to the Salt River Project 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, Salt River Project's water SCADA system operated a 131-mile canal system, which was used to deliver water to customers in the Phoenix metropolitan area. The attacker 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 [11].

Source Sector: User

MO: Root Compromise, Trojan

Impact: Disclosure

Target Sector: Gov

3.4 Worcester, MA Airport (1997)

In March 1997, one hacker penetrated and disabled a telephone company computer that serviced Worcester Airport in Massachusetts. As a result, the telephone service to the Federal Aviation Administration control tower, the airport fire department, airport security, the weather service and various private airfreight companies was cut off for six hours. Later in the

day, the juvenile disabled another telephone company computer, this time causing an outage in the Rutland area. The outage caused financial losses and threatened public health and public safety [3].

Source Sector: User

MO: Root Compromise, Denial of Service

Impact: Disrupt

Target Sector: Gov

3.5 Gazprom (1999)

In 1999, hackers broke into Gazprom, a gas company in Russia. The attack was collaborated with a Gazprom insider (disgruntled employee). The hackers were said to have used a Trojan Horse to gain control of the central switchboard, which controls gas flow in pipelines [8].

Source Sector: Intl

MO: User Compromise, Trojan

Impact: Disrupt

Target Sector: Intl

3.6 Bellingham, WA Gas Pipeline (1999)

In June 1999, 237,000 gallons of gasoline leaked from a 16" pipeline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1 1/2 hours after the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek causing 3 deaths and 8 documented injuries. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. The National Transportation Safety Board (NTSB) report issued October 2002 cited one of the five key causes of the accident was the Olympic Pipe Line Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline [10]. While not technically an attack, the loss of human life in this incident illustrates the dangers of any type of failure in a critical infrastructure system.

Source Sector: User

MO: Misuse of Resources

Impact: Disrupt

Target Sector: Com

3.7 Maroochy Water System (2000)

In Maroochy Shire, Queensland, Australia in 2000 a disgruntled ex-employee hacked into a water control system and flooded the grounds of a hotel and a nearby river with a million litres of sewage. The Maroochy Shire attack was not one attack but a whole series of attacks over a prolonged period [6].

Source Sector: Intl

MO: Misuse of Resources, User Compromise

Impact: Disrupt

Target Sector: Intl

3.8 California System Operator (2001)

Attackers, possibly from China, were able to gain access into one of the computer networks at the California Independent System Operator (Cal-ISO) in May 2001. The Cal-ISO has hierarchical control over a number of PCS networks operated by its constituent transmission owners. This hack was unsuccessful at penetrating any PCS network, yet it uncomfortably extended a period of longer than two weeks [9].

Source Sector: Intl

MO: Root Compromise

Impact: Unknown

Target Sector: Gov

3.9 Davis-Besse Nuclear Power Plant (2003)

In January 2003, the SQL Slammer worm infected the Davis Besse nuclear power plant in Ohio, USA. As a result of the worm's activity, the plant's Safety Parameter Display System and Plant Process Computer were disabled for several hours [8].

Source Sector: Unknown

MO: Worm

Impact: Disrupt

Target Sector: Com

3.10 CSX Corporation (2003)

In a similar case to the SQLSlammer worm, also in 2003, a computer virus named Sobig was reported to have shut down train signaling systems in Florida, U.S. The virus was reported to have been one of the fastest spreading e-mail attachment viruses at the time. It shut down the signaling, dispatching and other systems at CSX Corporation; one of the largest transportation suppliers in the U.S. While there were no major incidents caused by this case, trains were delayed [7].

Source Sector: Unknown

MO: Virus

Impact: Disrupt

Target Sector: Com

3.11 Tehama Colusa Canal Authority (2007)

A former electrical supervisor at Tehama Colusa Canal Authority (TCAA) installed unauthorized software on the TCAA's SCADA system. The employee is reported to have installed the software on the day that he was dismissed, having worked at the company for 17 years. No technical reports or analysis have been publicly released that detail the unauthorized software, nor has there been any insight as to whether or not damage was caused [7].

Source Sector: User

MO: Misuse of Resources

Impact: Unknown

Target Sector: Gov

3.12 Stuxnet (2010)

In June 2010, it was discovered that a worm dubbed Stuxnet had struck the Iranian nuclear facility at Natanz. Stuxnet used four 'zero-day vulnerabilities' (vulnerabilities previously unknown, so there has been no time to develop and distribute patches). The worm employs Siemens' default passwords to access Windows operating systems that run WinCC and PCS7 programs. The worm would hunt down frequency-converter drives made by Fararo Paya in Iran and Vacon in Finland. These drives were used to power centrifuges used in the concentration of the uranium-235 isotope. Stuxnet altered the frequency of the electrical current to the drives causing them to switch between high and low speeds for which they were not designed. This switching caused the centrifuges to fail at a higher than normal rate [4].

Source Sector: Intl

MO: Worm, Root Compromise, Trojan

Impact: Disrupt, Distort

Target Sector: Intl

3.13 Night Dragon (2011)

In February 2011 McAfee reported that five global energy and oil firms were targeted by a combination of attacks including social engineering, trojans and Windows-based exploits. The attacks, code-named 'Night Dragon', have been confirmed to have been ongoing for over two years and are believed to have been of Chinese origin. It is noted that the attackers may simply be using Chinese tools and compromised Chinese computers in order to mask their identity. While no SCADA systems were directly attacked, the corporate network segments belonging to companies that operate SCADA infrastructures were attacked. It is reported that attackers exfiltrated data such as operational blueprints [7].

Source Sector: Intl

MO: Social Engineering, User Compromise, Root Compromise

Impact: Disclosure

Target Sector: Intl

3.14 DUQU (2011)

In 2011, Virus Researchers discovered a new form of Malware that utilized many of the same techniques as Stuxnet. The new code was named Duqu and contained parts that were nearly identical to Stuxnet. Duqu was not self-replicating and did not contain a payload. It appears to be designed to conduct reconnaissance on an unknown industrial control system [13].

Source Sector: Intl

MO: Virus

Impact: Disclosure

Target Sector: Intl

3.15 Flame (2012)

Researchers have recently discovered a piece of malware operating in Iran, Lebanon, Syria, Sudan, the West Bank and other places in the Middle East and North Africa for at least two years. This malware dubbed "Flame" appears to be sponsored by the same group that was behind Stuxnet. Early analysis indicates that it's designed primarily to spy on the users of infected computers and steal data, including documents, recorded conversations and keystrokes. It also opens a backdoor to infected systems to allow the attackers to tweak the toolkit and add new functionality. Flame was discovered after the United Nations International Telecommunications Union asked researchers to look into reports in April that computers belonging to the Iranian Oil Ministry and the Iranian National Oil Co. had been hit with malware that was stealing and deleting information from the systems [12].

Source Sector: Unknown

MO: Worm

Impact: Disclosure, Destruct

Target Sector: Intl

Table 2: Summary of Incidents

Year	Title	Source Sector	MO	Impact	Target Sector
1982	Siberian Pipeline Explosion	Unknown	Trojan	Distort	Intl
1992	Chevron Emergency Alert System	User	Misuse of Resources, User Compromise	Disrupt	Com
1994	Salt River Project	User	Root Compromise, Trojan	Disclosure	Gov
1997	Worcester, MA Airport	User	Root Compromise, Denial of Service	Disrupt	Gov
1999	Gazprom	Intl	User Compromise, Trojan	Disrupt	Intl
1999	Bellingham, WA Gas Pipeline	User	Misuse of Resources	Disrupt	Com
2000	Maroochy Water System	Intl	Misuse of Resources, User Compromise	Disrupt	Intl
2001	California Systems Operator	Intl	Root Compromise	Unknown	Gov
2003	Davis-Besse Nuclear Power Plant	Unknown	Worm	Disrupt	Com
2003	CSX Corporation	Unknown	Virus	Disrupt	Com
2007	Tehama Colusa Canal Authority	User	Misuse of Resources	Unknown	Gov
2010	Stuxnet	Intl	Worm, Root Compromise, Trojan	Disrupt, Distort	Intl
2011	Night Dragon	Intl	Social Engineering, User Compromise, Root Compromise	Disclosure	Intl
2011	Duqu	Intl	Virus	Disclosure	Intl
2012	Flame	Unknown	Worm	Disclosure, Destruct	Intl

4. ANALYSIS OF INCIDENTS

Figure 1 represents the Source Sectors for the attacks surveyed in Section 3. We found five attacks from International sources, four were a single user source and four were unknown.

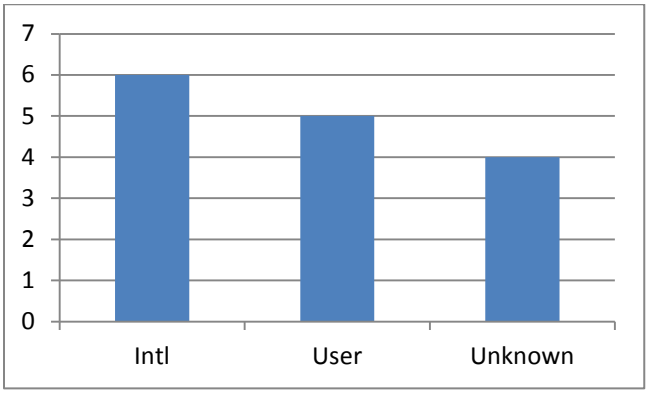

Figure 1: Source Sectors

Figure 2 details the attacks by Method of Operations. Five of the attacks surveyed utilized a Root Compromise, four took advantage of a User Compromise, four others used a Trojan, three of the attacks involved a Misuse of Resources, two attacks used a Worm, one utilized a Denial of Service, one was a Virus, and one was a Social Engineering attack.

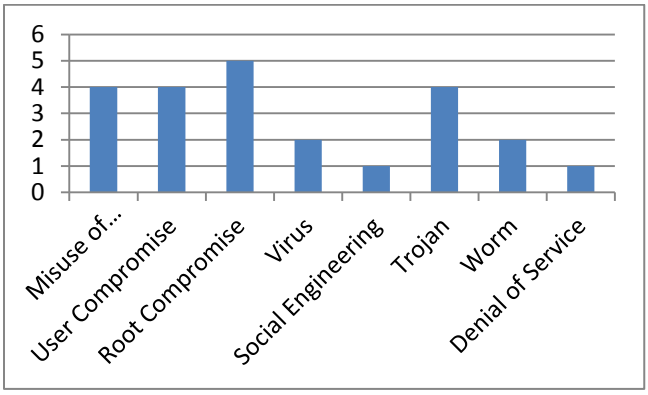

Figure 2: Method of Operations

We next look at the Impact of these attacks. The majority of the attacks disrupted operations, three disclosed data, two distorted data, one destroyed data, and one had unknown impact.

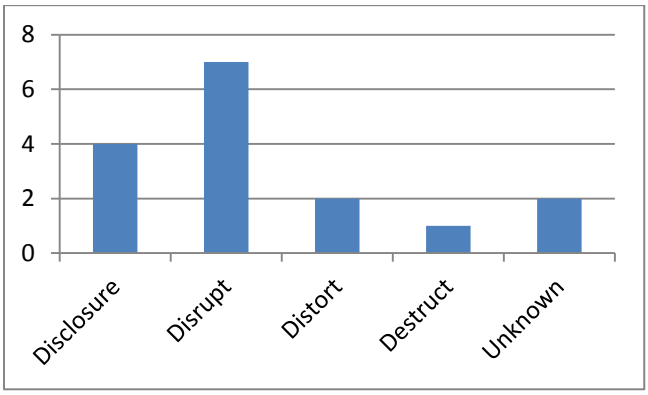

Figure 3: Impact

The Target Sectors of the attacks break down as follows. Five attacks were against Intl targets, four were Gov, and 3 were Com.

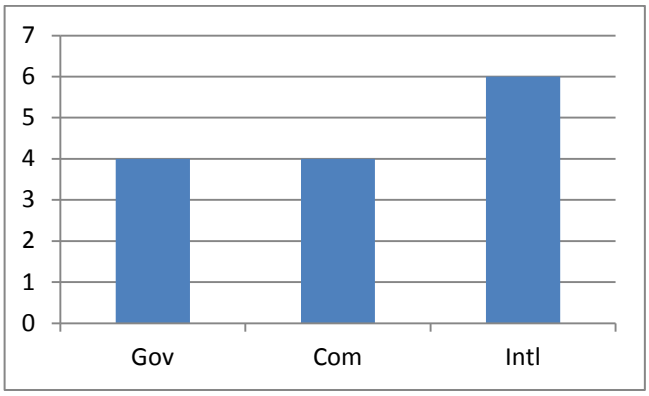

Figure 4: Target Sectors

The frequency of incidents is increasing as can be seen when we chart the number of incidents by year.

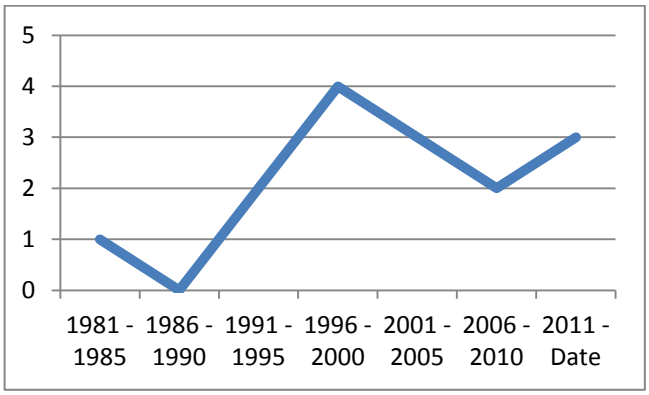

Figure 5: Incidents by Year

Care should be taken in interpreting these above figures due to the incomplete dataset. The incidents covered represent some of the more visible and documented attacks to date but is incomplete. In the creation of a database to analyze such attacks we intend to provide a quantifiable measure for identifying and subsequently presenting 'significant' attacks.

5. CONCLUSIONS

The preceding list and analysis is a sampling of malware attacks. To include a complete list would extend this paper well beyond its intended length. As of 2005, the RISI database included over 120 such incidents [11]. Understanding the nature of SCADA attacks and their evolution over time can assist the development of new techniques to mitigate their impact. We propose compiling a comprehensive database of incidents using a standardized terminology and quantifiable data to determine the severity of the incident. We also propose making such information freely available to other academic and nonprofit research organizations. This database shall include references to research papers that present an interpretation of an incident.

6. ACKNOWLEDGEMENTS

We acknowledge and thank the individuals and organizations that have taken significant steps in documenting SCADA incidents.

7. REFERENCES

[1] Cheung, S. et al. 2006. Using Model-based Intrusion Detection for SCADA Networks.

[2] Daniela, T. 2011. Communication security in SCADA pipeline monitoring systems. *Roedunet International Conference (RoEduNet), 2011 10th*.

[3] Denning, D.E. 2000. Cyberterrorism: The Logic Bomb versus the Truck Bomb - Centre for World Dialogue. *Global Dialogue*. 2, 4 (2000).

[4] Farwell, J.P. and Rohozinski, R. 2011. Stuxnet and the Future of Cyber War. *Survival*. 53, 1 (Feb. 2011), 23–40.

[5] Kjaerland, M. 2006. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*. 25, 7 (Oct. 2006), 522–538.

[6] Mustard, S. 2005. Security of distributed control systems: the concern increases. *Computing & Control Engineering Journal*.

[7] Nicholson, A. et al. 2012. SCADA Security in the light of Cyber-Warfare. *Computers & Security*. 31, 4 (Mar. 2012), 436–418.

[8] Remenyi, E. by D.D. et al. 2006. *Proceedings of the 5th European Conference on Information Warfare and Security: National Defence College, Helsinki, Finland, 1 - 2 June 2006*. Academic Conferences Limited.

[9] Stamp, J. et al. 2003. Common vulnerabilities in critical infrastructure control systems. *Sandia National Laboratories*. (2003).

[10] Tsang, R. Cyberthreats, Vulnerabilities and Attacks on SCADA Networks.

[11] Turk, R.J. 2005. Cyber Incidents Involving Control Systems. *Contract*. October (2005).

[12] Zetter, K. 2012. “Flame” spyware infiltrating Iranian computers - CNN.com. *Wired*.

[13] Zetter, K. 2011. Son of Stuxnet Found in the Wild on Systems in Europe. *Wired*.