Security of Critical Control Systems Sparks Concern

David Geer

For about 50 years, sophisticated industrial control systems have kept major infrastructure, manufacturing, and utilities operations in check. These systems gauge and adjust factors such as temperature, electrical current, pressure, and flow rate to keep dams, factories, nuclear power plants, and other similar facilities functioning properly and safely.

Control systems are growing in popularity. For example, as Figure 1 shows, global revenue from sales of the systems will grow from $10.3 billion in 2000 to $12.4 billion this year to $13.9 billion in 2009, predicted Datamonitor, a market research firm.

"Control systems are being adopted at an increasing rate around the globe. Every country has infrastructures and industry that need these devices," noted Michael J. Skroch, manager of the Information Operations Red Teaming and Assessments Department at the US's Sandia National Laboratories.

Securing control systems has become a much more serious issue since the advent of the Internet and the rise in terrorist threats. Today, many government and private operations have connected their controls to the Internet through unhardened operating systems.

Internet connectivity can make control operations more convenient, but it also can leave the systems vulnerable to the same hackers, malware, and attacks that threaten other online activities. Several attacks on Internet-based control systems have already occurred.

The issue is so serious that the US House of Representatives Committee on Homeland Security recently heard testimony from experts in the fields of security and control systems in an effort to identify vulnerabilities and determine whether federal and private organizations are addressing them adequately.

Fred Cohen, a research professor at the University of New Haven, said a principal problem is that exposing critical control systems to the Internet and its dangers is simply a bad idea. He said those responsible lack control-system expertise and "are anxious to make a change just for the sake of making a change or because of some perceived cost reduction."

Larry Todd, director of security, safety, and law enforcement for the US Bureau of Reclamation, agreed in his testimony before the congressional hearing. "We have maintained a policy of not connecting our [control] systems to our administrative networks," he said, "and we adhere to that policy in all but the most unusual of situations."

Nevertheless, organizations are continuing to connect their control systems to insecure networks such as the Internet. Therefore, government and private groups throughout the world are trying to determine how to make such connections more secure.

VULNERABLE CONTROL SYSTEMS

During the past 40 years, organizations have upgraded most manually operated, stand-alone control systems to computer-run systems, with many connecting them to the Internet since the early 1990s.

The newer control systems are basically computers with sensors, actuators, and software, noted Sandia's Skroch.

"These systems have taken the place of control rooms with people watching lots of dials, turning valves, and sliding actuator switches to keep things within a normal range or deal with exceptional conditions. When those can be replaced with simple, computer-controlled actuators, it reduces the manpower and costs and very often allows for faster responses," said Purdue University professor Eugene Spafford.

There are two major types of computer-run control systems: Supervisory control and data acquisition (SCADA) systems are generally used with utility and other infrastructure operations, while process-control systems (PCSs) are typically used in production facilities.

SCADA sensors gather data in real time from remote locations and feed it to a computer running special software. The computer processes the data in a timely manner, records and logs all events, and sounds an alarm when conditions become hazardous.

Published by the IEEE Computer Society

The technology is used in power plants; oil and gas refineries; and telecommunications, transportation, water, and waste-control facilities.

According to Cohen, PCSs typically use sensors to track specific factors such as temperatures and the volumes and levels of liquids and gases in a system. The systems then analyze those values against a model of proper behavior and issue signals to actuators that induce the desired physical changes, he explained.

PCSs can handle more complex environmental measurements than SCADA systems, process more complicated calculations, and make decisions and issue commands to control more types of devices, said Skroch.

Because of their connections to the Internet and other networks, newer control systems have become as vulnerable as other connected systems, as Figure 2 shows.

According to Skroch, most dedicated SCADA and PCS applications have not included built-in security features and at most have used only passwords or physical keys to prevent unauthorized access, which doesn't provide adequate protection.

In addition, he said, SCADA and PCS systems are often assembled

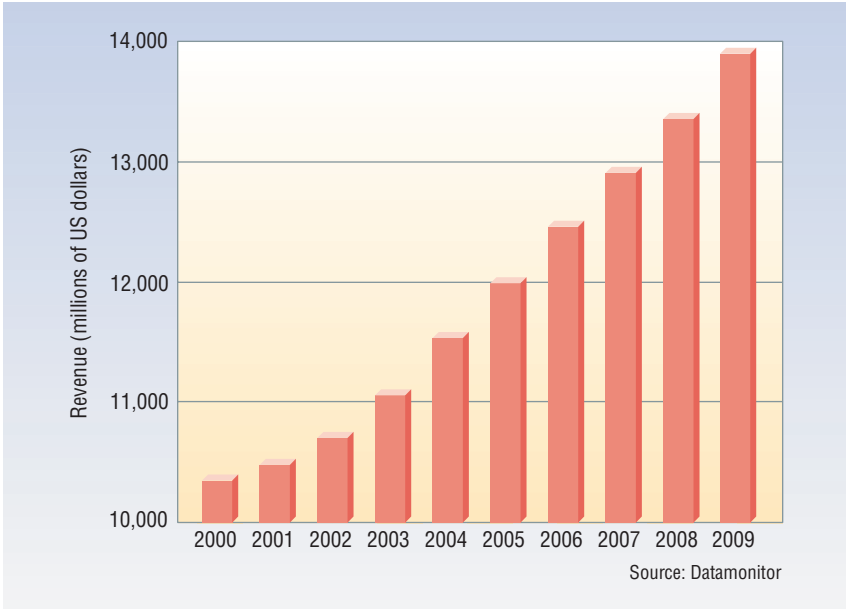

Figure 1. Datamonitor, a market research firm, predicts revenue from the sales of the increasingly popular control systems will grow between 3.5 and 4 percent per year through 2009.

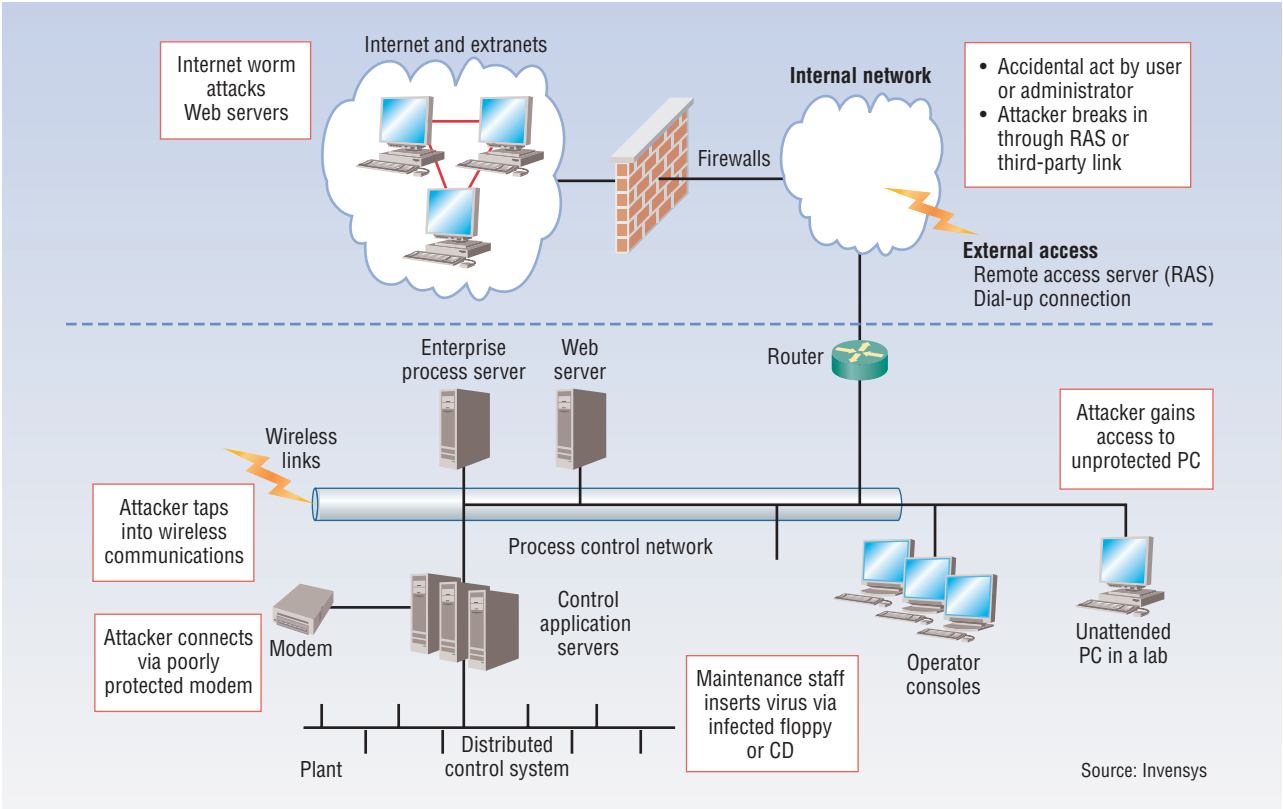

Figure 2. Industrial control systems connected to the Internet or private networks, like those used in factories and nuclear power plants, face a number of threats that could cause serious safety problems. This has prompted concern about the systems' security.

from numerous vendors' devices, components, and communications services. However, the companies responsible for integrating these elements often don't design system security holistically.

Moreover, explained Alan Paller, director of research at the SANS Institute, a computer- and communications-security training and information organization, "The people who adopted these systems aren't security experts, so they didn't know they needed to harden them."

PAST ATTACKS

Viruses and worms often attack control systems via vulnerabilities in host operating systems. The malware may either write data to the hard disc that makes the drive crash, or it may make multiple server requests, tying up the control system's server in a denial-of-service attack. In DoS attacks, hackers send large amounts of useless data to a system, keeping it so busy it cannot handle normal functions.

Hackers not knowledgeable about control systems could use such techniques to mount the same types of attacks they would launch against any computer, noted Skroch.

However, he said, experienced attackers could launch better targeted, well-timed assaults that cause more significant problems.

The January 2003 Slammer worm struck the computerized safety monitoring system at the Davis-Besse nuclear power plant in the US, which was shut down for repairs at the time, noted Donald Purdy, acting director of the US Department of Homeland Security's National Cyber Security Division.

The worm's scanning activities caused congestion that slowed down the plant's network, eventually crashing the safety-parameter display system, which monitors the most important safety indicators.

"The managers had considered the plant secure because the outside network connection was protected by a firewall," Purdy explained. "But the worm entered the plant network via a contractor's infected computer connected by telephone directly to the plant's network, thereby bypassing the firewall." As with every other successful Slammer worm attack, he noted, the victimized system had unpatched holes.

An attacker using a computer and radio transmitter remotely hacked an Australian sewage treatment plant's SCADA system in March 2000, altered data, and changed valve settings, causing sewage to back up into the city of Maroochy Shire, Queensland.

Security is becoming an increasingly important issue for control systems.

In the early 1990s, a hacker broke into several US government systems, including a Department of the Interior network in Portland, Oregon, and eventually gained root access over the computers that controlled every dam in Northern California. However, the attacker caused no damage.

In 2003, two hackers, in an alleged extortion plot, gained access to control technology for the US's Amundsen-Scott South Pole Station, which ran life-support technology for 50 scientists there.

Noted the SANS Institute's Paller, "We will never know about most of the break-ins because the victims will not tell the public."

PROTECTING CONTROL SYSTEMS

Older control systems were not connected to the Internet. Their chief vulnerability was telephonic access designed to let third-party vendors work with the software as needed.

Attackers had to be familiar with older systems to exploit access they gained, said Sam Varnado, director of Sandia's Information Operations Center. Simply breaking in wasn't enough.

This is not the case with Internet-based systems.

"Now," Varnado noted, "you have people who can hurt you who are not control-system engineers. All it requires is that you know how to hack computers." Once a hacker gains access, the simple application of generic computer attacks can cause problems, he explained.

The best first steps for securing control systems are becoming more aware of both their vulnerabilities and the potential solutions, as well as implementing stronger safety policies and procedures, said Ernest A. Rakaczky, director of control system security for Invensys Process Systems, a vendor of products and services for the automation of industrial-plant operations.

The Department of Homeland Security's Purdy said federal officials "are trying to make it easier to understand the business case for taking steps to help create a security framework against which they can do a risk assessment of their systems."

According to Paller, control-system users should apply the same measures they use with other systems to block unauthorized access. These include techniques like authentication, implemented via measures such as usernames, passwords, and personal identification numbers; and identification, implemented via approaches such as digital tokens.

And, said Sandia's Skroch, organizations can harden operating systems by removing services or features not necessary for control-system operation, properly implementing security settings, and immediately downloading available patches.

Paller noted that many users haven't hardened their OSs, even though the US National Security Agency and Defense Information Systems Agency, the nonprofit Center for Internet Security, and other organizations have published guidelines for doing so.

Users can also implement firewalls and intrusion-prevention systems,

which can block or even short-circuit attacks.

In addition, organizations can encrypt communications between control systems and the outside world. These communications, which can include transmissions of authentication codes, could help a hacker figure out how to break into a system.

In some cases, users can exploit their purchasing power, as the US Air Force did when it bought hundreds of thousands of Microsoft Windows systems on the condition that the company harden them first.

CHALLENGES TO PROTECTING CONTROL SYSTEMS

"I'm worried about our use of commercial off-the-shelf products in secure systems," said Sandia's Varnado. "Some of the software programs on computers today have 20 million lines of code. We can't even get in there to see what the bits and bytes are doing. We're trying to build trusted systems out of untrusted components."

According to Purdue's Spafford, users are likely to resist taking measures that would require expensive retrofitting of existing systems.

Added Sandia's Skroch, "Control systems have not been secured because the benefit of doing so has not been demonstrated sufficiently to the industries that develop or purchase them. Fortunately, this situation seems to be changing. We can only hope improved security comes in time."

Many experts are pushing established approaches to securing control systems, such as the US Department of Energy's "21 Steps to Improve Cyber Security of SCADA Networks" (www.ea.doe.gov/pdfs/21stepsbooklet.pdf) and the US National Institute of Standards and Technology's "Security Configuration Checklists Repository" (http://checklists.nist.gov/repository/category.html).

That way, Varnado explained, users would know how the approaches work and how they should be configured. However, he noted, hackers would also know these things and could use them to try to exploit vulnerabilities.

In addition, Paller said, hardening OSs could close network access to systems that some control applications require to function properly.

Improperly implemented security could also fail by making control systems difficult to use. For example, Skroch explained, "If designers of security make it hard for authorized employees to perform their jobs, the security will likely be circumvented by the ultimate insider: the employee."

Control systems could face dangerous new threats in the future. For example, Paller said, terrorists, extortionists, or other malicious hackers could install Trojans on computers inside utilities and receive information that could help them threaten control systems. Criminals could also aggregate these Trojans, as they do for distributed DoS attacks or spyware installation, and sell them to people who want to disrupt operations, he added.

With such threats in the offing, said Invensys' Rakaczky, "the big success will be for [users] to just adopt something." Many users have no security but spend time worrying about what ideal approach they could adopt when there are effective interim steps they could take now, he explained.

In general, concluded Purdue's Spafford, "Control system security is going to be increasingly important because we are deploying more complex systems over greater distances."

David Geer is a freelance technology writer based in Ashtabula, Ohio. Contact him at david@geercom.com.

Editor: Lee Garber, Computer, l.garber@computer.org