THE LINE

Sound security strategy, whether military, physical, or cyber security, is the concept of "Defense in Depth"—firewalls don't fail me now

By Eric Byres

It is November 1918, World War I, the greatest war the world has ever seen, has just ended, and France is reeling from the devastation.

The conflict has killed over one million French citizens, wounded a further four million, and destroyed much of the countryside of eastern France. A fierce debate begins to rage—"how should France ensure that another invasion of their beautiful country by the German hordes never occurs again?"

While there are a number of opposing ideas on how to achieve this, the one that carries the day is to build a defensive line of fortresses along the border with Germany.

Therefore, between 1930 and 1936, the French government pours approximately three billion francs into building 400 miles of fixed concrete fortifications known as the Maginot Line.

Everyone in France now can feel secure knowing their country is safe behind the massive barrier of concrete and guns.

Then on 10 May 1940, Hitler attacks France. While German decoys sit opposite the Line, Hitler's second Army Group cuts through Belgium, the Netherlands, and the undefended Ardennes Forest. These troops completely bypass the Line, and within a week, Nazi troops are deep inside France. A month-and-half later, France surrenders. The Line is hardly involved in the defense of France.

What went wrong? The Line certainly achieved its intended task, preventing a direct assault against France's eastern border.

However, France's strategic use of the Line was poor. The Maginot Line was only part of what should have been a multilayered plan, involving other defense systems and the French Army.

Same mistake: 75 years later

Today sound security strategy, regardless of whether it is military, physical, or cyber security, leverages the concept of "Defense in Depth."

Effective security comes by layering multiple security solutions, so if the one fails, another takes up the torch of defense.

Conversely, basing a security design on hiding behind a single monolithic solution—the Bastion model—results in the possibility of a single point of failure.

With the inevitable help of Murphy's Law, intruders and hackers will eventually bypass this single point (like the Maginot Line) or there will be some sort of malfunction or untoward event at that single point. When that happens, the system will be wide open to attack.

The Bastion model of security is all too common in both the information technology (IT) and industrial controls worlds. Many companies base their plant floor and SCADA security solutions on a single firewall between the business network and the control system network.

Even worse, others depend on single firewall between business and the Internet to protect the control system. In either case, these companies believe this firewall will be the ultimate security filter and prevent anything evil from ever getting to the control system.

Nothing could be further from the truth.

FAST FORWARD

- Firewalls are a fantastic tool in the security toolbox, but industry has misused them.
- Effective security comes by layering multiple security solutions.
- Poorly patched Windows-based computers abound.

For related information, see "What happens in plant stays in plant," page 14.

> "If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere."

Many roads for invading Rome

To understand why the Bastion model fails, it is helpful to look at the Slammer Worm and how it has affected control systems since its creation in 2003.

According to records in the Industrial Security Incident Database, this one worm has been responsible for more documented incidents of process disruption than any other source.

A few of its "achievements" include interrupting power distribution SCADA systems, infecting the safety parameter display system in a nuclear plant, and curtailing oil operations in the Gulf of Mexico.

What is particularly interesting is the Slammer worm has used at least five different pathways to get to its control system victims.

In one case, it got into a petroleum control system via a maintenance laptop that was used at home (and infected) and then brought into the plant. In another case, it infected a paper machine's human-machine interface (HMI) via a remote support dial-up modem. In a third case it passed right through a poorly configured firewall.

In all these examples there were firewalls in place, but the worm either bypassed them, a la the Maginot Line, or took advantage of some flaw in the firewall's deployment.

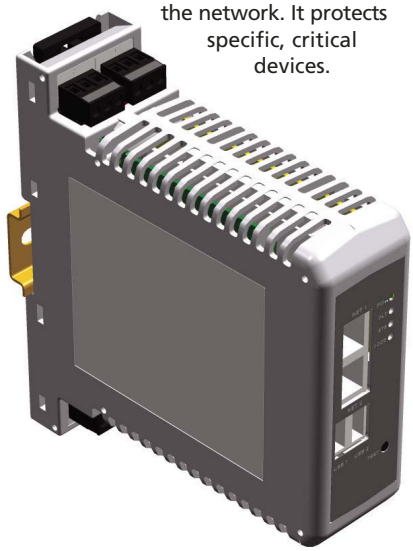
Slammer is just one example—an analysis of

75 security incidents against controls systems between 2002 and 2006 shows over half the external attacks come through secondary pathways such as dial-up connections, wireless systems, and mobile devices. In these cases, like the Maginot Line, the firewall did its job, but the security strategy failed.

In other cases, the firewall appears to allow attacks to go right through it. Even this is not usually the fault of the firewall, but the fault of poor configuration. A typical IT-style firewall requires considerable expertise to design, commission, and maintain. The complexity of this task is too often underestimated.

In a seminal paper on firewall configuration errors, Dr. Avishai Wool showed many IT firewalls in major corporations are enforcing poorly written rulesets and are vulnerable to attack.

In the study, Wool defined 12 serious firewall configuration errors (each very general in nature) and then inspected the firewall configurations of 37 major corporations. He found on average seven serious errors per firewall, with some having as many as 12 errors.



A security device like this can mount inside the firewall and between a control apparatus and the network. It protects specific, critical devices.

"Almost 80% of firewalls allow both the 'Any' service on inbound rules and insecure access to the firewalls. These are gross mistakes by any account," Wool said.

When bad guys (and bugs) get in

Once a virus or hacker does get past the business or control system firewall, the typical control system is an easy target for attack. Poorly patched Windows-based computers abound, and anti-virus software is the exception rather than the rule.

For example, during a security survey conducted at a major refinery, we discovered only 55% of the Windows 2000/XP Machines in control rooms had the patch that prevented Blaster infections, and even fewer (38%) had the patch for the Sasser Worm installed.

Yet both these patches had been available for over two years, and the control system vendor had approved them at the time of the survey. Even the most inexperienced hacker could have taken over this control system in a matter of hours.

The actual control devices, such as the programmable logic controller (PLC) or Remote Terminal Unit (RTU) are even

softer targets than the unpatched PCs. In a study by CERN, Europe's laboratory for high energy physics, 25 industrial control devices (mostly PLCs) were tested using standard IT security tools (such as Nessus and Netwox) that are available to the average attacker.

Almost half of the devices failed the tests, usually due to communications failures, system crashes, and unprotected services. For experts in the field, these results were not very surprising because the vast majority of the PLCs and RTUs currently in use offer no authentication, integrity, or confidentiality mechanisms and are subject to complete control by any individual that can "ping" the device. Nor can one easily update them or add security features to them.

Defense in depth: The perimeter

At this point, one might be thinking firewalls are bad technology.

This is not the case. Firewalls are a fantastic tool in the security toolbox, but industry has misused them. The solution to securing the plant floor is to build a proper defense-in-depth strategy that does not over rely on any single technology. It also means first creating a proper electronic perimeter around the control system and then hardening the devices within.

The security perimeter for a control system is both policy and technology. First, policy sets out what truly belongs on the control system network and what is outside. Next, a primary control system firewall acts as the choke point for all traffic between the outside world and the control system devices.

Proper design and deployment of this control system firewall is critical—ideally, it should be deployed in the appropriate multi-layer architecture described in guidelines like the "NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks."

Often this is not the case.

Paul Dorey of BP noted in his keynote speech at the Process Control Security Forum in June 2006 that comments like "My networks aren't connected" and "My server uses a separate network card to connect to the PCN and the corporate network," do not indicate a secure network design and are simply a great way to infect both business and control system networks.

Similarly, using routers or switches in place of true firewalls is generally not acceptable. Detailed reasons for using proper firewalls and the basics of designing multi-layer architectures described in the NISCC Good Practice Guide.

Defense in depth: Plant floor

Once the electronic perimeter of the control system is secure, it is necessary to build the secondary layers of defense on the control system itself.

For those control components (such as HMIs and data historians) that sit on traditional IT operating systems such as Windows and Linux, this should take advantage of the proven IT strategies of Patch and Anti-Virus (A/V) Management.

Many control engineers mistakenly believe patching or anti-virus deployment is not possible on control systems. While one cannot blindly deploy new A/V signatures or patches into the industrial control environment, the safe deployment of anti-virus software or patches on control systems is very achievable.

A number of leading companies have demonstrated that careful A/V and patching policy can balance the need for system reliability with the need for system security.

For example, at ISA EXPO 2006, industry giants Dow Chemical, Proctor and Gamble, and Astrazeneca Pharmaceutical all described how they successfully deployed anti-virus technology and patch management on their control systems.

In the power industry, the Edison Electric Institute has detailed recommendations on a tiered approach to patch management for control systems.

Finally, most major control equipment vendors now offer guidance on both patch management and A/V deployment for their control products. Thus, there is little reason for control systems not to have hardened computers on the plant floor through good patch and A/V programs.

Defense in depth: The controller

For those devices like PLCs, RTUs, and DCS controllers where patching or antivirus solutions are not readily available, the use of industrial security appliances is a good idea.

This rapidly evolving security solution rests on the use of low-cost security modules deployed directly in front of each control device (or group of devices) that needs protection.

Terminology

Murphy's Law is a popular adage in Western culture that broadly states, "Things will go wrong in any given situation, if you give them a chance."

Slammer worm: The SQL slammer worm is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic on 25 January 2003. The worm was possible because of software security vulnerability in SQL Server first reported by Microsoft on 24 July 2002. A patch had been available from Microsoft for six months prior to the worm's launch, but many installations neglected to install the patch, including some at Microsoft.

Sasser worm is a computer worm that affects computers running vulnerable versions of the Microsoft operating systems Windows XP and Windows 2000. It spreads by exploiting the system through a vulnerable network port. Thus, it is particularly potent in that it can spread without the help of the user, but a properly configured firewall can easily stop it.

PLC: A programmable logic controller is an electronic microprocessor device that stores and executes automatically a series of programmed commands that produce a machine's sequence of operation.

RTU is a remote terminal unit. In SCADA systems, an RTU is a device installed at a remote location that collects data, codes the data into a format that is transmittable, and transmits that data back to a central station, or master.

Industrial security appliances provide local protection for critical control devices, similar to the way personal firewalls (like Windows firewall), antivirus software, or intrusion detection systems (like TripWire) provide local protection for desktop computers.

This way if a hacker or virus manages to get through the electronic perimeter firewall, it will still need to breach an army of control-focused security devices before it can do any damage.

Two examples of this type of security solution are the Honeywell C300 firewall and the MTL Instruments Tofino Security Solution.

The first is a small module that is preconfigured to protect Honeywell controllers from possible attack. Its focus on a specific control device and its industrial design results in a firewall solution that is simple for field personnel to install correctly.

The Tofino Solution is equally simple to install, avoiding the complexity of the typical IT firewall. Field technicians simply connect it between the control device and the rest of the network, apply power and walk away, yet it can also be configured, monitored, and managed from a Central Management Platform located somewhere on the corporate network.

Because of their focus on protecting a small number of critical devices rather than a whole network, both of these appliances can specifically tune to meet the security needs of the device they are protecting.

Finally and metaphorically, recall that: "The Maginot Line did not fail France, but the 'Maginot mentality' did cause her defeat."

Industrial security designs that assume all evil traffic will flow through a single choke point are succumbing to the same dangerous set of beliefs. Depending on a single firewall is building a security solution based on a single point of security failure.

Only a proper defense in depth design where the control devices and systems are hardened, both individually and collectively, can provide reliable security for the plant floor.

RESOURCES

The Jericho Forum
http://www.JerichoForum.org

Uncovering Cyber Flaws
www.isa.org/link/Uncovercyber

SP99 counterattacks
www.isa.org/link/SP99counter

Who's the enemy? Don't look at IT
www.isa.org/link/enemywho

ABOUT THE AUTHOR

Eric Byres (Eric@byressecurity.com) is the CEO of Byres Security, a registered P.Eng., and a senior member of ISA. He is a member of ISA-SP99: Manufacturing and Control Systems Security. He founded the Critical Infrastructure Research Center at the British Columbia Institute of Technology.

View the online version at www.isa.org/intech/20070306.