INL/CON-05-00001
PREPRINT

Process Control Systems in the Chemical Industry: Safety vs. Security

20th Annual CCPS International Conference

Jeffrey Hahn
Donna Post Guillen
Thomas Anderson

April 2005

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

Process Control Systems in the Chemical Industry: Safety vs. Security

Jeffrey Hahn, Donna Post Guillen, Thomas Anderson

Idaho National Laboratory, Control Systems Security and Test Center
Idaho Falls, Idaho
Jeffrey.Hahn@inl.gov, Donna.Guillen@inl.gov, Thomas.Anderson@inl.gov

ABSTRACT

Traditionally, the primary focus of the chemical industry has been safety and productivity. However, recent threats to our nation's critical infrastructure have prompted a tightening of security measures across many different industry sectors. Reducing control system vulnerabilities against physical and cyber attack is necessary to ensure the safety, reliability, integrity and availability of these systems. The U.S. Department of Homeland Security has developed a strategy to secure these vulnerabilities. Crucial to this strategy is the Control Systems Security and Test Center (CSSTC) established to test and analyze control systems and their components. In addition, the CSSTC promotes a proactive, collaborative approach to increase industry's awareness of standards, products and processes that can enhance the security of control systems. This paper outlines measures that can be taken to enhance the cybersecurity of process control systems in the chemical sector.

1. INTRODUCTION

Evidences of safe working environments and practices and secure working places are found in almost every chemical plant. The evidence for cybersecurity is not as readily apparent. However, keeping computers and networks free from viruses and hackers (and available for productive use) is just as important as keeping thieves and terrorists out of the plant. The purpose of this paper is to establish the need for cybersecurity for the chemical industry and to identify the common vulnerabilities of control systems.

2. DISCUSSION

The Safety Mind-Frame

Security, like safety, must be an integral part of any chemical process. Operating procedures are developed with the safety of workers, the public, and our environment in mind. Equipment is designed with safety in mind. The proper protective equipment is worn with safety in mind. Physical security surrounds the chemical plant. "Guards, gates and guns" are used to ensure the environment is safe for the workers. It protects the documents and processes that are business sensitive and classified. The right people are let through the guard gate and the wrong people are kept out.

Both physical security and cybersecurity are put in place with safety in mind. cybersecurity protects control systems to keep the chemical processes working safely and efficiently. It ensures the data are not compromised. It keeps the computer viruses, worms, Trojans, etc. from infecting the computers on the network and from affecting the control systems. It lets the right people access the controls and information, and keeps the wrong people off the controls denying them access to sensitive and proprietary information and out of the network.

Cybersecurity – Is the Threat Real?

Cybersecurity threats are real and they happen every day to people in all walks of life. With the modernization of control system equipment more systems are interconnected and more importantly, more systems are linked at some level to the internet. With each additional connection comes one more doorway by which a hacker, curious or malicious, can enter. Additionally the control system networks are becoming more public. Operations within a chemical or electrical have traditionally been closed and little was known about them to the outsider. Last year at one of the principle cyber forums in this country, a hacker gave a presentation on control systems. Interest and curiosity is rising along with the visibility.

Cyber attacks can slow the computer's response and the networks speed or bring everything to a complete halt, causing a denial of service. Cyber attacks can also cause unwanted and unexpected results. In the world of chemical processing where efficiency is critical to making a profit, an undetected cyber attack can slow the process and reduce the efficiency of the plant. An article from the Rand Corporation stated, "Attacks in cyberspace blur traditional boundaries between nations and private interests, cannot be foreseen or tracked via classical intelligence methods, and are all but indistinguishable from accidents, system failures or even hacker pranks."[1] The critical infrastructure of the United States provides many lucrative targets.

A well known example of a cyber attack that had disastrous results occurred in Australia. A contractor who had been instrumental in installing the network for a waste management company "caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel. . . Marine life died, the creek water turned black and the stench was unbearable for residents."[2] A series of cyber attacks had been occurring for at least 2 months before the waste management company learned what was happening and identified the source of the trouble.

In January 2003, the slammer worm caused the Internet to slow down to a crawl. The Bank of America reported "that customers at a majority of its 13,000 automatic teller machines were unable to process customer transactions."[3] It is not hard to imagine how a

Chemical process could become paralyzed if a similar worm were to infect their network system.

The CERT Coordination Center has kept statistics on the number of incidents that have been reported to them between 1988 and 2003. The number of cybersecurity incidents reported each year has been rising rapidly. In 1999, there were about 10,000 incidents reported. In 2003, there were almost 140,000 incidents reported. This exponential increase in incidents demonstrates another interesting and important fact. There are more and more people who are proliferating cyber attacks. As shown in Figure 1, the cyber attacks are becoming more and more sophisticated yet the average person's knowledge required to spawn an attack is actually being reduced. One of the major reasons for this is because the internet has enabled hackers to share their experiences and techniques and obtain tools. For example, a New Jersey man was charged with computer criminal activity and attempted criminal activity for placing spyware on his landlord's computer to see how she was going to proceed collecting a $10,000 judgment from him. A service provider verified that the spyware came from his email address. He is currently out on $30,000 bail.[4]

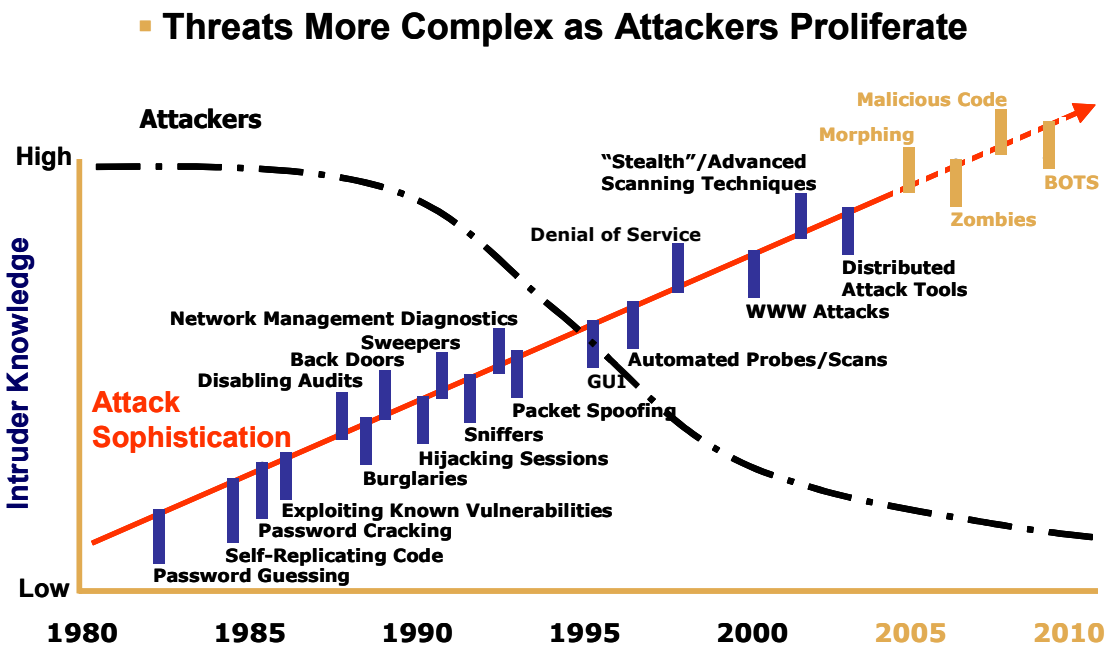

Figure 1 – Intruder Knowledge vs. Attack Sophistication

Cyber threats are real. Cyber attacks come from a wide variety of sources including, viruses/worms/trojans/etc, an insider or a disgruntled employee, neighborhood hackers, industrial espionage, terrorists. Reconnaissance is typically a pre-cursor to an attack. All of the above mentioned sources can cause problems with control systems. However, some of these sources have the intent to create problems on a very large scale. Two examples are note worthy. First, the Washington Times reported that "China is actively developing options to create chaos on the island, to compromise components of Taiwan's critical infrastructure."[5] Then Media Corp News reported that "North Korea has trained more than 500 computer hackers capable of launching cyber warfare against the United States. . . The Military hackers had been put through a five-year university course

training them to penetrate the computer systems of South Korea, the United States and Japan."[6]

The U.S. Department of Homeland Security (DHS) has an objective to "create a national-level capability to coordinate between government and industry to reduce vulnerabilities and respond to the threats associated with the control systems that comprise our National Critical Infrastructure."[7] The mission of the DHS National Cyber Security Division is to be the focal point for addressing cyber security issues in the United States."[8] In order to accomplish that mission, the DHS National Cyber Security Division has established the Control System Security and Test Center (CSSTC). The CSSTC is working to identify, analyze and eliminate vulnerabilities associated with the control systems in critical infrastructure applications. A major effort is being made to increase awareness of the need for cybersecurity and what to do to reduce vulnerabilities in control systems.

Taking action to reduce or eliminate a vulnerability will reduce the probability of a successful cyber attack. There are common things that any company can do to reduce the vulnerabilities in their control system. Below are the top 10 vulnerabilities commonly found within control systems.

Top 10 Vulnerabilities in Control Systems

10. **Insufficient network separation (protection) between corporate and real-time control systems.** The corporate and process control networks should be separated by a properly configured firewall. The architecture of the network is essential to good cybersecurity. Figure 2 shows the recommended network architecture.

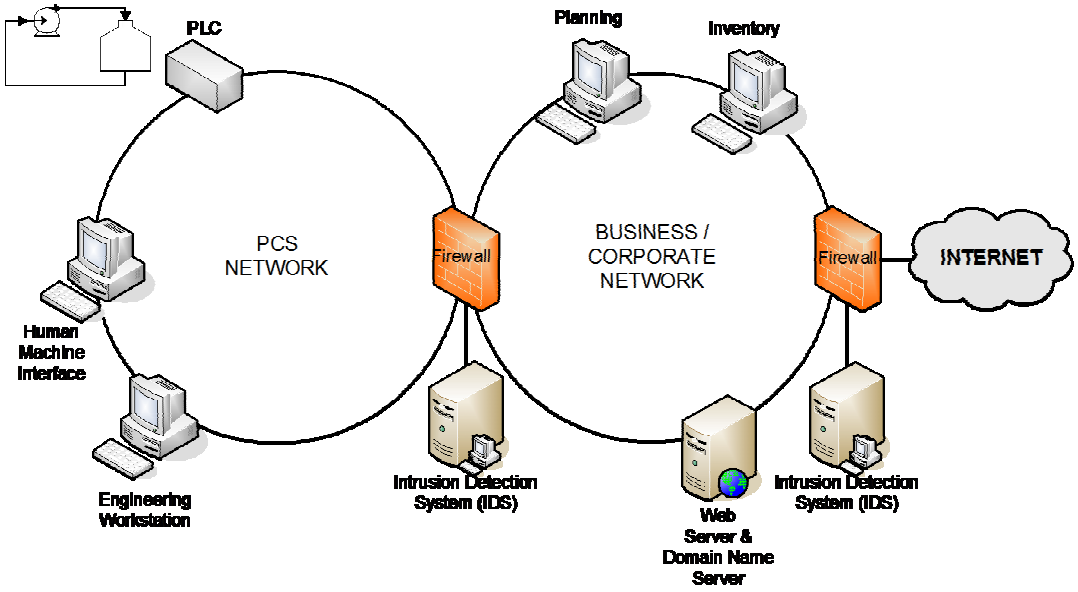

Figure 2 – Recommended Network Architecture

9. **Security efforts focused solely on corporate internet interface point.** When the IT organization assumes that if the corporate network is protected then the rest of the control system is protected it leaves the process control

network open for attack. Some of the best and most secure networks have been compromised by an employee bringing in a laptop w/an embedded Trojan or Worm, connecting to the production network and introducing the malicious code. Therefore, practicing defense in depth is an essential cybersecurity practice.

8. **Remote access to the process control LAN not properly secured.** Many control systems have modems or wireless access. These communication points need to be secured with, for example, encryption or passwords. Equipment vendors frequently leave open ports for remote maintenance of equipment.

7. **Dual-Network cards installed and in use, bridging the two networks**. If a single computer has direct access to both the corporate and process control networks through separate network cards, a hacker can bypass the firewall. This can include remote communications when the remote user connects through a commercial ISP service.

6. **Null-Session Authentication, shared folders, and "everyone" permissions defeat any internal IT controls**. Everyone needs to be trained on good cybersecurity practices. These commonly found security "no-no's" are primarily used for exploiting a system once access is gained. The fewer internal access controls are in place the easier it is for a successful penetration to turn into a successful exploitation.

5. **Process LAN and associated systems easy to find by obvious PC name**. If a hacker can make it into the process control network, it only makes life easier for them if they can easily recognize the names of the equipment, instrumentation and controllers. There are many instances of people making life easier by naming their systems with critical information, i.e., Firewall1, Primary DNS, Historian or History1.

4. **No outbound filtering of data.** Data needs to be filtered as it exits the process control network as well as filtering the data stream as it enters. The only way to know what is being transferred into and out of your network is to look at the data. Know which systems should be talking to which systems and look for anomalies.

3. **Workstations / Servers running process control applications not properly patched.** Nearly every critical exploit for the past several years has had an existing patch. Patches are created by the vendor to make their system work better and operate more securely. Keep your anti-virus software updated, too. Patching in control systems is not easy. We must test, retest and then carefully examine both the need and the net gain. If equal protection or mitigation can be gained another way for the short term then use it while you plan and patch.

2. **Policies either not in place, not followed, inadequate or not enforced (password, backup/restore, etc…)**. Event the best training program and the best network architecture will be defeated if the company policies are inadequate or not enforced. Passwords have been found taped to the system, under the keyboard, in a file on the system named "Passwords" or "psswd" and even shared with coworkers.

1. **Social engineering (i.e., human factors) and physical security extremely weak.** Your friendly industrial espionage agent will tell you that a few secrets learned through social engineering or by gaining access to the network system will make the hackers' job infinitely easier. An effective counterintelligence or Operations Security program and strict adherence to policies and procedures are essential.

3. CONCLUSION

Cybersecurity is critical to success in today's business world. It helps defend against cyber attack on control systems for both the casual and the malicious intruder as well as industrial espionage. Cyber attacks are a reality in today's world, and critical infrastructures are increasingly the target. The number of cyber incidences and the sophistication of the attacks have dramatically increased. Companies can defend themselves against these attacks by reducing their process control network vulnerabilities and following good security practices and procedures. Critical infrastructures, such as the chemical industry, need to be proactive and protect their assets from potential cyber attacks and to ensure the safety of workers, the public and our environment.

4. ACKNOWLEDGEMENTS

This work was performed for the Department of Homeland Security under a Work For Others Agreement under DOE-NE Idaho Operations Office Contract DE-AC07-05ID14517.

5. REFERENCES

1 *Strategic Warfare*, by Roger C. Molander, Andrew S. Riddle, and Peter A. Wilson, MR-661-OSD. http://www.rand.org/news/Press.95.96/cyberwar.html

2 The Register, Hacker jailed for revenge sewage attacks; authored by Tony Smith, October 31, 2001, http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

3 MSNBC, Virus like attack slows web traffic, authored by Bob Sullivan, January 26, 2003; http://www.netserv.ch/docs/msnbc260103.pdf

4 The Star Leger, Father accused of spying with software, January 12, 2005. http://www.nj.com/news/ledger/morris/index.ssf?/base/news-4/1105511417114630.xml

5 Washington Times, Chinese Information Warfare Threatens Taiwan, authored by Bill Gertz, October 13, 2004.

6 MediaCorp News – Channel News Asia International, North Korea ready to launch cyber war: report, October 4, 2004. http://www.channelnewsasia.com/stories/afp_asiapacific/view/109911/1/.html

7 U.S. Executive Branch, White House Staff, Homeland Security Presidential Directive HSPD-7, White House Press, December 17, 2003. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

8 Executive Branch, White House Staff, The National Strategy to Secure Cyberspace, White House Press, February 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

9 Jonathan Pollett, Risk Mitigation – Top Ten Security Issues, UTC SCADA Security Conference, September 22, 2004