

SP99

counterattacks



Standard is taking a more precise look at the security requirements for control systems.

BY ERIC BYRES, RON DERYNCK, AND NICHOLAS SHEBLE

Why not just apply the already developed practices and technologies from information technology security to plant floor security?

Indeed.

Wouldn't that be enough to protect these industrial-strength information and control systems?

No, not without some fine-tuning.

Process engineers hesitate to blindly employ information technology (IT) practices, because they sense that some practices don't mix well with the plant floor environment.

They're correct, for four very good reasons.

First of all, the goals of IT are different from those of process control. The IT world sees performance and data integrity as paramount, while the industrial world sees human and plant safety as its primary responsibility.

These differences in goals mean huge differences in acceptable security practice.

For example, using standard password lockout procedures just isn't acceptable for most human-machine interface (HMI) stations—the default needs to let the operator in, not lock him out, which is the opposite of the IT assumption.

Imagine the immediate future of the security manager when, during a reactor meltdown, the operator panicked and misspelled his password three times, causing the HMI to lock out all access for the next ten minutes.

Second, the assumptions regarding what to protect on the IT network and process control network are different. In the IT world, the primary focus is to protect the central server and not the edge client.

In process control, the edge device is far more important than a central host. Thus, standard architecture of commercial network security—the firewall protecting the server—may not be appropriate for industrial applications.

Unless we put a firewall in front of every controller, our most important assets are largely undefended.

Clearly industry needs some economical technology that gives us the protection of firewalls while being widely distributed to protect our critical edge devices.

It is worth noting that this server-centric security mentality permeates many of the IT communications documents, such as the wireless Ethernet standard, IEEE 802.11 (Institute of Electrical and Electronics Engineers standard).

In the current version of this standard, the authentication procedures validate only that the workstation signing into the central access point is the authorized device. The access point never has to prove it is valid and authorized to the edge device.

This protects the central access point from rogue workstations signing on to the system,

but it certainly does not stop rogue access points from fooling workstations into joining the wrong network.

Maybe the IT world considers workstations expendable, but a programmable logic controller (PLC) on the edge of a wireless network is not.

Third, many processes require real-time performance and continuous operation that is rare in IT applications.

The process control industry needs to evaluate the performance impacts and trade-offs of using many information security technologies before they deploy in industrial real-time control systems.

Finally, the nature of process control systems, with their reliance on unusual operating systems and applications, means that many of the software-based security solutions will not run, or if they do run, they will interfere with the process systems.

A case in point, when an emergency shutdown system on a boiler failed to operate correctly, investigators discovered antivirus software installed on the computer used to configure the safety system. That software *blocked* the correct operation of the safety system.

MORE SPECIFIC TECHNOLOGIES

With the Twin Towers, the Taliban, and homeland security freshly in mind, ISA-SP99 held its first meeting in October 2002 at the ISA Expo in Chicago.

Now, in October 2003, the committee is releasing a first technical report on security technologies. The working group (WG1) has compiled a list of six general classes of security technologies and 27 more specific technologies.

As WG1 looks at these technologies, they address seven subsections for each of the aforementioned 27 technologies.

The seven subsections are:

- security vulnerabilities addressed by this technology
- typical deployment
- known issues and weaknesses
- assessment of use in manufacturing and control system environment
- future directions
- recommendations and guidance
- references

Here, *InTech* presents a version of the just-released ISA-SP99 technical report one (TR1) section on dedicated firewalls—one of the 27 technologies that TR1 covers.

NOT TRANSPARENT TO END USERS

A firewall is a mechanism used to control access to and from a network and protect attached computers from unauthorized uses.

Firewalls enforce access control policies using mechanisms that either block or permit certain types of traffic, thus regulating the flow of information.

Firewalls block traffic from the outside of a protected area to the inside of a protected area, while typically permitting users on the inside to communicate freely with outside services.

However, more restrictive policies are also possible and likely to be appropriate in a manufacturing and control systems context.

“A lot of people want to get things moving quickly. So that’s pretty encouraging. People want to make sure we cover their areas: SCADA, DCS, PLC, HMI, and of course control systems.”

—Bryan Singer, chairman
ISA-SP99, Manufacturing and Control Systems Security

There are three general classes of firewalls:

Packet filtering: This type of firewall compares header information—IP addresses, TCP port numbers—in each packet of data to a set of criteria before forwarding the packet. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator.

The advantages of a packet filtering firewall include low cost and low impact on network performance, because it usually only examines the source address in the packet.

For example, the firewall identifies each packet’s source address. Then an established rule determines if the system should discard or forward the packet. Some call this method *static filtering*.

Stateful inspection: These firewalls filter packets at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the application layer.

Stateful inspection keeps track of active sessions and uses that information to

determine if packets should go forward or not. These firewalls offer a high level of security, good performance, and transparency to end users, but are expensive.

Due to their complex nature, they can be less secure than simpler types of firewalls unless a highly trained person administers them. Some refer to this method as *dynamic packet filtering*.

Application proxy: This class of firewalls examines packets at the application layer and filters traffic based on specific application rules, such as specified applications (like browsers) or protocols (like file transfer protocol).

They offer a high level of security, but have a significant impact on network performance. They are not transparent to end users and require manual configuration of each client computer.

THE OUTSIDE WORLD INCLUDES

A firewall serves the same purpose on your network as a guarded gate does for your site’s physical premises. It protects a computer or network of computers from unauthenticated use by people from the *outside* world.

For the manufacturing and control system environment, the outside world typically includes corporate local-area network (LAN) users who do not have authorization to operate control center equipment.

Firewalls can:

- control access into a protected network
- control access to specific devices in the protected network
- prevent undesirable packets from entering a protected network
- hide hosts so they are not visible outside the protected network segment
- control outgoing traffic to the unsecured network
- record information useful for traffic monitoring and intrusion detection

Dedicated firewalls typically act as a gateway by splitting a network into a trusted—protected—side and an unprotected side.

This type of firewall acts as a perimeter defense device that provides a single *choke point* where you can apply access control policies and monitor network traffic.

Firewalls usually also perform important logging and auditing functions by providing summaries of the kinds and amounts of traffic passing through and the number of break-in attempts.

A standard is born

The ISA-SP99 committee is addressing manufacturing and control systems that if compromised could result in any or all of the following situations:

- endangerment of public or employee safety
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on national security

The concept of manufacturing and control systems' electronic security applies in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries.

- Manufacturing and control systems include, but are not limited to, hardware and software systems such as distributed control systems, PLCs, SCADA, networked electronic sensing, and monitoring and diagnostic systems.
- Associated internal, human, network, or machine interfaces provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Physical security is an important component in the overall integrity of any control system environment, but it is not specifically addressed in this series of documents.

ALLOW TROJANS TO TUNNEL

Firewalls do not protect the network and workstations against most data-driven attacks—viruses or attacks in which malicious code is mailed or copied to an internal host, where it is then executed—some denial-of-service attacks, social engineering attacks, and malicious insiders.

They cannot protect against attacks that do not go through the firewall, dial-up access via modems for instance. Nor can they prevent tunneling over application protocols to infected or poorly written clients—tunneling over hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and other protocols.

Properly configured firewalls are nearly impenetrable. However, a dedicated firewall can be the single point of attack to a network. With skill, hackers may be able to:

- identify the firewall type through port scans or banner grabbing
- determine the access control list rules through scanning
- scan downstream hosts using allowed source ports (stateless firewalls only)
- allow Trojans to tunnel out using allowed ports or Internet message control protocol (ICMP) services

Firewalls often come across as some kind of panacea, potentially providing a false sense of security when they should be looked at as one part of a larger network security approach.

Firewall deployment does not remove the need to implement software controls on internal networks or proper host security on servers.

Firewalls won't help if you do not understand the kind of access you want to allow or deny. Developing effective access control rules is a complex process that typically requires trained personnel who specialize in network security issues.

LIMIT HIGH-RISK E-MAIL

In a manufacturing and control system environment, firewalls are most often deployed

between the process control networks (PCNs) and the corporate LAN.

Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security.

They can also potentially improve PCN responsiveness by removing nonessential traffic from the network.

Although firewalls cannot protect a network against some types of data-driven attacks, they can control which workstations (sources of data) will have the liberty to pass through the firewall.

Firewalls can block services and ports that are favorite transport vehicles for malicious code.

When designed, configured, and maintained properly, dedicated hardware firewalls can contribute significantly to increasing the security of today's manufacturing and control system environments.

Firewalls provide several tools to enforce a security policy that cannot be accomplished locally on the present set of available process control devices, including the ability to:

Block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected manufacturing and control system

“Over the last six months I have moved away from the camp that believes we have to throw out all the IT security technologies and start from scratch.

“Instead we need to really understand how we differ from the average IT environment—not just utter general statements like, ‘Control systems are real time,’—and then borrow and modify the IT security technologies to fit our world.

“We did a great job of modifying the underlying communication technologies. Look at all the industrial Ethernet cable, connectors, and switching hardware on the market today. Now we need to do the same with the firewalls, VPNs, and the rest.

“That is really what I think this SP99 working group technical report document does. It says, ‘Here are all the wonderful IT security technologies available and where they might give the plant floor engineer both hope and grief. Now we have to fix the grief part—and be careful with this stuff until we do!’”

—Eric Byres, chair of the security technologies working group, WG1 of ISA-SP99