

Test Case Summary of the Yokogawa CENTUM CS 3000 Vnet Router AVR10D, CENTUM CS 3000 Field Control Unit AFV10D and the ProSafe-RS Vnet/IP Safety Control Unit SSC50D.

PREPARED FOR:
YOKOGAWA ELECTRIC CORPORATION

PREPARED BY:
WURLDTECH SECURITY TECHNOLOGIES

DATE:
APRIL 25, 2007

Overview

Wurldtech Security Technologies was engaged by Yokogawa Electric Corp to conduct cyber security testing of its CENTUM CS 3000 Field Control Unit, ProSafe-RS Vnet/IP Safety Control Unit and Vnet Router against a variety of Ethernet and TCP/IP level and Vnet/IP protocol level cyber attacks. This document sets forth a description of the tests performed, and results obtained from the testing conducted from February 5th to February 16th 2007.

Tests were performed by Wurldtech using the Achilles Assurance Platform. Wurldtech was selected as an independent party due to its expertise in network test methodologies. All testing was completed at the Wurldtech Labs facility located in Vancouver Canada.

Wurldtech Labs' test results indicate that the CENTUM CS 3000 Field Control Unit , ProSafe-RS Vnet/IP Safety Control Unit, and Vnet Router are well designed systems offering robust protection against cyber attacks. Each of the CENTUM CS 3000 Field Control Unit , ProSafe-RS Vnet/IP Safety Control Unit, and Vnet Router have earned Achilles Level 1 + Vnet/IP Certification.

The software revision number of the CENTUM CS 3000 was R3.08 and the ProSafe-RS was R1.02.

CENTUM CS 3000 Vnet Router AVR10D

Device
Model: AVR10D
Serial Number: C2GF10054C
Hardware Revision: S2
Firmware Revision: Rev9.18 *This firmware sub revision (.18) is internal. The next release products "R10" will have this feature.
Certification Level: 

Family	Test Case	Result
Discovery	Open TCP Discovery	Pass
Discovery	Open UDP Discovery	Pass
Data Link	Ethernet Random Storm	Pass
Data Link	Ethernet Unicast Storm	Pass
Data Link	Ethernet Broadcast Storm	Pass
Data Link	Ethernet Multicast Storm	Pass
Data Link	Ethernet Grammar	Pass
Data Link	ARP Flood	Pass
Data Link	ARP Grammar	Pass
Network	IP Random Storm	Pass
Network	IP Unicast Storm	Pass
Network	IP Broadcast Storm	Pass
Network	IP Multicast Storm	Pass
Network	IP Fragmentation	Pass
Network	IP Grammar Fuzz	Pass
Network	IP Grammar Fragmentation	Pass
Network	IP Grammar Options	Pass
Network	ICMP Grammar Destination Unreachable	Pass
Network	ICMP Grammar Echo	Pass
Network	ICMP Grammar Echo Reply	Pass
Network	ICMP Grammar Fuzz	Pass
Network	ICMP Grammar Parameter Problem	Pass
Network	ICMP Grammar Redirect	Pass
Network	ICMP Grammar Source Quench	Pass
Network	ICMP Grammar Time Exceeded	Pass
Network	ICMP Grammar Time Stamp	Pass
Network	ICMP Grammar Type/Code Cross Product	Pass
Transport	TCP SYN Floods	Pass
Transport	TCP/IP LAND	Pass
Transport	TCP Grammar Fuzz	Pass
Transport	TCP Grammar Options	Pass
Transport	TCP Grammar Urgent	Pass
Transport	UDP Grammar Fuzz	Pass
Proprietary	Vnet/IP Grammar	Pass
3rd Party	Nessus "Safe Plugins"	Pass

CENTUM CS 3000 Field Control Unit AFV10D

Device
Model: AFV10D
Serial Number: C2GF10055C
Hardware Revision: S2
Firmware Revision: Rev9.18 *This firmware sub revision (.18) is internal. The next release products "R10" will have this feature.
Certification Level: 

Family	Test Case	Result
Discovery	Open TCP Discovery	Pass
Discovery	Open UDP Discovery	Pass
Data Link	Ethernet Random Storm	Pass
Data Link	Ethernet Unicast Storm	Pass
Data Link	Ethernet Broadcast Storm	Pass
Data Link	Ethernet Multicast Storm	Pass
Data Link	Ethernet Grammar	Pass
Data Link	ARP Flood	Pass
Data Link	ARP Grammar	Pass
Network	IP Random Storm	Pass
Network	IP Unicast Storm	Pass
Network	IP Broadcast Storm	Pass
Network	IP Multicast Storm	Pass
Network	IP Fragmentation	Pass
Network	IP Grammar Fuzz	Pass
Network	IP Grammar Fragmentation	Pass
Network	IP Grammar Options	Pass
Network	ICMP Grammar Destination Unreachable	Pass
Network	ICMP Grammar Echo	Pass
Network	ICMP Grammar Echo Reply	Pass
Network	ICMP Grammar Fuzz	Pass
Network	ICMP Grammar Parameter Problem	Pass
Network	ICMP Grammar Redirect	Pass
Network	ICMP Grammar Source Quench	Pass
Network	ICMP Grammar Time Exceeded	Pass
Network	ICMP Grammar Time Stamp	Pass
Network	ICMP Grammar Type/Code Cross Product	Pass
Transport	TCP SYN Floods	Pass
Transport	TCP/IP LAND	Pass
Transport	TCP Grammar Fuzz	Pass
Transport	TCP Grammar Options	Pass
Transport	TCP Grammar Urgent	Pass
Transport	UDP Grammar Fuzz	Pass
Proprietary	Vnet/IP Grammar	Pass
3rd Party	Nessus "Safe Plugins"	Pass

ProSafe-RS Vnet/IP Safety Control Unit SSC50D

Device
Model: SSC50D
Serial Number: C2GJ21125C
Hardware Revision: S1
Firmware Revision: Rev9.18 *This firmware sub revision (.18) is internal. The next release products "R10" will have this feature.
Certification Level: 

Family	Test Case	Result
Discovery	Open TCP Discovery	Pass
Discovery	Open UDP Discovery	Pass
Data Link	Ethernet Random Storm	Pass
Data Link	Ethernet Unicast Storm	Pass
Data Link	Ethernet Broadcast Storm	Pass
Data Link	Ethernet Multicast Storm	Pass
Data Link	Ethernet Grammar	Pass
Data Link	ARP Flood	Pass
Data Link	ARP Grammar	Pass
Network	IP Random Storm	Pass
Network	IP Unicast Storm	Pass
Network	IP Broadcast Storm	Pass
Network	IP Multicast Storm	Pass
Network	IP Fragmentation	Pass
Network	IP Grammar Fuzz	Pass
Network	IP Grammar Fragmentation	Pass
Network	IP Grammar Options	Pass
Network	ICMP Grammar Destination Unreachable	Pass
Network	ICMP Grammar Echo	Pass
Network	ICMP Grammar Echo Reply	Pass
Network	ICMP Grammar Fuzz	Pass
Network	ICMP Grammar Parameter Problem	Pass
Network	ICMP Grammar Redirect	Pass
Network	ICMP Grammar Source Quench	Pass
Network	ICMP Grammar Time Exceeded	Pass
Network	ICMP Grammar Time Stamp	Pass
Network	ICMP Grammar Type/Code Cross Product	Pass
Transport	TCP SYN Floods	Pass
Transport	TCP/IP LAND	Pass
Transport	TCP Grammar Fuzz	Pass
Transport	TCP Grammar Options	Pass
Transport	TCP Grammar Urgent	Pass
Transport	UDP Grammar Fuzz	Pass
Proprietary	Vnet/IP Grammar	Pass
3rd Party	Nessus "Safe Plugins"	Pass

Test Case Descriptions

The Achilles testing procedure is modeled after the generally accepted process used by an attacker when trying to penetrate an unknown system with a specific target or goal. Typically, the goal is to attain information or control of a system of importance. In process control systems, the goal is to attain unauthorized control over the process.

Generally, the process used when moving through each portion of the network, or zone, is as follows:

1. Reconnaissance – Gathering intelligence about a system (such as network addresses, available services, protocols used, credentials, etc)
2. Selection of targets (often includes more refined reconnaissance)
3. Enumeration of possible vulnerabilities on a specific host
4. Exploitation of one or more possible vulnerabilities

Depending on how the network is configured, only part of the network may be visible to an attacker from a particular node on the network. For example, if the attacker is on a node on the Internet, then the corporate firewall limits the attacker's visibility of the organization's internal network. If the attacker is able to gain access to a system behind the firewall then his visibility of the network increases dramatically. As his visibility increases, so does his choice of targets and ultimately empowers him to achieve the desired goal.

Achilles testing focuses primarily on steps one and three of the process described above. Achilles uses Discovery test cases as well as information provided by the Vendor to complete reconnaissance on the target devices. The remaining test cases are focused on enumerating the possible vulnerabilities of the target device, first by attacking each specific layer of its network stack and then by attacking proprietary protocols and application layer software as relevant to the particular device. Each test case family and test case is described in the following sections.

Discovery

The first phase of a test involves discovering particular information about the device under test (DUT). Through proper reconnaissance, testers are able to gain a level of knowledge about the device that would be equivalent to or above that of a deliberate hacker. The information collected in this phase is used to calibrate the test cases to attack services and protocols that are known to be available.

There are very few publicly available tools that will accurately profile process control equipment because these tools are generally focused on all purpose computers. The open source tool Nmap (<http://www.insecure.org/nmap>) is by far the most common scanning utility that is widely available and so is used to accurately expose equipment to traffic it would likely experience if being probed. As Nmap is generally an IT tool, it will often incorrectly identify the operating system or applications (especially proprietary software), but it provides a great deal of useful information about industrial control devices and has even triggered critical errors itself.

Open TCP Discovery

Nmap version 4.1 is used for two purposes in Open TCP Discovery. The first is to perform TCP port scans employing a variety of techniques, including SYN, Connect, ACK, FIN, NULL, Window, Maimon (FIN/ACK) and Christmas Tree scans. The second is to perform TCP-level operating system and application fingerprinting.

Open UDP Discovery

Nmap version 4.1 is used for Open UDP Discovery in a similar manner as it is for Open TCP discovery. Since UDP is a much simpler protocol, it is more difficult to derive information about the device at the UDP level. Along with UDP port scans, Nmap is also used for version scanning at the UDP level as it helps to discriminate between truly open ports and network stacks that are not exactly conformant to the UDP protocol.

Data Link

Data link level protocols provide the interface between network hardware and the DUT's network protocol stack. The Achilles hardware is designed primarily to support testing of Ethernet (IEEE 802.2/802.3) –enabled devices, although other data link types have been tested. The Achilles test suite includes support for the Address Resolution Protocol (ARP) as well, which is used by many different data link protocols and network technologies.

At the Ethernet level, we begin by examining the Denial of Service (DoS) potential of the DUT for various types of Ethernet traffic. We then move on to specific attacks, followed by a grammar-based examination of the DUT's ability to handle malformed IEEE 802.2 and IEEE 802.3 Ethernet frames.

The DUT's Address Resolution Protocol (RFC 826) implementation is used to associate network layer protocol addresses with data link layer addresses. Achilles examines ARP via a common attack known as flooding, and also grammar testing which observes the device's behavior in response to malformed packets.

Ethernet Random Storm

This test is designed to determine the DUT's ability to maintain legitimate communication under deteriorating link conditions most likely caused by a virus or malfunctioning device. This test case involves generating large numbers of random Ethernet frames to saturate the communication link between the DUT and VCS.

With a randomized destination MAC address, the DUT's network interface card should ignore almost all of the traffic. Few or none of the transmitted random Ethernet frames contain a destination MAC equal to the DUT's network interface card. As such, there is very little software or network stack processing cost incurred by the DUT during this test; the point of failure is the link itself.

Ethernet Unicast Storm

This test is designed to determine the device's ability to maintain legitimate communication under deteriorating link conditions most likely caused by a legitimate attack. This test case involves sending large numbers of frames directed at the DUT. With a targeted destination MAC address, the DUT's network interface card must accept and process all traffic. The DUT's processing costs during this test are considerably higher than those of the Random Frame Ethernet Storm but similar to those of Broadcast Frame Ethernet Storm and Multicast Frame Ethernet Storm.

The ability of a network interface card to handle frames may vary with the size of the frames. In order to examine this, the frame size of the transmitted packets varies but is limited to no larger than the maximum frame size parameter specified during the test. Several runs of this test were done at varying frame sizes and traffic rates to examine the DUT's Ethernet frame handling ability.

Ethernet Broadcast Storm

This test is designed to determine the device's ability to maintain legitimate communication under deteriorating link conditions most likely caused by a legitimate attack. This test case involves sending large numbers of broadcast Ethernet frames to the DUT. Since by default the device must accept and process all broadcast traffic, the DUT's processing costs during this test are considerably higher than those of the Random Frame Ethernet Storm but similar to those of Unicast Frame Ethernet Storm and Multicast Frame Ethernet Storm.

The ability of a network interface card to handle frames may vary with the size of the frames. In order to examine this, the frame size of the transmitted packets varies but is limited to no larger than the maximum frame size parameter specified during the test. Several runs of this test were done at varying frame sizes and traffic rates to examine the DUT's Ethernet frame handling ability.

Ethernet Multicast Storm

This test is designed to determine the device's ability to maintain legitimate communication under deteriorating link conditions most likely caused by a legitimate attack. This test case involves sending large numbers of multicast Ethernet frames. Since by default the device must accept and process all multicast traffic, processing costs during this test are considerably higher than those of the Random Frame Ethernet Storm but similar to those of Unicast Frame Ethernet Storm and Broadcast Frame Ethernet Storm.

The ability of a network interface card to handle frames may vary with the size of the frames. In order to examine this, the frame size of the transmitted packets varies but is limited to no larger than the maximum frame size parameter specified during the test. Several runs of this test were done at varying frame sizes and traffic rates to examine the DUT's Ethernet frame handling ability.

Ethernet Grammar

The Ethernet Grammar checks for improper handling of Ethernet frames with header fields that are either malformed or have edge case values. An edge case value is one that borders on the limit of permitted values for that field in the header. IEEE 802.2 and IEEE 802.3 standard frames are constructed with each frame having a single malformed or edge case value in a field. These frames are then sent to the DUT.

ARP Flood

ARP implementations include a finite-sized cache of IP/MAC address combinations. ARP flooding involves sending large numbers of unsolicited ARP replies onto the network in an attempt to fill this cache with invalid entries. Historically, many devices accept unsolicited ARP replies and will cache them regardless of their source.

ARP Grammar

The ARP grammar examines the device's handling of ARP packets that have either malformed or edge case field values.

Network Layer

Network layer protocols are responsible for interconnecting network segments as defined at the data link layer. The Achilles test suite currently includes support for two network layer protocols, the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP).

The DUT's Internet Protocol (RFC 791) implementation is examined via Denial of Service attacks for all IP traffic types, specific attacks against IP state and form, as well as grammar-based test case generation. DoS attacks at the IP level examine resource exhaustion on the DUT.

The DUT's Internet Control Message Protocol (RFC 792) implementation is examined for reliability and stability. There were no ICMP DoS tests conducted. Each ICMP message has a different header structure and will be discussed in the corresponding test cases.

IP Random Storm

This test is designed to focus on the device's ability to handle large amounts of random IP traffic. Specifically, the test focuses on determining if the DUT has any issues handling large amounts of IP traffic not addressed to the DUT. This traffic pattern might be seen if the destination MAC address is broadcast or the device is listening in promiscuous mode. The IP layer of the DUT's network stack should drop every frame since the destination IP address will not match, but some stacks may have trouble processing an excessively high packet rate.

The ability of a DUT's IP stack to handle high rates of IP traffic may vary with the size of the frames. In order to examine this aspect the frame size of the transmitted packets varies but is limited to no larger than the maximum frame size parameter specified during the test.

IP Unicast Storm

This test is designed to focus on the device's ability to handle large amounts of traffic addressed to its IP address. Specifically, the test focuses on determining if the DUT has any issues handling large amounts of unicast IP traffic. The IP layer of the DUT's network stack will have to process every frame since by default the stack must process IP traffic addressed to it.

The ability of a DUT's IP stack to handle high rates of IP traffic may vary with the size of the frames. In order to examine this aspect the frame size of the transmitted packets varies but is limited to no larger than the maximum frame size parameter specified during the test. Several runs of this test were done at varying frame sizes and traffic rates.

IP Broadcast Storm

This test is designed to focus on the device's ability to handle large amounts of traffic addressed at the IP level to the broadcast address. Specifically, the test focuses on determining if the DUT has any issues handling large amounts of broadcast IP traffic. The IP layer of the DUT's network stack will have to process every frame since by default the stack must process broadcast IP traffic.

IP Multicast Storm

This test is designed to focus on the device's ability to handle large amounts of traffic addressed at the IP level to a

multicast address. Specifically, the test focuses on determining if the DUT has any issues handling large amounts of multicast IP traffic. The IP layer of the DUT's network stack will have to process every frame since by default the stack must process multicast IP traffic.

IP Fragmentation

Fragmentation of IP packets enables the transfer of large blocks of data from the transport layer in a seamless manner. The IP layer on the receiving end of the fragments must reassemble the fragments properly. This Multiple Fragment Test checks the behavior of the DUT's stack when it receives multiple copies of the same fragment.

IP Grammar Fuzz

IPv4 packets have twelve standard header fields not including IP Options. Each of the fields have specific legitimate values for a given communication state. The IP Field Fuzzer grammar checks the boundary conditions of acceptable values for IP header fields.

IP Grammar Fragmentation

Fragmentation is necessary when IP packets are larger than the maximum transmission unit (MTU) of a network segment on which they must traverse. Fragment reassembly uses the IP fragment offset field of the IP header to determine where to place the fragment in the reconstructed packet. IP header flags are used in conjunction with IP offset fields to control fragmentation and packet reassembly.

The IP Fragmentation Grammar Test examines the IP Flags and offset field handling of the DUT.

IP Grammar Options

The IP header has a variable-length field for specifying optional parameters. Proper interpretation of an IP packet with options relies on the IP header length field since the options field can be variable length.

Many of the IP stacks deployed in embedded devices either completely ignore IP options, or they assume that the IP header is of constant length. The IP Options Grammar examines the stack of the DUT for support of IP options.

ICMP Grammar Destination Unreachable

When a device on an IP network attempts to communicate with another device that is not reachable on the network, routers respond by returning an ICMP Destination Unreachable message.

This packet informs the sender of the original packet that it needs to figure out a different route to the system it wants to communicate with. This particular attack attempts to trick the DUT into thinking that the VCS is unreachable by sending it crafted ICMP destination unreachable packets.

ICMP Grammar Echo

The ICMP echo request message is sent to a system in order to quickly check network connectivity between two TCP/IP communication endpoints. An ICMP echo request packet has 6 fields; type, code, checksum, identifier, sequence number, and implementation dependent data portion.

The Echo Request Grammar Test attempts to check the DUT's handling of the edge case values of most of the fields in an ICMP echo request packet.

ICMP Grammar Echo Reply

The ICMP echo reply message is sent to a system in response to an ICMP echo request message. Echo requests and replies are used to quickly check network connectivity between two endpoints. An ICMP echo reply packet has 6 fields; type, code, checksum, identifier, sequence number, and implementation-dependent data portion.

The Echo Reply Grammar Test attempts to check the DUT's handling of the edge case values of most of the fields in an ICMP echo reply packet.

ICMP Grammar Fuzz

The ICMP protocol has a variety of other message types that are not covered by the specific ICMP grammar invocations. The ICMP Fuzz Grammar test does a basic fuzz of standard ICMP fields to check the device's handling of edge case values and non-standard message types.

ICMP Grammar Parameter Problem

The ICMP parameter problem message is sent to one device by another in order to inform the device that the packet that it was trying to send has a problem with one or more of its packet header fields. An ICMP parameter problem packet has 6 fields; type, code, checksum, pointer, unused 16 bit field, and the IP header plus eight bytes of data from the undeliverable packet.

The ICMP Parameter Problem Grammar test attempts to check the DUT's handling of the edge case values of most of the fields in an ICMP parameter problem packet.

ICMP Grammar Redirect

The ICMP redirect message is sent to a device by router in order to inform the device that the packet that it was trying to send should have been directed to another system. An ICMP redirected packet has 5 fields; type, code, checksum, IP address, and the IP header plus eight bytes of data from the misdirected packet.

The ICMP Redirect Grammar test attempts to check the DUT's handling of the edge case values of most of the fields in an ICMP redirect packet.

ICMP Grammar Source Quench

The ICMP source quench message is sent to a device by router in order to inform the device that the router is currently under heavy load and that the packet should be rerouted to its target using a different router or rate of communication should be slowed down. An ICMP source quench packet has 5 fields; type, code, checksum, an unused 32 bit field, and the IP header plus eight bytes of data from the misdirected packet.

The ICMP Source Quench Grammar test attempts to check the DUT's handling of the edge case values of most of the fields in an ICMP source quench packet.

ICMP Grammar Time Exceeded

The ICMP time exceeded message is sent to a device by a router in order to inform the device that the time-to-live field in a packet it was trying to send has reached zero. When a time-to-live field in an IP packet reaches zero the packet is no longer considered routable or active. An ICMP time exceeded packet has 5 fields; type, code, checksum, an unused 32 bit field, and the IP header plus eight bytes of data from the misdirected packet.

The ICMP Time Exceeded Grammar test attempts to check the DUT's handling of the edge case values of most of the fields in an ICMP time exceeded packet.

ICMP Grammar Timestamp

The ICMP timestamp request message is sent to one device from another in order to request the targeted device reply with its current timestamp via an ICMP timestamp reply. This system is an easy way for two hosts to synchronize time. An ICMP timestamp request packet has 8 fields; type, code, checksum, identifier, sequence number, and then three timestamp fields. An ICMP timestamp reply message has the exact same field structure.

The ICMP Timestamp Grammar test attempts to check the DUT's handling of the edge case values from most of the fields in both the ICMP timestamp request and reply messages.

ICMP Grammar Type/Code Cross Product

All ICMP packets have a standard packet structure with four basic fields; ICMP Type, ICMP Code, Checksum, and data. Not all of the ICMP type and code combinations are valid messages. When an ICMP packet comes in, the network stack will parse the packet's header to determine what type of ICMP packet it is and then hand the packet off to a handler routine for that type of packet. This attack checks the DUT's ICMP stack support for mishandling of ICMP packets with types and codes that are not typically implemented.

Transport Layer

Transport layer applications are responsible for delivering data to and from specific applications and services on the target device. The Achilles test suite includes support for the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

The DUT's Transmission Control Protocol (RFC 793) implementation is examined via a SYN Flood Test (a DoS attack) to determine the maximum number of connections supported. Following the SYN Flood test, specific TCP protocol attacks are conducted on protocol state and packet format.

The DUT's User Datagram Protocol (RFC 768) implementation was checked for correctness using Achilles' grammar-based test case generation system.

TCP SYN Flood

A TCP connection between a client and server requires a three-way handshake in order to establish communication. The three-way handshake starts with the client sending a Synchronize (SYN) packet to the server to indicate its interest in communicating with it. If the host offers a service on the port indicated in the initial SYN packet, it responds with a Synchronize-Acknowledge (SYN-ACK) packet. After the server issues the SYN-ACK packet, the connection

is said to be in a pending state because the server must wait for the final ACK packet from the client before the connection is fully established. When the client receives the SYN-ACK the TCP protocol states that it must respond with an Acknowledge (ACK) packet thus establishing the communication link.

The server must keep track of pending connections until it receives the final ACK packet and the connection is fully established. Some TCP stacks may only be able to process a single pending connection while others maintain a finite queue of pending connections. The SYN Flood attack attempts to fill this queue and prevent any new connections from being established by not sending the final ACK of the three-way handshake.

TCP/IP Land Attack

A Land Attack consists of sending crafted TCP/IP packets to an open port on a target device. The crafted traffic has the source IP address equal to the destination IP address equal to the IP address of the DUT and has the TCP source port equal to the destination port.

TCP Grammar Fuzz

The TCP protocol has 12 header fields. These fields serve a variety of functions and can contain a variety of values. The TCP Fuzz Grammar test does a basic fuzz of standard TCP fields to check the DUT's handling of edge case and bad field values.

TCP Grammar Options

TCP Options may or may not appear in TCP packets; there may be zero or more options. Many TCP stacks within embedded devices either completely ignore TCP options and just skip them, or they assume that the TCP header is of constant length. The TCP Options grammar examines the DUT's TCP stack for proper support of TCP options.

TCP Grammar Urgent

One of the many TCP flags is the urgent data flag. This flag was used in the past to indicate to TCP/IP stacks that the data in the packet should be given priority processing (i.e. it is urgent). The urgent data pointer is used to point to the data in the TCP stream that corresponds to the urgent data. A mechanism such as this works well when a network administrator can control all of the traffic and no "unauthorized" packets can have their urgent flag set. Attackers do not play by those rules. Some TCP/IP implementations have been found to give preferential treatment to TCP data with the urgent flag set. The TCP Urgent Grammar Test checks for this data processing vulnerability.

UDP Grammar Fuzz

A UDP datagram has four header fields. The UDP Grammar test does a basic fuzz of standard UDP fields to check the DUT's handling of edge case values with various payload sizes.

Proprietary Protocols

Proprietary protocols serve a large number of functions in process control networks, from application layer services such as MODBUS TCP to complete replacements of the standard TCP/IP protocol suite. Often, they use some portion of the TCP/IP suite and replace specific functions within the suite to better suit the requirements of the system.

Vnet/IP Grammar

The Vnet/IP protocol test grammar is a software module that produces automated test cases for the Real-time Ethernet Vnet/IP data link protocol as specified in IEC/PAS 62405 Ed.1.0. The test cases are designed to discover vulnerabilities in Vnet/IP protocol implementations as well as interoperability issues with the lower protocol layers. To maximize test coverage, each test case is composed of two major segments: a Vnet/IP Protocol Data Unit (PDU) and a transport method, which may be tested separately or together. The Vnet/IP PDU contains a Vnet/IP header and all subsequent payload data. The transport method consists of the lower-layer protocols used to transport the Vnet/IP PDU from Achilles to the DUT. Each test PDU includes a DLPDU Header and a DLPDU body of various formats depending on the message type indicated in the DLPDU Header.

All DLPDU message formats specified in IEC PAS 62405 Ed.1.0 as well as undocumented DLPDU body types observed during live testing were investigated. Messages containing Yokogawa proprietary data in the DLPDU body were observed during testing, but were not covered as they were outside the scope of this test. All other fields in the DLPDU header and bodies were given a set of invalid, valid, and edge-case values to facilitate optimal coverage.

3rd Party Tools

A major motivation for addressing system and device security in the process control industry is that process control networks have increasingly been connected to IT and public networks (intentionally or not). While the current generation of publicly available security tools is not particularly effective for attacking or taking control of process control equipment, they will often be employed automatically by viruses and worms or by attackers who came across the target by accident and are unaware of what they are actually attacking.

Because this threat exists, it is critically important that the DUT can survive being scanned by these common tools. Further, while freely available tools may not be capable of successfully taking control of process control equipment today, the history of IT network security suggests that it is simply a matter of time before these tools are modified and made effective in these now accessible process control environments.

Nessus Plugins

Nessus by Tenable Networks (<http://www.nessus.org>) is a network vulnerability scanner that has been available for many years and is a common utility employed by attackers and penetration testers for discovering possible vulnerabilities in target systems on IT networks. Nessus includes over 13,000 individual plugins that are designed to scan for vulnerabilities in many operating systems and applications. While Nessus generally does not include SCADA-specific plugins (although this is starting to change), it is expected that all networked equipment should be able to withstand a Nessus scan.



wurldtech
— security technologies —

WURLDTECH SECURITY TECHNOLOGIES

SUITE 208 - 1040 HAMILTON STREET
VANCOUVER BC CANADA
V6B 2R9

TOLL FREE

TEL
FAX
EMAIL
WEB

1 877 369 6674

604 669 6674
604 669 2902
INFO@WURLDTECH.COM
WWW.WURLDTECH.COM