Global Information Assurance Certification Paper

The Challenge Of Process Control Security To the Chemical Industry

Bill Harvey
GSEC Practical, Version 1.4b
Option 1
February 8, 2004

Abstract

Not many years ago, process control systems used in the chemical and other process industries were completely isolated from companies' business systems: managed from consoles to which only a small number of technicians had access, and physically separated from the rest of the business and the Internet. System standardization and developments in data communications, networking, and enterprise integration are now driving the demand for interconnectivity between process control systems and business systems. This interconnectivity is unleashing a new set of problems and threats that are motivating the chemical industry to pull together to work on common solutions. This work is being done in other forums in which chemical companies take part, including process control industries overall and national critical infrastructure protection.

The purpose of this report is to identify the top challenges facing the chemical industry, and to some extent, all process control industries, due to the integration of process control systems into the mainstream of corporate information systems, and to describe the security processes and technologies that these organizations need to implement to meet those challenges. These techniques, while selected for their appropriateness to the process control issues described, are drawn for the most part from security best practices recognized by SANS and other experts, and should be familiar to most readers.

The Chemical Threat: No Exaggeration

The critical infrastructure industry that received the most negative press in 2003 had to be the electricity utilities, as a result of the northeastern U.S. blackout in August. However, the chemical industry had its own moment in the spotlight in the fall when it caught the attention of "60 Minutes", which aired a report on lax security practices at chemical plants [60 Minutes]. This report, based on the investigative work of Pittsburgh Tribune-Review report Carl Prine, emphasized, as does Prine's work, unlocked gates, oblivious guards, and the purported indifference of companies managing production and storage facilities to their vulnerability [Prine]. Although these reports did not deal with the process control system issue, they do, for our purposes, provide a glimpse at the potential for injury and loss of life from any accidental or malicious release of chemicals: "60 Minutes" reported that the U.S. has at least 100 plants where an accident or sabotage could endanger a million or more people [60 Minutes].

The inference from these reports is that chemical plants must be counted as natural targets of terrorism. Why would serious cyber-terrorists attack computers, information, or property if the means existed to launch large-scale attacks on human life? The U.S. General Account Office (GAO) reported to Congress in October 2003 that the FBI believes that terrorists are knowledgeable about and already using information exploitation tools to attack U.S. systems and data, and provided forceful examples of both actual verified attacks and theoretical attack channels against process control systems [GAO, pages 15-17]. The unavoidable conclusion: there is no more important

information security concern than critical infrastructure protection, and in turn there is no critical infrastructure more demanding of protection than chemicals.

Some Background

About Chemical Industry Groups and other Forums

The structure of standards, safety, and IT forums within the chemical industry can be confusing even to insiders. This should not be too surprising, given the industry's scope and diversity. Here is a brief introduction. Companies in the chemical industry participate in trade associations based on company size (the American Chemistry Council represents 145 of the largest companies), type of chemistry (The Chlorine Institute's 240 member companies are all involved with chlorine and related chemicals), or some other organizing principle (The National Association of Chemical Distributors has a membership of more than 300 chemical distribution companies). Ten of the major trade associations, comprising 2000 plus companies, support the Chemical Sector Cybersecurity Information Sharing Forum. This forum is responsible in turn for a Cybersecurity strategy and program. All of these initiatives started in 2002 [Chemical Cybersecurity]. In early 2003, the industry tapped the Chemical Industry Data eXchange (CIDX), an industry- funded institution that had previously developed the Chem eStandards XML-based data exchange standard, to pursue a CyberSecurity Practices, Standards and Technology Initiative. It is this CIDX initiative's participants who are leading the work on best practices for process control security for the industry [Chemical Cybersecurity].

Since process control security is important to many industries besides chemicals, this CIDX team wisely sought out the best resources already at work on the issue. At the end of 2003, they had identified and begun participating in two major initiatives beyond chemicals. The Instrumentation, Systems and Automation Society (ISA) is developing ISA-SP99, a standard for Manufacturing and Control Systems Security. CIDX is viewing this standard as guidance for process control security best practices that can be adopted soon or now. The other initiative the CIDX team is investing in is the Process Control System Requirements Forum (PCSRF). This forum is sponsored by a complex web of standards and security groups with its foundations in both the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). CIDX's alignment with the PCSRF is intended to address the chemical industry's future needs for process control security [Grant, slides 41, 43-45].

The effect of all these alliances is that the chemical industry, already committed to improving its information security position by high-level participation in national critical infrastructure protection initiatives, is also strengthening its commitment to process control security through both broader industry (ISA-SP99) and government (PCSRF) initiatives.

About Process Control Systems

As it may be apparent from the last section, process control systems are known by a variety of names. The ISA is expansive ("Manufacturing and Control Systems

Environment"); the GAO is crisp ("control systems"). Other overall identifiers include "manufacturing and process management", "manufacturing execution systems", and so on. From system vendors and developers one hears "embedded" and "real-time" systems. The point of this discussion is that, as with any broad area of knowledge or technology, expect even the experts to diverge on naming. For our purposes, "process control" and "process control system" (abbreviated PC and PCS in this paper) are acceptable terms that many authors rely on, whatever others they may use.

PCSs are computer-based systems used to monitor and control sensitive processes, typically by collecting sensor measurements and field data, processing and displaying this information, and relaying control commands to local or remote equipment [GAO, page 10]. In the chemical industry, PC is typically used to control chemical-making equipment and monitor sensors. If anything goes wrong, the PCS reacts by adjusting the environment in a predefined way, such as shutting off the flow of a chemical to prevent a leak or explosion [Schwarz].

A generation ago, PCS security was not the issue it has become today because a PCS was generally a proprietary system with no connection to other company information systems and certainly no connection to the Internet. It was accessible only from a console that was protected by strong physical security. The only people allowed at the console were qualified operators with specialized knowledge of the PCS [Haynes]. Due to the proprietary nature of the system, a malicious outsider let loose in the control room would have had a hard time discovering how to do serious damage [Williams, slide 12].

Unfortunately, this older security paradigm survives today, even though PCS technology has changed significantly. PCSs are increasingly connected to corporate LANs and the Internet, and becoming web-enabled [PCSCS]. They are built using standard components and technologies, including Microsoft Windows and Unix operating systems, TCP/IP, Ethernet, and Intel-based workstations. More importantly, PCSs are being connected to corporate business systems in order to support quality control, more timely information on production progress, and just-in-time production [Haynes]. The bulk of this paper deals with some of the security problems these changes have wrought.

PCS Integration with Traditional IT: Major Challenges

Most of the challenges presented in this section are a direct result of this recent transition of PCSs from proprietary to standard technology. The good news is that traditional IT can provide many of the security solutions needed to deal with these challenges. The bad news is that the industry needs to do a lot of catch-up work; critical infrastructure will remain at high risk until it makes significant progress.

Standard Vulnerabilities; Integration into Corporate IT and the Internet

As PCSs have evolved toward standardization, they have lost whatever "security through obscurity" they once possessed and are now subject to all the vulnerabilities and exploits facing mainstream IT. And as companies have increasingly connected individual PCSs as well as PC networks to standard corporate networks, with ever

increasing access to and from the public Internet, outside attackers are gaining a route into these systems that never existed before. Furthermore, process applications themselves are designed to be better able to utilize WANs and the Internet to share data among geographically separated sensors, controllers, processors, and monitoring stations. These developments are paralleling the web enabling of embedded systems in home control systems, household appliances, and entertainment systems; PCSs are, after all, largely based on embedded systems themselves [Monkman].

Antivirus and Other Security Updates vs. High Availability

Two problems PCSs pose for security patching are incompatibility of patches because of customization of standard software, and applying tested patches to high-availability systems. The main concerns are with OS security-related and antivirus updates, but database and other application software needs to be maintained as well. Even though PCSs often now use standard operating systems, the implementation may use custom settings that complicate the application of vendor-supplied patches, or even require rewriting the PCS to work with the patch. Antivirus updates can be next to impossible to apply on Windows and Linux systems due to PCS customization [Schwarz]. A further consideration is that PCSs have an exceptionally high reliance on software stability [Williams, slide 23].

The requirement that patches be tested before deployment complicates things further. First, PCS customization often leads to longer and more problem-prone testing. Second, companies often cannot afford separate test systems, so they must “test” the patches, if at all, directly on production machines. Third, testing on production machines, if not done while the PCS is out of service, will likely cause production problems that are unacceptable in the PCS environment. Fourth, shutting down these “always-on” systems is costly, so companies simply postpone testing and applying the patches [Schwarz].

Internet Access for Maintenance and Support

For the proprietary PCS, Internet access was rarely an option. With the modern PCS supporting Internet connectivity, organizations sometimes now leave dial-up modems on equipment to allow the vendor to conveniently perform diagnostics, maintenance, or system status checks. This access is too often not protected by adequate authentication or encryption, leaving the PCS vulnerable to hackers [GAO, page 15]. Remote access is also frequently provided to internal PCS specialists or operators, to free them up from spending all their time at the console waiting for the unexpected to happen [Williams, slide 16].

Password practices

Another area where PCSs have not made the transition to modern approaches is in password use. It is still common for users of a PCS to share a single password; too often, that password is easy to guess, infrequently changed, the default that came with the system, or nonexistent [GAO, page 12]. In the worst case, every machine of a particular type worldwide uses the same password, and everyone who has every worked on that type retains access to all such machines [Schwarz]. This lax password

practice developed from a concern that stronger passwords might interfere with rapid response to an emergency condition on the PCS. Also contributing is the historic downplaying of the importance of passwords based on the prevalence of strong physical security and the fact that only a small number of operators with specialized knowledge could really do any damage.

Lack of Standard Security Software

It may just be that PC is such a different paradigm from general-purpose computing that security processes and tools that work for one are a difficult fit for the other. PC's specialized, deterministic logic has enabled its creators to use chips and program code tightly matched to limited inputs, outputs, and processing. Low-cost, resource-constrained microprocessors are often used, including CPUs that are considered archaic or obsolete in general-purpose computing. As a result, PCSs often lack the bandwidth, processing power, and memory required for modern security technologies like authentication, encryption, and intrusion detection [GAO, page 12]. The market for these technologies, both original products and security updates, may be weak or nonexistent.

Separation between Corporate and Process Control IT Organizations

One overriding challenge is for organizations to close the gap that exists between their corporate IT and process control groups. Corporate IT focuses on, among many things, enterprise security. The PC group is primarily concerned with the reliable performance and physical safety of control systems. These different goals are reflected in a lack of both understanding and collaboration between the groups. As a result, organizations fail to take advantage of even those security technologies that can be implemented easily for "quick wins".

Security Recommendations to Meet the Challenges

Based on an emerging profile of the PCS as a system

- With a potential for catastrophe that demands strong security measures if it is to be exposed at all to the corporate network and the Internet;
- Increasingly making use of well-defined services on and exchanging data with other corporate systems;
- Requiring much more limited exchange of services and data with the public Internet, primarily for security and functionality updates from manufacturers and antivirus and other software vendors;
- Requiring both periodic and emergency access by outside specialists in order to perform maintenance and support;
- And without reserves of memory, storage, processing power, or bandwidth that are more likely to be available to a general-purpose system,

here are specific security recommendations to address each of the challenges previously described. These are best thought of as tactical responses to these challenges that would all be part of a broader security program.

Perimeter Defense

For systems and networks without plentiful resources to run internal security processes, perimeter defense is of primary importance. The organization's PCSs should be on their own network segment isolated by a switch from the rest of the private network. The private network itself should be protected by a firewall, configured to enforce an aggressive policy of denying all traffic except that which is explicitly allowed. A tightly configured border router between the firewall and the ISP is recommended for additional protection. At a minimum the router should have all unneeded services and protocols shut off, and all generic packet types with the potential for security exposures blocked, following the SANS Twenty Most Critical Internet Security Vulnerabilities [SANS] or a comparable guideline. Since the PCS will have both inbound and outbound traffic, one of these perimeter devices or an additional proxy server should provide network address translation to protect the actual IP addresses of the PC nodes.

If a risk assessment indicates that the protection of a PCS is exceptionally important, additional layers of defense should be added. A second firewall, of a different type or from a different vendor, can be deployed in series between the first one and the PCS network. This firewall would allow only inbound and outbound traffic that specifically supports PC and system support operations. Since any other inbound traffic is potentially hostile, the default Deny All stance is particularly important at this level. One chemical company, DuPont, as part of a major project to improve PC network security, concluded that each process system needed to be either totally isolated from business systems by keeping it physically disconnected, or well protected by a dedicated firewall [Schwarz].

Network Security Maintenance

A regular program of network security maintenance activities should complement the perimeter defense across the PC network:

- Periodic network mapping and port scanning of the PC network segment(s) to stay on top of everything that is connected to it and what services are available;
- Regular network sniffing to develop familiarity with legitimate traffic, which will help with the recognition of anomalies;
- Progressively more extensive vulnerability scanning to identify attack vectors missed by the firewalls and other defenses and then harden systems accordingly;
- Network-based intrusion detection to defend against outsider attacks that bypass or penetrate the perimeter. Network-based, rather than host-based, is a good place to start with intrusion detection, because it does not increase the load on the network or hosts, and therefore provides a better fit with resource-constrained PC.

Availability Protection; Change Management; Security and Antivirus Updates

The problem of the need for high availability preventing security and other updates from being tested and installed regularly needs to be addressed from several perspectives.

First, basic availability issues may need to be addressed. Networks may require redesign to incorporate both redundant servers and other critical components and failover mechanisms to prevent a single component failure from stopping an entire process. A business continuity and recovery plan must be created and tested in order to ensure that processes remain available following a natural disaster or other severe interruption that takes out an entire building or site.

Second, there is no substitute for having solid change management processes in place. If it is prohibitively expensive to have separate hardware for testing changes, then the organization might evaluate instead using a virtual test environment that offers a simulation of the controlled process. Perhaps more than with business systems, corporate policies need to be in place that allow for clearly defined emergency exceptions that would necessitate bypassing normal change management procedures.

Last, the importance of applying antivirus, OS, and other security updates must begin to outweigh other concerns. PCS customization will continue to present an obstacle to straightforward patching, but one that is increasingly offset by improvements in tools. There are now numerous sources of information on recommended security patches; standardized delivery of updates in service packs and hot fixes; tools to determine what updates are needed for a particular system state, and whether they have been applied; automatic notification of critical patches; and, for Windows OSs especially, automatic delivery systems. Despite this progress, some updates may still require reboots or limited downtime, and there may be a requirement for regularly scheduled maintenance windows.

Internet Access for Maintenance and Support

Modem access is not an acceptable solution. There should be no dial-in modem on the PCS network that can be used to establish a direct connection to an external ISP. It is advisable to conduct periodic network sweeps using a war dialer to make sure that there are no modems set to auto-answer. If there is an exceptional situation that absolutely requires modem access, the connection should be supervised and monitored.

Instead of modem access, both employees and vendors needing access for PCS maintenance and support should be provided with extranet access through the same VPN that is typically used for all remote access to corporate resources and systems. The VPN can enforce the same security policies for access control that apply to a connection directly on the network.

Access Control and Password Practices

Additional controls should be implemented to address the two parts to this problem: shared accounts and weak password practices. The rationalizations for both practices certainly had some merit when PCSs were more isolated, but that older model is out of step with modern connectivity and the associated risks.

Individual employees must have individual account access to PCSs in any organization that values and promotes individual accountability and compliance with policies and standards. If organizational policy supports monitoring and auditing of individual system access in order to promote security, performance, or other objectives, those efforts will be undermined by the inability to track activity by account.

Given the increased risk associated with attacks on PCSs, password practices for these systems should be, if anything, more stringent than for other types of systems. What is needed is an organizational policy that requires the creation of strong, hard-to-crack passwords; offers practical guidance on what employees are expected to do to protect their passwords; and mandates that employees change their passwords periodically and that system administrators enforce periodic updating. It may be advisable to step up from one-factor to two-factor authentication for PCSs, or from two-factor to three-factor.

Hardening PCSs by Turning Off Unneeded Services

As a partial response to the challenge presented by the lack of standard security software on PCSs, it has already been proposed that security organizations promote the acceptance and implementation to the greatest extent possible of perimeter defenses, network security maintenance activities, security updates, and stronger access control and authentication. These technologies, as valuable as they are, are still likely to run into obstacles and compromises in implementation based on the special-purpose limitations of PC.

It is possible, however, to turn these limitations into a security advantage by uninstalling or disabling all network and system services that, while useful in general computing, are completely unnecessary to PC, such as email or Internet browsing. It may not be too difficult to get corporate policies in place that recognize that the convenience of offering these services from a PC workstation, assuming they can be offered, is far outweighed by the security risk. Other services will probably be found that can be turned off without any convenience to anyone, once they are identified. In addition to stopping services from running on a PC server by either uninstalling or disabling them, it is important to configure the firewall protecting the PC network to filter out all unnecessary traffic by protocol. Turning off services by these means will also improve performance and reliability, results that are right in line with providing the best possible conditions for PC, given both its resource constraints and safety requirements.

Understanding and Teamwork between PC and the Rest of IT

PC engineers, operators, and the business users relying on these systems should all receive the security awareness training provided to the rest of the organization. In addition, the engineers and others responsible for managing PCSs should be given security technology training in order to get them speaking the same language and working toward solutions in partnership with corporate IT. Not only should PC personnel learn computer security; security experts will benefit from cross training on aspects of PC technology. Cross-assignments between the groups on projects and ongoing responsibilities can also be valuable to develop a shared understanding of issues and possible solutions. DuPont has learned, for example, in the course of its process

network security initiative, that the work demands the combination of the PC experts' knowledge of the complex relationships among control systems, the controlled processes, and the PC network, and the IT security experts' knowledge of general security processes and technologies [Schwarz].

Two other points of cooperation can be used to develop the relationship. Corporate IT and security needs to involve PC personnel in teams and steering committees that make decisions on policies and practices. And, finally, it is important to make sure that PC systems and networks are covered under, and that its engineers and IT support people are involved in creating the organization's business continuity and recovery plan. Working together on the plan provides a great opportunity for all to understand shared risks and how to mitigate them.

Developments To Come

Just as most of the challenges described in the paper are the result of a new "generation" of process control systems that arrived with many benefits but also many accompanying security problems, yet another generation, due in another 10 to 15 years, will no doubt solve most these problems and bring new ones that we cannot foresee.

The chemical industry cannot afford to wait for another generation. The initiatives industry groups are participating in are moving forward, and should start to yield tangible results in 2004. Although not published in time for inclusion in this discussion, the ISA-SP99 standard for Manufacturing and Control Systems Security has been issued in draft. It should be published early this year. It promises to offer authoritative guidance on the use of a broad range of security technologies and practices, and to raise the awareness in chemical companies of their need to invest more resources in securing process control.

The other initiative supported by the industry, the Process Control Security Requirements Forum, has an important longer-term objective of providing specifications that can be used to engage PC vendors to work on products that meet higher security requirements [Grant, slides 51-52]. Progress in this direction is important, but it is just as critical for organizations to do much more in the pursuit of process control security with the means already in their hands.

References

Please note: identifiers in [square brackets] at the head of each entry match citation identifiers used throughout the text.

[Chemical Cybersecurity]
_____. “Chemical Sector Cybersecurity Program.” Chemical Sector Cybersecurity Forum. 2003. URL: http://www.chemicalcybersecurity.com/ . (8 February 2004).

[GAO]
Dacey, Robert F. “Critical Infrastructure Protection: Challenges in Securing Control Systems.” United States General Accounting Office. GAO-04-140T. 1 October 2003. URL: http://www.gao.gov/new.items/d04140t.pdf .

[Grant]
Grant, Theresa. “CIDX Progress To-Date.” CIDX (Chemical Industry Data eXchange). 25 September 2003. URL: http://www.cidx.org/Meetings/pdfs/CIDXCSProgramtodate.pdf .

[Haynes]
Haynes, Tony. “Manufacturing Process Control Security.” NCMS (National Center for Manufacturing Sciences. July 2002. URL: http://trust.ncms.org/MfgTrust0702.htm .

[Monkman]
Monkman, Robert. “Enhancing Embedded Security. EDN Magazine/Reed Electronics Group. 17 October 2002. URL: http://www.reed-electronics.com/ednmag/article/CA250807?text=robert+monkman&stt=000 .

[PCSCS]
_____. “Today’s Business Environment Requires Attention to PCS Cyber Security.” PCSCS (Process Control Systems Cyber Security) Forum. URL: http://www.pcscs.org/intro_background.php. (8 February 2004).

[Prine]
Prine, Carl. “Chemical Sites Still Vulnerable.” Pittsburgh Tribune-Review. 16 November 2003. URL: http://www.pittsburghlive.com/x/tribune-review/specialreports/potentialfordisaster/s_165518.html .

[60 Minutes]
Kroft, Steve. “U.S. Plants: Open To Terrorists.” 60 Minutes/CBS News.17 November 2003. URL: http://www.cbsnews.com/stories/2003/11/13/60minutes/main583528.shtml .

[SANS]
_____. “The Twenty Most Critical Internet Security Vulnerabilities.” SANS. Version 4.0. 8 October 2003. URL: http://www.sans.org/top20/ .

[Schwarz]

Schwarz, Mathew. “Wanted: Security Tag Team.” Computerworld. 30 June 2003. URL: http://www.computerworld.com/printthis/2003/0,4814,82505,00.html .

[Williams]
Williams, David. “Security Process Control Systems – IT Security.” European Parliament, Brussels. 10 September 2003. URL: http://www.europarl.eu.int/workshop/itsecurity/pptpdf/williams.pdf .