TOFINO SECURITY
A BELDEN BRAND

White Paper

Understanding Deep Packet Inspection (DPI) for SCADA Security

By Eric Byres, P. Eng., ISA Fellow, CTO and VP of Engineering, Tofino Security, a Belden Brand.

Table of Contents

Executive Summary 1
The Need for Better Security Technology 2
Some Firewall Basics 2
The Problem: SCADA/ICS Protocols Have No Granularity 2-3
The Solution: Deep Packet Inspection 3
DPI SCADA Security in the Real World 3-4
Why New Malware Demands DPI Technology 4-5
DPI Provides Robust Security for SCADA 5
References 5

Executive Summary

The world's manufacturing, energy and transportation infrastructures are currently facing a serious security crisis. These critical systems are largely based on legacy SCADA and Industrial Control System (ICS) products and protocols. Many of these products are decades old and were never designed with security in mind.

Yet industry has also embraced new network technologies like Ethernet and TCP/IP, which have enabled instant access to data throughout the organization, including the plant floor. While this interlinking improves efficiency, it also significantly increases the exposure of these control systems to external forces such as worms, viruses and hackers.

Given the 20 year life cycle common for industrial systems, it will be many years before more secure ICS and SCADA devices and protocols are in widespread use. This leaves millions of legacy control systems open to attack from even the most inexperienced hacker. If a hacker or worm can get any control system access, it can exploit the protocol to disable or destroy most industrial controllers.

The good news is that there is an effective and easy-to-deploy solution to this security crisis. Using an advanced technology called "Deep Packet Inspection" (DPI), SCADA-aware firewalls can offer fine-grained control of control system traffic. This white paper explains what DPI is and how it compares to traditional IT firewalls. It then outlines how engineers can use DPI to block the malicious or inappropriate traffic, while avoiding needless reliability impacts on the control system. A case history illustrates how a seaway management company used Modbus DPI firewalls to secure a mission critical canal system.

The Need for Better Security Technology

Over the past decade, industry has embraced network technologies like Ethernet and TCP/IP for SCADA and process control systems. This has enabled companies to operate cost effectively and implement more agile business practices through instant access to data throughout the organization, including the plant floor.

While companies reap the benefits of these new technologies, many are also discovering the inherent dangers that result from making control systems more accessible to a wider range of users. Linking corporate systems together to provide access to managers, customers and suppliers significantly increases the exposure of these systems to external forces such as worms, viruses and hackers.

To make matters worse, network protocols used by SCADA and Industrial Control Systems (ICS) were never designed with security in mind. If they offer any capability to restrict what users can do over the network, it is primitive and easy to subvert. If an individual is allowed to read data from a controller, then they can also shut down or reprogram the controller.

These issues are likely to remain with us for at least the next decade. Industrial control systems are rarely replaced; their useful lives may be 10, 20 or more years. Similarly, the security limitations of the SCADA and ICS protocols cannot be addressed through patches, as their functionality is defined in established standards that take years to change.

It will be years before newer, more secure ICS and SCADA devices are in widespread use. This leaves millions of legacy control systems open to attack from even the most inexperienced hacker. If a hacker or worm can get any control system access, it can exploit the protocol to disable or destroy most industrial controllers.

The good news is that there is a solution to this problem. It is easy to use. It doesn't require the complete replacement of billions of dollars of existing SCADA and ICS equipment. And it is very effective.

The solution is a technology called "Deep Packet Inspection" (DPI) and it offers fine-grained control of SCADA network traffic. This white paper explains what DPI is and how it is being used to secure critical SCADA systems throughout the world.

Firewall Basics

To understand how DPI works, it is important to understand how the traditional IT firewall works. A firewall is a device that monitors and controls traffic flowing in or between networks. It starts by intercepting the traffic passing through it and comparing each message to a predefined set of rules (called Access Control Lists or ACLs). Any messages that do not match the ACLs are prevented from passing through the firewall.

The traditional firewall allows ACLs to check three primary fields in a message :

1. The address of the computer sending the message (i.e. the Source IP Address),
2. The address of the computer receiving the message (i.e. the Destination IP Address),
3. The application layer protocol contained by the IP message, as indicated in the destination port number field (i.e. the Destination Port).

The source and destination address checks are easy to understand. These restrict traffic flows to specific computers, based on their IP addresses. As long as the addresses remain the same, the firewall can control which computers can interact.

The destination port number needs a bit more explanation. These ports are not physical ports like an Ethernet or USB port, but instead are special numbers embedded in every TCP or UDP message. They are used to identify the application protocol being carried in the message. For example, the Modbus/TCP protocol uses port 502, while the web protocol, HTTP, uses port 80. These numbers are registered under the Internet Assigned Numbers Authority (IANA) and are rarely ever changed.

To put this all together, imagine you only want to allow web traffic (i.e. HTTP traffic) from a client at IP address 192.168.1.10 to a web server with an address of 192.168.1.20. Then you would write an ACL rule something like:

```
"Allow Src=192.168.1.10
Dst=192.168.1.20 Port=HTTP"
```

You would load this ACL in the firewall and as long as all three criteria were met, the message would be allowed through.

Or perhaps you want to block all Modbus traffic from passing through the firewall. You would simply define a rule that blocks all packets containing 502 in the destination port field.

Seems simple, doesn't it?

The Problem: SCADA/ICS Protocols Have No Granularity

The problem with this simple scheme is that it is very black and white. Using a traditional IT firewall, one can either allow a certain protocol or block it. Fine-grained control of the protocol is impossible.

This is an issue because the SCADA ICS protocols themselves have no granularity. From the perspective of the port number, a data read message looks EXACTLY like a firmware update message. If you allow data read messages, from an HMI to a PLC, to pass through a traditional firewall, you are also allowing programming messages to pass through. This is a serious security issue.

For example, in the spring of 2009 a US Government agency produced a report for major energy companies that stated:

> "A vulnerability has been identified and verified within the firmware upgrade process used in control systems deployed in Critical Infrastructure and Key Resources (CIKR)... development of a mitigation plan is required to protect the installed customer base and the CIKR of the nation. Firmware

> Vulnerability Mitigation Steps [includes] blocking network firmware upgrades with appropriate firewall rules."

Unfortunately, the IT firewalls available on the market could not differentiate between the different SCADA commands. As a result, "blocking network firmware upgrades with appropriate firewall rules" results in the blocking of all SCADA traffic. Since the reliable flow of SCADA traffic is critical to the average industrial facility, most engineers opted to let everything pass and take their chances with security.

The Solution: Deep Packet Inspection

Clearly the firewall needs to dig deeper into the protocols to understand exactly what the protocol is being used for. And that is exactly what Deep Packet Inspection does. After the traditional firewall rules are applied, the firewall inspects the content contained in the TCP/IP messages and applies more detailed rules. It is designed to understand the specific SCADA protocols and then apply filters on fields and values that matter to control systems. Depending on the protocol, these fields might include commands (such as Register Read vs. Register Write), objects (such as a Motor Object), services (get vs. set) and PLC address ranges.

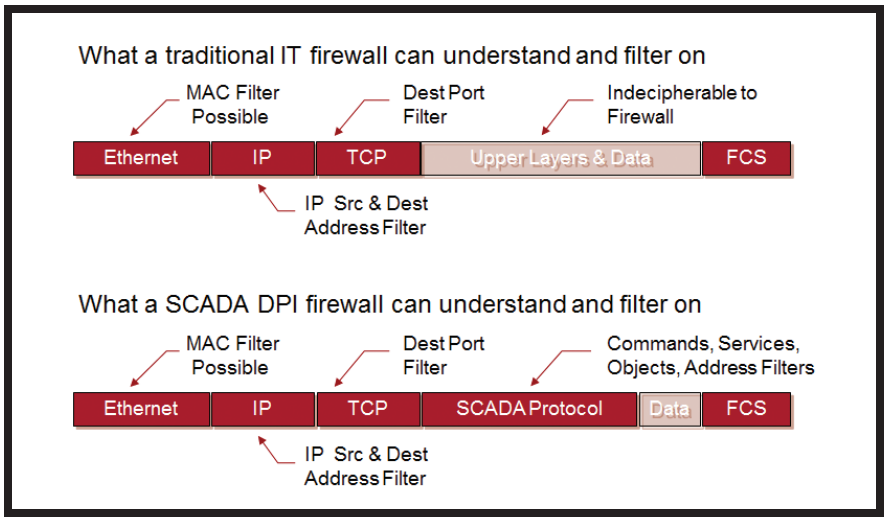

Figure 1: Comparing filtering options in a traditional firewall and a DPI Firewall. A traditional firewall cannot understand the SCADA protocol and thus can only allow or deny all SCADA messages as a group.

For example, a Modbus DPI firewall (such as the Honeywell Modbus Read-only Firewall or the Schneider ConneXium Tofino Firewall) determines if the Modbus message contains a read or a write command and then drops all write messages. Good DPI firewalls can also "sanity check" traffic for strangely formatted messages or unusual behaviours (such as 10,000 reply messages in response to a single request message). These sorts of abnormal messages can indicate traffic created by a hacker trying to crash a PLC and need to be blocked.

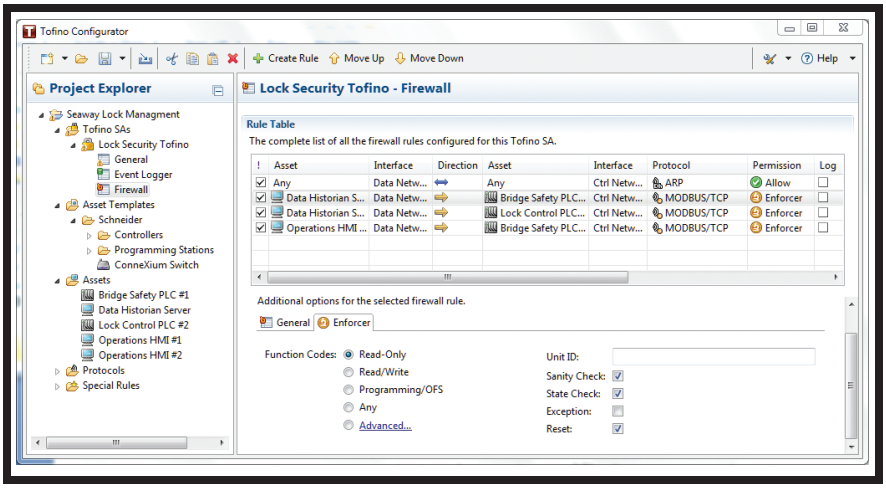

Figure 2: Firewall rules restricting Modbus traffic between the Data Historian and PLCs to Read-only commands. Other filters such as 'Sanity-Check' and 'State Check' ensure that all traffic match the Modbus specifications.

DPI SCADA Security in the Real World

Fine-grained control of SCADA/ICS traffic can significantly improve the security and reliability of a system. For example, consider the real world case of a seaway management company. It uses Schneider PLCs at all its control locks and bridges to ensure the safety of ship and vehicle traffic. Making sure that these PLCs are not tampered with is critical for the safety of both the ships and the public traveling over bridges at the locks.

The problem this company faced was that a number of operations computers needed to continuously access PLCs for data. However only special control computers should be permitted to send commands and impact the operation of equipment. Traditional password

or IT firewall solutions were not considered secure, because they didn't offer the fine-grained control needed.

The solution was to use Modbus DPI firewalls to control all traffic to the PLC. Only Modbus Read messages were allowed to reach the PLCs (except for a few high security computers). All remote Modbus programming commands were blocked so that programming was restricted to onsite engineers. A total of 54 DPI firewalls were installed in 24 locations and the system has run without incident since late 2008.

Why New Malware Demands DPI Technology

Five years ago, DPI was considered a nice-to-have capability. Now thanks to the current generation of worms like Stuxnet, Duqu and Conficker, it is a must-have technology if you want a secure ICS or SCADA system.

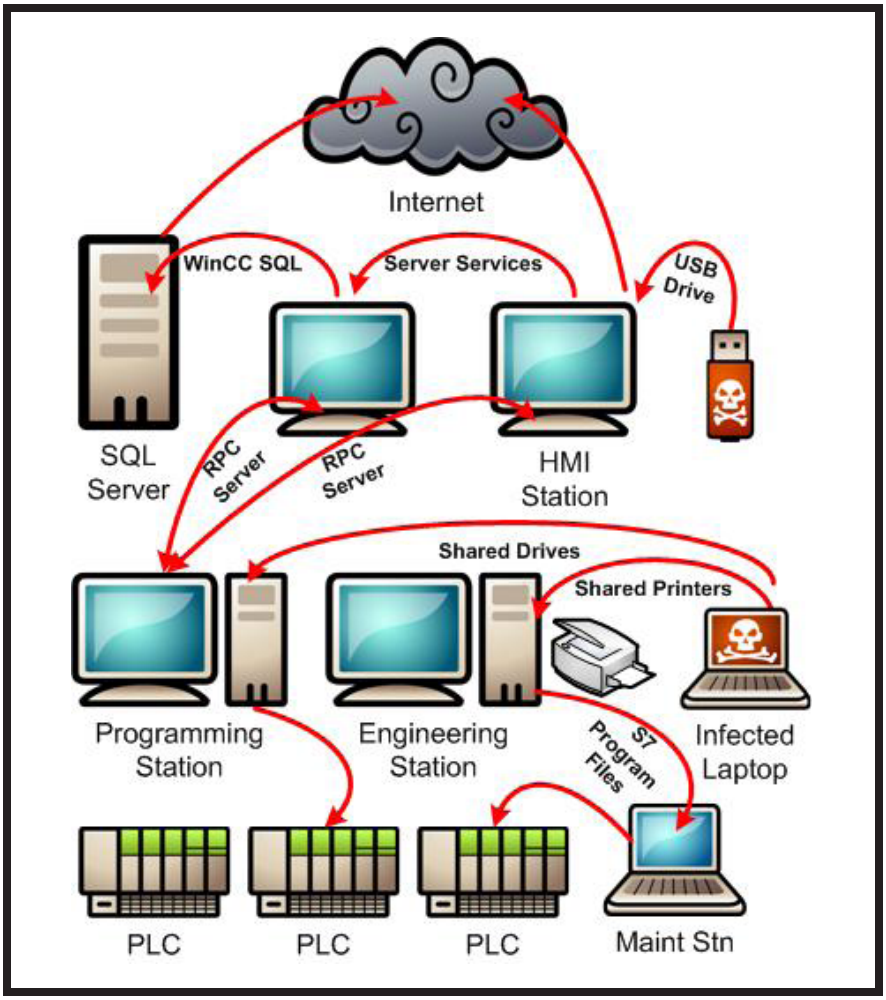

Figure 3: Stuxnet spread many ways, including using the RPC protocol as a vector. Deep Packet Inspection could have detected this non-standard use of the protocol and restricted some of the ways the worm spread.

Today's malware designers know that firewalls and intrusion detection systems will spot the use of an unusual protocol instantly. They know that if the protocols on a network are normally HTTP (i.e. web browsing), Modbus and MS-SQL (i.e. database queries) then the sudden appearance of a new protocol will put the smart system administrator on his or her guard.

Thus worm designers work to stay under the radar by hiding their network traffic inside protocols that are already common on the network they are attacking. For example, many worms now hide their outbound communications in what appear to be normal HTTP messages.

Stuxnet is a particularly good example of this covert use of otherwise innocent protocols. It made heavy use of a protocol called Remote Procedure Call (RPC) for both infecting new victims and for peer-to-peer (P2P) communications between infected machines.

RPC is an ideal protocol for SCADA and ICS attacks because it is used for so many legitimate purposes in modern control systems. For example, the dominant industrial integration technology, OPC Classic, is based on DCOM and this in turn requires that RPC traffic be allowed.

Furthermore, control system servers and workstations are routinely configured to share files or printers using the Microsoft SMB protocol, which also runs on top of RPC. Perhaps most relevant in this example, all Siemens PCS 7 control systems make extensive use of a proprietary messaging technology that travels over RPC. If you were an administrator watching network traffic on a Stuxnet infected network, all you would see was a little more RPC traffic than usual, hardly a cause for alarm.

Even if you suspected something was wrong, you would be thwarted if all you had was a normal firewall. The simple blocking of all

RPC traffic would likely result in a self-induced denial of service for your entire factory. Without tools to inspect the content of RPC messages and block suspicious traffic (i.e. Deep Packet Inspection), you would be unable to stop the malware.

DPI Provides Robust Security for SCADA

DPI technology is a very powerful tool in the security tool box. It allows the engineer to block the malicious or inappropriate SCADA/ICS traffic, yet avoid needless impact on the control system. Without it, the designers of modern worms clearly have the upper hand. In order to stay ahead of today's advanced threats, DPI capability has become a must-have in all industrial firewalls.

References:

1. How Stuxnet Spreads https://www.tofinosecurity.com/how-stuxnet-spreads
2. PLC Security Risk: Controller Operating Systems https://www.tofinosecurity.com/blog/plc-security-risk-controller-operating-systems
3. "Tofino Enforcer Revolutionizes Modbus TCP/IP Security http://www.tofinosecurity.com/article/tofino%E2%84%A2-enforcer%E2%84%A2-revolutionizes-modbus-tcpip-security
4. Tofino Modbus TCP Enforcer Loadable Security Module Information https://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM
   The Data Sheet for this product follows this White Paper.
5. Tofino OPC Enforcer Loadable Security Module Information http://www.tofinosecurity.com/products/Tofino-OPC-Enforcer-LSM
   The Data Sheet for this product follows this White Paper.
6. Securing Your OPC Classic Control System http://www.opcfoundation.org/DownloadFile.aspx?CM=3&tRI=781&tCN=KEY&tCI=282&tCU=4
7. Using Tofino™ to Control the Spread of Stuxnet Malware http://www.tofinosecurity.com/professional/using-tofino-control-stuxnet
8. Video: MTL Instruments' security video showing how a worm on a USB key attacks a PLC over Modbus TCP http://www.youtube.com/watch?v=G4E0bxZGZL0

TOFINO SECURITY
A BELDEN BRAND

Sales Inquiries: **1.877.297.3799**

www.tofinosecurity.com