# WOLVES AT THE DOOR(S) OF THE HOUSE OF STRAW

*The need for inherently secure control systems*

**by Eric Byres**

In most respects, the security plan for the petroleum drilling operation seemed like a good one. There was a well-managed corporate firewall protecting the corporate intranet from the Internet and switches with virtual local area networks (VLANs) separating that intranet from the automation network. Software patching was done on the business servers as much as possible, though it was pretty haphazard for some of the computers on the automation network, due to fears that the new patches might impact production. Certainly there could be a few improvements, but most of the control staff were pretty sure that all the bad things happening on the Internet were going to stay there and not bother their isolated operation in far north Alaska.

Then late one cold January night in 2003, the operators at the main facility noticed that they were intermittently losing communications between their consoles and the SCADA servers connected to the drill sites. Next they noticed that the PLCs and DCSs at the drill sites were losing connectivity. As the night wore on, the situation became increasingly serious, and a shutdown of operations became a possibility. Then IT support staff reported that the automation system was under a massive Slammer worm attack—five HMI PCs running an unpatched version of MS-SQL server were creating a traffic storm that was clogging up all the routers and switches throughout the automation network.

The offending computers were shut down, the automation system was disconnected from the corporate network, and the situation was saved. Both production and drilling operations had escaped. The impact was limited mostly to loss of alarm data for a few hours. Of course, the impact on the support staff was significant, as it took several days to track down and patch all the offending automation and business systems. But everyone knew that they had been lucky—at the time of the incident, the main facility DCS used a proprietary, non-Ethernet HMI interface, so it wasn't affected. However, that system was scheduled to be replaced with an Ethernet-based system soon, so the next time things could be much worse.

### What Went Wrong?

There was a good firewall in place, but somehow it was bypassed by the worm. Probably there was configuration error in its rule sets (see sidebar), but it also could have been that an infected laptop was brought into the network. (Three-and-a-half months later this happened to a refinery in Louisiana.) Maybe a dial-up modem was the culprit.

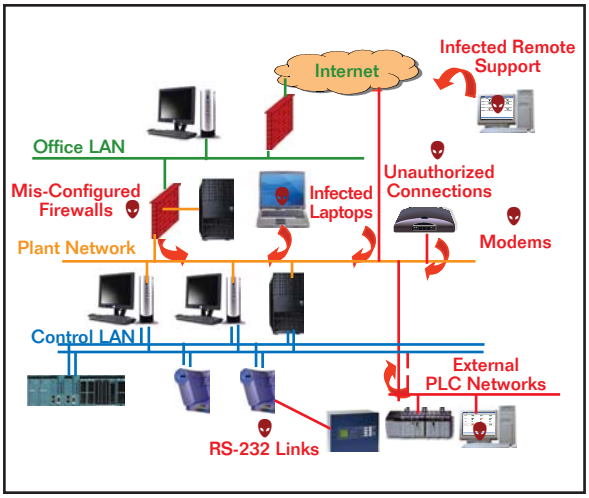
We will probably never know how the Slammer worm made it into this facility, but the fact is that once the worm was on the inside, it found a very soft target and really could begin to do its worst. The VLANs separating the automation system from the corporate network were never up to the job of protecting control systems from a worm—they were designed to limit broadcasts and simplify network administrationa—and the unpatched computers were just sitting ducks, waiting to be infected.

The real culprit in this incident was the fact that this facility had depended on what is known as the "bastion model" for its security design. The bastion model is based on the idea of hiding all key assets behind a single, monolithic security solution and letting it provide all the security to the system. It this case, the bastion was the single firewall between the business network and Internet.

Most corporate Information Technology (IT) departments gave up on the bastion model years ago. Sure they still have big boundary firewalls, but just try installing a computer on their network that doesn't have anti-virus soft-

**FIGURE 1.**

**THE POROUS BOUNDARY**




**Current security arrangement allow many pathways into the control system.**

ware, current patches or a personal firewall installed and see what happens. Chances are the IT department will cut you off the network faster than you can say, "Bastion firewall, please don't fail me now."

It's not that IT departments don't trust their firewalls; they just know that depending on a single firewall for all security protection is introducing a single point of failure into their system. With a technology as complicated as computer networking, a single point of failure is an invitation for Murphy and his Law to play havoc with the security of an entire system. So the IT department does its best to secure the overall network, but it also expects that each device on the network is secure in its own right.

**A single point of failure invites Murphy and his Law to play havoc with the entire system.**

Unfortunately, in the control system world, we don't have the same philosophy. We believe that as long as we have some sort of device separating the control network from the business network, we are safe. As the incident at the drilling operation showed, this belief is misguided at best—the existence of five unpatched computers (in an automation network comprising of hundreds of computers and controllers) put the entire system at serious risk.

### Where Did That Boundary Go?

IT departments have also learned that their networks are becoming so complicated, it is difficult find the network boundary. For example, the laptop that I am writing this article on is behind my home firewall right now. Yesterday it was behind the corporate firewall at my office. Tomorrow it will be on the unprotected wireless network provided by the local airport. At the same time, it will be connected into a number of key corporate servers back at my head office. So where is the corporate network boundary and what is on it? The answer is "We don't really know." So can we depend on one firewall to provide all the security? No!

Now control system networks may not have laptops moving around, but they do have a lot of interconnections that we tend to forget about. Besides the usual link to the business LAN, there can be a myriad of other connections into the control system, including serial links, wireless systems, third-party maintenance connections, remote-site connections over leased public telecommunications networks and dial-up modems. In fact, when ARC Advisory Group recently surveyed control engineers about the types of connections that their automation networks had to the outside world, this is what it found:

- 47.5% — Company Intranet/Business Network
- 42.5% — Direct Internet Connections
- 35% — Direct Dial-up Modems
- 20% — Wireless Modems
- 17.5% — No Connection
- 8.0% — Other Connections

Notice that the percentages in the ARC study do not add up to 100%, indicating that most facilities have multiple pathways into the control system. One security survey of a large refinery uncovered 14 different pathways. The bottom line is that modern control systems are so complex that expecting every single byte of information flowing in or out of the automation network to be inspected by a single firewall is just no longer realistic.

So if the bastion model of security won't protect our control systems, what will? One place to look is in the work of a little-known, but influential, non-profit foundation called the Jericho Forum (www.opengroup.org/jericho/).

**Eric J. Byres, PE,** is principal at Byres Security, Inc. He can be reached at eric@byressecurity.com.

**The next installment of this series will discuss the Jericho Forum and its approach to control system security.**

## WHEN GOOD FIREWALLS GO BAD

**While technologies used inside boundary firewalls are well understood, research indicates that configuring them correctly is still more of an art than a science. In a landmark paper on firewall configuration errors, Avishai Wool showed that even core firewalls in major corporations can be enforcing poorly written rule sets and 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 an average seven serious errors per firewall, with some having as many as 12 errors. The results clearly indicate the complex nature of firewall management and that many SCADA/PCN firewalls may be little more than dangerous placebos, offering protection more illusionary than real.**

### NUMBERS OF CRITICAL ERRORS IN PROFESSIONALLY CONFIGURED FIREWALLS