What happens in plant stays in plant

The user experience. By using this site, you consent to the placement of these cookies. View the ISA Privacy Policy.

By May Permann, John Hammer, Ken Rohde, and Kathy Lee

While players in automation are becoming more aware computer systems are vulnerable to cyber attack, especially those controlling our nation's critical infrastructure, some don't always implement control system security procedures and devices consistently and effectively. In response, the Department of Homeland Security National Cyber Security Division established the Control Systems Security Center at the Idaho National Laboratory (INL) to help industry and government improve security in those control systems.

While significant differences between control system architectures permeate the industry, supervisory control and data acquisition (SCADA) systems, process control systems, and distributed control systems make up the general configurations. To remotely manipulate a control system, an attacker must gain access to the control system local area network (LAN), discover and understand the process, and then control the process.

Fortunately, most control system networks are no longer directly accessible from the Internet. It is becoming more of an industry practice to separate the business LAN from the control system LAN with some type of network isolation technology such as firewalls, which keep hackers out and isolate the LAN from worms and other maladies that may infect the corporate network. A firewall can also separate the control system network into sub-networks called demilitarized zones (DMZs) and control access between them.

Onsite assessment work provides an opportunity for cyber security professionals to meet with industry personnel to increase the security posture of a specific control system installation. Some security issues are unique to each implementation, yet there are commonalities among some of these installations.

When prioritizing security tasks, consider cost, probability, and consequence. Balance the risk of an intruder compromising your system with the risk of potentially degrading system operability. Above all, the control system must be reliable and perform its required mission. So build security into a system before putting it into production or adding security into an existing system in small increments. When adding security to a production system, test it on a backup system first to allow quick recovery to the previous configuration in the event any security measure affects system operation.

Effective security policies and procedures are the first step to a secure control system network. It is possible to apply some of the same policies used for information technology security for corporate systems directly to control system networks. The SANS Institute provides free templates for security policies and can be a valuable resource for control system network administrators in developing their own policies.

Security policies must be practical and enforceable. To ensure they do not impact productivity, are not cost prohibitive, and do not lack support, include management and system administrator personnel. Network and system administrators have the technical knowledge but also need authorization and support from management to implement the policy.

In several cases those in charge of the control system network do not have adequate security training, usually because of insufficient funding or appreciation for its importance. Training provides an understanding of a network architecture's security implications and how to design a more secure network. Network administrators require constant retraining to keep them up to date with the fast-paced changes of the network security field, including the latest network architecture designs and firewall and intrusion detection system (IDS) configurations.

Since new techniques are constantly under development to attack and defend computer networks, everyone should go through training to protect against e-mail attacks. If formal training is cost prohibitive, you can get some of this information from books, papers, and Web sites.

The INL onsite system assessments identified cases in which network administrators are competent at designing and maintaining reliable networks, but do not understand the security implications of their designs. Some examples are networks with redundant firewalls, IDSs, backup system networks, and DMZs for non-control system critical computers. At first glance, these appeared to be secure configurations, but a closer look revealed direct connections from the DMZ to the control system network circumventing the firewall, incomplete firewall rules, and non-validated IDS signatures.

Password policies

Sometimes operators need to share IDs and passwords because of critical system operations. Unacceptable consequences might occur because of a locked user ID or a forgotten password. Typical continual manning of operating consoles provides additional physical security that reduces the need for distinct operator user IDs and passwords.

Don't leave the default password from the manufacturer on your control system and networking equipment because they can give an attacker easy access to the equipment that controls the process. Unless your control system software requires it, always change default passwords to robust, unpublished passwords. Implement a password policy that enforces strong passwords to greatly impede password cracking and guessing. The SANS Institute's password policy provides guidance on creating, protecting, and changing passwords.

Some have found passwords in control rooms on small pieces of paper on the bottom of the keyboard and in a drawer. If a password is too complicated and difficult to remember, or changes too often, users will undermine their security in order to remember them. Complex passwords protect against some of the advanced password cracking attacks, but they create a physical and social engineering vulnerability an attacker could exploit. Never use an auto-generated password, but create one from pass phrases or other memorable means.

Response procedures, patches

Incident response procedures tell employees what steps to take if a hacker compromises a computer on the network. They ask questions regarding what indications are present that an incident has occurred or is in progress, what immediate actions you should take, whom you should notify and in what order, how you should preserve forensic evidence (if you should leave the computer on), and how you can restore affected computers. The National Institute of Standards and Technology has developed a Computer Security Incident Handling Guide...
that provides guidance to security personnel in developing an incident response procedure.

Operating system patches repair vulnerabilities that could allow an attacker to exploit the computer, but unique challenges to consider include system functionality, security benefit, and timeliness. For security, download patches to a trusted server off the control network, and burn them to a CD. Then use the CD to patch the machines on the network. Other methods of patching could include the same process, but instead of loading each computer separately with the patch, the administrator could feed the new patch into a patch management server on a secure DMZ.

The system vendor should test operating system patches for compatibility with their system and supply the testing results to users. Make the results available as soon as possible after the patch release to limit the length of time the user's system is vulnerable to the exploit. Always test patches on a backup system first, before implementing them on a production system. This testing period should be long enough and include full operational evolutions to make any side effects apparent. Cases exist in which the vendor tested and approved the patch, but at installation, it rendered the control system inoperable. Therefore, even if the vendor tests patches and updates, they should test them on the backup or test system as well.

Some control systems are still vulnerable to exploits that have had patches available for a long time. A widely available tool could exploit a system not patched for the overflow vulnerability, thus compromising the system. This particular exploit would allow complete graphical remote control of the system because the attacker has control of the HMI.

Applications, services

Services or applications running on a system open up different network ports to be able to communicate to the outside world. Each open port provides a possible access path for an attacker that can send exploits and receive data. An attacker can only gain access to, and receive information from, the control system through an open port. The more ports and services accessible, the greater risk of successful exploits due to service vulnerabilities.

New vulnerabilities appear everyday in computer applications and services, some of which see publication shortly after discovery. Yet some stay a close secret, allowing a few hackers to exploit computers at will, with no patches available to stop them. Decreasing the number of installed applications and services decreases the likelihood of an attacker finding vulnerability on the computer. Remove all unneeded applications and services. Allocate adequate resources to ensure complete patching of all services and applications is up to date using the patches process.

Privileges

A common problem with applications and services is they run with system or root level privileges. In this case, an attacker can cause the application to crash; the exploit code will run with those same privileges, giving him full access to that device. A number of software products run with these super-user permissions by default, and yet, will function running as a less privileged user. You should therefore lower permission levels of applications and services only to what is necessary for their required functions. Another common problem is allowing users to operate a computer system (consoles, servers, and the like) with more permissions than necessary. Carefully evaluate user accounts for interactive logon for the lowest set of permissions necessary.

A related issue is file permissions. Share files with only the computers and accounts that require them. Restrict the read and write permissions to these shared files and directories to the minimum required for each user. Give each user and process the minimal privileges necessary for system operation. This is an emerging practice in the IT world that you can bring over to the control system domain as well.

Cases also exist in which users need to restrict file access permissions to prevent information gathering. In our assessments, we discovered systems with information and vendor code shared to all computers on the control system LAN. In one example, even though the control system network was segmented, an intruder gaining access to the network would have access to all control system-specific information. In another case, a corporation housed the critical control system diagrams and documentation on an anonymous file transfer protocol (FTP) server for engineers' easy use. They could view this FTP server from the Internet, making all the data accessible to anyone seeking the information.

Security perimeter defense

We consider any connection into the control system LAN part of the perimeter. Often users don't document these perimeters well and neglect some connections. You should know all entry points into the control system LAN, and your security policy should strictly manage them. Most common entry points include vendor access, typically through a virtual private network (VPN) connection or by dialup modem. A corporate LAN connection is connected to the Internet, so it has the most potential for giving an attacker access to the control system LAN. Routinely check for unauthorized connections such as modems and direct cables to give operators remote access to the control system.

Know where the communication lines go for your control system. Only access the vendor VPN when you need it, and then immediately unplug it.

About the Authors

John Hammer, May Permann, and Ken Rohde are computer security researchers at Idaho National Laboratory (INL) in Idaho Falls, Idaho. Kathy Lee is a SCADA security researcher at INL.
SCADA security not just talk

By Ellen Fussell Policastro

With all the talk about security and how plants need to pay more attention to their control systems, who's doing what to ease concerns and keep control systems secure? Homeland Security is pushing for security awareness for infrastructure companies and governmental agencies, said Bill Drake, Frontline Test Equipment director of operations in Charlottesville, Va. Concerns center around attacks disrupting city water departments, oil pipelines, and rail lines. "The private and public sector infrastructures have to be aware they're vulnerable, not only from terrorist attacks, but hackers and disgruntled employees," he said.

It starts with the easy things where people simply start implementing passwords, so disgruntled employees have their passwords disabled. Other network structures include firewalls and virus scans. "It's not terribly new, but by raising the awareness, it's got people paying more attention," he said. "Sometimes a password structure is enabled, but when we tested it, we found people left their password as 'password.' So we're raising those levels of awareness."

To maintain the sewage pump stations at the Clark County Water Reclamation District (CCWRD) in Las Vegas, Nev., Mark Binney and his team use a graphical user interface or human machine interface (HMI) to check remote sites, which are up to 75 miles away, in under five minutes. When checking for flow or pump runs, Binney's team can see historical trends, how the site has run through the night or the past few weeks. With the trending and historical data, "if there's a problem, you can adjust level, pump on, pump off, and which pump runs. And you know more about the activities of the site from HMI than you do actually standing in the site."

Physical security strong

Another important aspect in securing your control system involves complicating access to physical facilities, Drake said. "A junction panel on the edge of a property has a padlock on it when it did not used to. Or a cable going up the side of a tank is enclosed in a conduit. Those kinds of things make it much harder for physical access," he said.

Ray Gonzales, telecommunications manager at Long Beach Water District handles SCADA, telephone systems, microwave connections, mobile communications, and audiovisual equipment. While Gonzales agrees the most important thing with SCADA control is security, he's more concerned with keeping viruses out than hackers because "it's the viruses that wipe out your computer," he said. "If someone really wanted to do the homework on your facility and figure out the application to talk with your machine, they would need to do a lot of research."

The security program Gonzales set up is not connected to the Internet or an intranet, so it is isolated. Computers are connected together through two highways disconnected from the outside world. Computers locked in cabinets run in limited mode, so there are no administrative rights to change things.

Encryption still viable tool

One important security move is to make encryption used on actual transmission of data to make it more difficult to figure out or to inject a message that would spoof something, Drake said. While some plants are doing this, others aren't, he said. And there are a variety of ways to attack wireless systems. A spoof, the most feared attack, involves the man in the middle, "where a person who's trying to disrupt your system creates a system that can emulate both ends of a wireless link," Drake said. Spoofing is successfully injecting a message that's not a correct message, but having the receiver think it's a correct message.

If a signal is sent into a system that's controlling a pump station that says, 'the tank you're filling is empty, turn on all your pumps,' you could explode a pipeline because of overpressure, or overflow a tank, or use up extra power. That doesn't hurt anyone. But what if that happens with a natural gas pipeline, oil pipeline, or rail line? It did happen a couple of summers ago, when a wrong message from a circuit breaker shut down the Northeast U.S. power grid."

About the author

Ellen Fussell Policastro is the associate editor of InTech. Her e-mail is efussellpolicastro@isa.org.

Standardization key to changes

What's precluding plants from being more vigilant about security?

"There's an industry wide lack of standardization, so the solutions tend to be proprietary, and that makes suppliers nervous" said Bill Drake, Frontline Test Equipment director of operations in Charlottesville, Va. The ISA-SP99 committee is trying to work out standards so equipment from different manufacturers will have interoperability and testable safeguards against attack.

Industry standards are a major factor in securing control systems because they provide a common architecture, language, and approach. Plus, they give people a basis for what to accept, said Joe Weiss, executive consultant at KEMA in Cupertino, Calif. (See "Paranoia prevails," in the September 2005 InTech, www.isa.org/link/Paranoia05.)

ISA-SP99 addresses manufacturing and control systems whose compromise could result in endangerment of public or employee safety, loss of public confidence, violation of regulatory requirements, loss of proprietary or confidential information, economic loss, and impact on national security.


Other standards bodies, such as the North American Electric Reliability Council (NERC), are still working on control system security education and standardization. The Department of Energy's "21 Steps to Improve Cyber Security of SCADA Networks" offers some guidance, and the NERC Control System Security Working Group (CSSWG) is working on more detailed guidance from the document.

As Weiss explained in the December 2006 InTech "Power to Security Standards" article www.isa.org/link/Security1206, the CSSWG is working on a Control System Patch Management Guideline and a Control System Electronic Connectivity Guideline for the secure connectivity between control system networks and business networks.
Plants need nutrients from the soil, water, and light from the sun to grow and stay alive. If plants did not get water, they would die. How much water each plant needs depends on what plant it is. Something like a cactus or a plant in the desert does not require as much water as a plant which grows in the rainforest. The two main things plants need water for are turgor, to keep the upright and make sure it doesn’t wilt and for photosynthesis. Answer 3 I found a scientific paper that says we are just starting to understand what happens to plants when they get dry, before they die. When plants are making seeds, the last stage is for the seeds to lose lots of water. That’s good for the seeds, because they would get moldy if they were too wet. The seeds can stay very dry for a long time without dying. Answer 4 Plants also can affect how nearby companions grow, as roots tangle and compete for the same resources of water and nutrients in the soil. Planting too close together limits the growth potential and often threatens plant health. Video of the Day. Spacing. The amount of spacing around a plant -- both soil and air -- is proportional to the plant’s size. Seedlings are grown in small containers in denser numbers than larger plants in bigger pots, such as tree saplings. Physical Effects. Plants that grow too close to each other compete for the same sunlight, water and soil nutrients. The first effect seen is competition for light. Crowded plants begin to grow upward to receive light, rather than developing a fuller, bushier silhouette.

RESOURCES
Security on a Roll
http://www.isa.org/intech/blog/2006/11/security-on-roll.html

ABCs of Industrial Network Security
www.isa.org/link/ABCs

ISA-SP99, Manufacturing and Control Systems Security
www.isa.org/link/ISA-SP99

Fast Forward
- Control system security is important, but inconsistencies still exist in implementation, Idaho National Lab study finds.
- Training, password policies, and privileges among problems.
- Building security into design, mitigation programs are keys to secure plants.

The International Society of Automation
67 T.W. Alexander Drive
PO Box 12277
Research Triangle Park, NC 27709
E-Mail: info@isa.org
Phone: (919) 549-8411
Fax: (919) 549-8288

Join ISA Now

The Industrial Internet of Things, Digitalization & the Future Of Business. The technology that powers an organization. https://t.co/VN3INOxDE6