Network Security Infrastructure Testing

Version 1.2

October 12, 2005

Prepared by: Sandia National Laboratories' Center for SCADA Security
Project Lead – Ray Parks
Technical Lead – Jason Hills
Technical Support – Sammy Smith, Tom Davis, Ana Baros, Patricia Cordeiro

This work was conducted for the DOE Office of Electricity Delivery and Energy Reliability under Contract M64SCADSNL

Contents

Sandia National Laboratories

1 Executive Summary

Control system communication protocols are used to manage remote systems, to communicate between control centers, and to control factory automation. The control system protocols have been functionally adapted to Transmission Control Protocol/Internet Protocol (TCP/IP) and other Information Technology (IT) infrastructure, but these protocols were developed for dedicated communications and are insecure in this new environment. Network Security Infrastructure (NSI)[1] products have not been designed to meet control system protocol needs leaving Supervisory Control and Data Acquisition (SCADA) protocols susceptible to network attacks on confidentiality, integrity and availability. While the control system industry is developing and implementing security features for standard protocols to solve this problem, control system upgrades are costly and fraught with risk to the system under control. Additionally, the security features introduced are not always sufficient to mitigate all the potential vulnerabilities. For these reasons, Sandia and others have recommended adapting the network security to the protocols' vulnerabilities, using network security infrastructure practices such as packet-filtering firewalls, Network Address Translation (NAT), and Virtual Private Networks (VPN).

Sandia conducted testing of NSI interactions with SCADA communication protocols in order to help vendors and industry users better secure these protocols when implementing them in TCP/IP networks over public telecommunications infrastructures. The testing addressed this goal by: determining NSI interactions with SCADA system protocols to improve acceptance of NSI by SCADA operators, and finding problems for feedback to SCADA vendors and NSI vendors to improve the security of implementations.

A series of compatibility tests, emulating communications between a control center and a remote facility, were performed between four commonly used SCADA communication protocols (DNP3, Modbus, Ethernet/IP, and OPC)[2] and industry standard firewall and VPN products.

The testing analysis showed: 1) the DNP3 protocol worked correctly and required minimal configuration of the NSI in all test modes, 2) the Modbus and Ethernet/IP protocols work similarly to DNP3 over TCP/IP networks, 3) the OPC protocol fits poorly with standard firewalls, did not work at all with NAT firewall tests, but works correctly over a VPN, 4) a SCADA network using OPC through a standard firewall exposes its own and collocated systems to network attack since the additional defense of NAT is unavailable with OPC, whereas 5) this would not be the case when using a VPN which provides additional protection since the firewall is not opened in order to provide access for the protocol being used.

---

[1] NSI includes standard information technology devices used to secure network enclaves and hosts from attack via the network, such as: firewalls, routers, switches, and other, more sophisticated, components.

[2] DNP3 - Distributed Network Protocol, Version 3; Modbus - Modicon Bus Protocol; OPC - Object Linking and Embedding (OLE) for Process Control

Sandia National Laboratories

2 Introduction

Modern control systems have evolved to using standard communication protocols implemented over computer networks. Legacy control systems used serial protocols, either over dedicated communication lines for local communications or over dedicated or dial-up lines for long-distance communications. Each of these protocols was developed by one of many vendors for their specific hardware. Over time, the control system industry has consolidated and transformed into fewer vendors who are using fewer protocols that have become either actual or *de facto* standards. As both the installation and operational costs of dedicated communications has risen, integrators and operators have turned to the ubiquitous information technology communications infrastructure. Protocols have been adapted to use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) riding within Internet Protocol (IP) packets over standard IT types of infrastructures. This testing only addressed protocols that use the TCP/IP protocol.

Control system communication protocols are used to manage remote systems, to communicate between control centers, and to control factory automation. The DNP3 protocol is used extensively in the electric power and water industries within North America, South America, Australia and China. The Modbus protocol is used in factory automation, including oil and gas refineries, to manage Intelligent Electronic Devices (IEDs) that control manufacturing devices as well as in electric power. The Ethernet/IP protocol is also used in factory automation. The OPC protocol is penetrating all SCADA markets since it enables the use of commercial off the shelf (COTS) personal computers for process control.

The control system communication protocols have been functionally adapted to TCP/IP and other IT infrastructure, but NSI products have not been designed to meet control system protocol needs. This leaves SCADA protocols susceptible to network attacks on confidentiality, integrity and availability. The control system industry is developing and implementing security features for standard protocols to solve this problem. However, control system upgrades are costly and fraught with risk to the system under control, so there is a natural inclination to retain legacy equipment using insecure protocols. Additionally, the security features introduced are not always sufficient to mitigate all the potential vulnerabilities. For these reasons, Sandia and others have recommended adapting the network security to the protocols' vulnerabilities, using network security infrastructure practices such as packet-filtering firewalls, Network Address Translation, and Virtual Private Networks.

One of the most effective practices to secure SCADA networks would be through the use of NSI. However, integrators and owners/operators are reluctant to implement NSI, partly because they often have a limited understanding of the difficulties associated with building successful NSI for control systems. NSI vendors are trying to adapt their products to control systems but lack experience and knowledge of the interactive effects of using network protocols with control

system protocols. To help alleviate these problems, Sandia determined the effects of NSI on SCADA (availability) and, conversely, the effects of SCADA on NSI (insecure firewall configurations).

3 Test Description

A control system communication protocol set was chosen from those previously identified as having market share and penetration into energy infrastructures. A scenario was then developed explaining how each protocol would plausibly interact with NSI. The test setup was changed to emulate each particular scenario. Next, NSI configurations were varied to find interactions with the protocol. Traffic shaping tools were used to test latency effects and vulnerability scanning tools were used to test NSI effectiveness when set up in an example SCADA configuration.

3.1 Test Plan

The initial testing plan called for a series of compatibility tests between four commonly used SCADA protocols (Distributed Network Protocol, Version 3 (DNP3), Modicon Bus Protocol (Modbus), Ethernet/IP, and Object Linking and Embedding (OLE) for Process Control (OPC)) and industry standard firewall and VPN products. The test configurations emulated communications between a control center and a remote facility. During the testing the Modbus setup did not actually transmit Modbus packets over the network. Instead, these packets were wrapped in the OPC protocol. This represents a trend in SCADA software that adapts older protocols to COTS platforms by using OPC as the transport protocol for the older protocol, old protocol traffic inside the new protocol.

3.2 Test Architecture

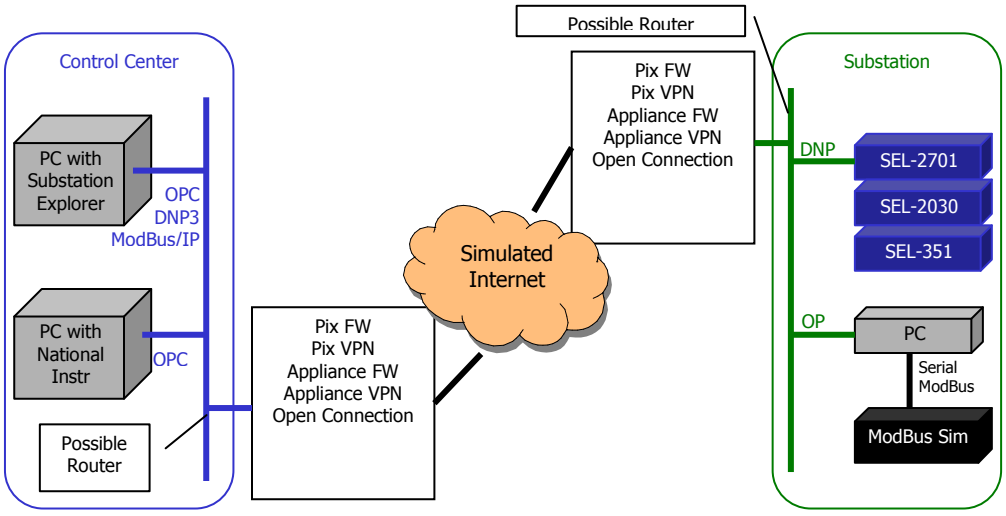

Figure 1 Test Architecture

The test architecture comprised two networks joined by NSI equipment. One network emulates a control center and contained (not always simultaneously) a

computer running National Instruments OPC client software and another computer running the Substation Explorer software. The latter can be used with all of the protocols in the test but was only used for the DNP3 testing.

The second network simulates a remote operation such as an electrical substation or pipeline pumping station. This network used a stack comprised of a Schweitzer Engineering Laboratories SEL-2030 Communications Processor with an SEL-2701 Ethernet port, an SEL-351 Directional Overcurrent and Reclosing Relay, and SEL-4000 Adaptive Multichannel Source to simulate part of an electric substation. A National Instruments Modbus protocol simulator and server software for Modbus testing provided the basic Modbus protocol setup. The National Instruments Modbus client and server translates the serial Modbus information into OLE for Process Control (OPC) for transmittal over the network. Therefore the Modbus testing was performed in this protocol-within-a-protocol configuration.

3.3 Test Configuration

The initial test configuration was limited to a single Pix firewall. However, this configuration did not allow VPN testing and was less realistic. Subsequently, a second Pix firewall and two Linksys firewalls were added to the test configuration.[3] This final test configuration allowed realistic tests with firewalls at each "location" as well as VPNs. The effects of packet-filtering firewalls, Network Address Translation, traffic shaping, and Virtual Private Networks on SCADA protocols were determined. Sufficient testing was performed in the three major configurations (standard, NAT, VPN) with the DNP3 protocol to understand this type of protocol's interactions with NSI. We were then able to generalize those results to similar standard implementations of Modbus and Ethernet/IP protocols. The testing allowed for determination of the effects the correct operation of the SCADA protocols had on the security of the NSI. In particular, configuration requirements to preserve functionality such as custom firewall rules were explored.

[3] The Pix firewalls were upgraded to the latest PixOS (6.3). They were not identical in that one had a crypto card and license while the other was in a stock configuration. The two Linksys firewalls were a BEFVP41 v1 with firmware version 1.41.1 and a BEFVP41 v2 with firmware version 1.01.04.

3.4 Expected Testing Outcomes

Substation / Control Center	Pix FW	Pix VPN	Appliance Firewall	Appliance VPN	Open
Pix FW	Possible NAT Problems; Open Ports?		Should work		Possible NAT, Routing problems
Pix VPN		Should work		May work	
Appliance Firewall	Should work		Should work		Possible NAT, Routing problems
Appliance VPN		May work		Should work	
Open	NAT, routing problems		Possible NAT, Routing problems		Works; No Security

Figure 2 Matrix of Expected Testing Outcomes

The expected testing outcomes matrix indicates the expectations at an early point in the testing. The matrix matches firewall product/configuration at the Substation with the corresponding firewall product/configuration at the Control Center. The mix of firewall product/configuration was based on Sandia's assessment experience and knowledge of SCADA systems. Later testing confirmed that the products worked according to expectations in all cases.

4 Analysis

4.1 Initial Testing

The initial testing used a subset of the eventual test bed. Initial testing only used a single Cisco PIX firewall. OPC encapsulated Modbus and the DNP3 protocols were operated through the PIX as if the firewall was protecting the substation.

Network Address Translation (NAT) is a common firewall technique to protect the IP addresses of systems internal to the firewall from direct exposure to outside attackers. NAT also expands the total space of IP addresses by allowing internal network systems to use private, non-routable IP addresses. The NAT testing quickly showed that the OPC protocol is not compatible with NAT. The OPC protocol requires that a wide range of ports be exposed through the firewall. These ports support the underlying OLE, DCOM, and RPC protocols for OPC. Unfortunately, in real-world implementations, these ports are constantly attacked from the Internet, so exposing them will leave internal networks open to attack. The SCADA systems using OPC are subject to these attacks as well as any other computers running the Windows operating system on the network. Ingress address filtering rules in the firewall can limit this exposure, although source addresses can still be spoofed.

The DNP3 protocol worked with NAT, but required special configurations on both the DNP3 slave and master hosts in which the firewall system's IP address is used instead of the slave and master IP addresses of the actual slave and master hosts. Since DNP3 uses a specific destination port but not a specific source port, NAT did not interfere with the limited port exposure required by DNP3, which opens a single, well-known port through the firewall. This exposes the DNP3 master system to attack from outside, but not any other systems on the network. Ingress address filtering rules can help limit this exposure.

4.2 VPN testing

After a second PIX firewall system and two appliance firewalls were added to the configuration an additional set of tests was conducted. With these systems, the test configuration could include Virtual Private Networks (VPNs) between the substation and control center networks.

It was determined that the DNP3 protocol works correctly through a VPN, and the VPN made the setup of the DNP3 protocol easier. By using a VPN, the master and slave port and address information doesn't need to be changed to work through the firewall. This indicates that a configuration set up in a laboratory or similar environment using the addresses and ports that are intended for use in the field doesn't need to be changed when the equipment is installed in the field.

It was determined that OPC works correctly through a VPN and enjoys the same advantage of easier setup and configuration.

Both the Cisco PIX VPN and the appliance firewall VPN worked with both protocols. It was determined that the PIX firewall VPN is more difficult to set up, primarily because of the additional steps required, but the trade-off is increased performance versus the appliance firewall VPN.

4.3 Dual firewall testing

Another set of tests consisted of pairs of firewalls configured without VPNs. In the case of the DNP3 protocol, this required further changes to allow the respective master and slave to find each other's IP address as well as configuring the firewall to route all DNP3 traffic directly to the master. The slave system in the substation is configured to use the control center firewall's IP address as the DNP master address. The substation firewall passes that traffic to the control center firewall. The control center firewall is configured to pass all DNP3 traffic directly to the master system. The master system is configured to use the substation firewall IP address as the DNP slave address and the substation firewall must be configured to pass that traffic directly to the slave. This configuration also works with NAT.

The OPC protocol testing with dual firewalls was scheduled after the DNP3 dual firewall testing. However, due to OPC's intolerance of NAT, as determined during the initial testing phase, and test system difficulties encountered with the OPC client and server systems, this testing was eliminated. This seemed

reasonable since it was unlikely that having a second firewall would make any improvements in the incompatibility of NAT and OPC.

4.4 Extrapolation

Examination of the DNP3 traffic and protocol characteristics indicated that it is fundamentally similar to Ethernet/IP and Modbus with respect to network security infrastructure. Therefore, we were able to predict with confidence that both of the latter protocols would display similar interaction with NSI.

5 Conclusions

The DNP3, Modbus, and Ethernet/IP protocols can be used with packet-filtering firewalls and NAT, although this may require special configuration of the systems at each end of the communications connection.

The OPC protocol cannot be safely used with packet-filtering firewalls and is incompatible with NAT. In the case of packet-filtering firewalls, the successful operation of OPC requires a firewall rule set that leaves a large number of ports open and exposes other systems to attack. The required open ports include TCP 135, 137, 139, 445, and 1000-5000 and UDP 135 and 137. These ports are common attack vectors for malicious software. The Modbus testing configuration revealed that OPC is becoming pervasive in SCADA infrastructures. It allows COTS PCs running Microsoft Windows to be easily integrated into these infrastructures and is used on SCADA hardware that runs Windows in embedded mode. However, these systems must either contain all communications within the local private network or the entire network will be opened to common attacks.

All tested SCADA protocols work correctly in a VPN environment and initial setup and configuration of the protocols is no more difficult than it is without using a VPN. Using a VPN does not expose any system to external attack. However, VPNs can require considerable setup and maintenance overhead for each pair of firewalls.

Open configurations (without firewalls) expose all systems including the SCADA systems to external attack.

These results can help industry users and vendors design more secure implementations when combining network protocols and SCADA protocols in control systems.

Sandia National Laboratories

6 Recommendations

Firewalls protect internal SCADA networks from external attack, but limited protection is achieved with packet filtering. The best configuration is to use VPN features of these firewalls. In operational SCADA systems with a large number of remote sites communicating with a small number or a single control center, dual firewall VPN configurations become cumbersome and extremely difficult to maintain. In these situations, the best solution may be to use a VPN concentrator at the control center and separate VPN firewalls at the remote sites. Additional research is necessary to confirm that VPNs are scalable in this configuration. The issue of scalability could be addressed through custom network simulation using OPNET modeling in the proposed Virtual SCADA Simulation Environment.

7 Acronyms

ACL..... Access Control Lists
CSS ..... Center for SCADA Security
COTS..... Commercial off the shelf products
DCOM..... Distributed Common Object Model
DNP3 ..... Distributed Network Protocol, Version 3
DOE ..... Department of Energy
IDART ..... Information Design Assurance Red Team
IEC..... International Electrotechnical Commission
IED..... Intelligent Electronic Devices
IORTA..... Information Operations, Red Teaming and Assessments
IP ..... Internet Protocol
IPSEC..... IP Security Protocol
Modbus® ..... Modicon Bus Protocol
NCC ..... Network Control Center
NMC..... Network Management Center
NSI..... Network Security Infrastructure (i.e. firewalls, routers, switches)
NSTB ..... National SCADA Test Bed
OLE..... Object Linking and Embedding
OPC..... OLE for Process Control
RPC ..... Remote Procedure Call
SCADA ..... Supervisory Control and Data Acquisition
SMS ..... (Microsoft) Systems Management Server
SNL..... Sandia National Laboratories
SNMP ..... Simple Network Management Protocol
TC57 ..... Technical Committee 57
TCP..... Transmission Control Protocol
UDP ..... User Datagram Protocol
VPN ..... Virtual Private Network
WWW..... World Wide Web