The Value of Bi-directional Countermeasures

Joseph J. Januszewski, III, CISSP
North American Electric Reliability Corporation

ICSJWG Journal Submission

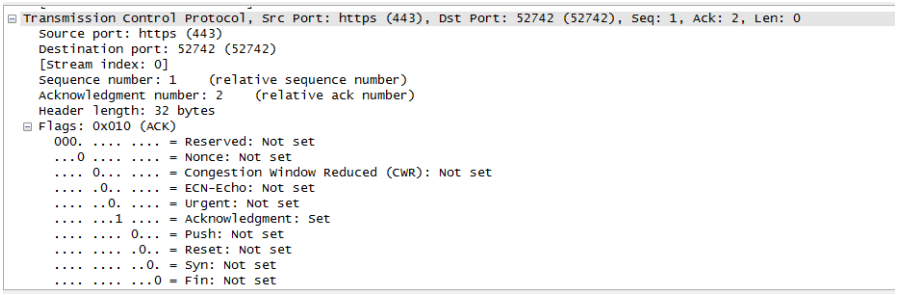
Introduction

A recent informal survey conducted by the author using various power sector technical publications and security journals revealed a serious problem that is occurring in border defenses: data exfiltration. This problem is occurring in various sectors. Several DHS ICS-CERT advisories have been written to advise the critical infrastructure community to protect specific resources. A common thread in complaints seen in the cyber community relate to how firewalls can fail an organization. The problem may not be the firewall, necessarily, but the configuration of the security policy. This is not to say that firewall products have not, overall, retained a currency and a relevance in light of a changing threat environment, based upon recent (and some not-so-recent attacks.) These attacks are leading many to declare the network firewall "dead" as a defensive tool. The author posits that in his experience, the under-utilization of creative and stringent policies and inadequate security architectures contribute to the ease with which attackers can successfully breach defenses.

"Statefulness" and the Vulnerability of Predictability in TCP/IP

While it is commonly viewed as a failure of the firewall architecture, or that of a particular product, the design of the TCP/IP protocol suite bears the responsibility in the predictability of state variables. To an extent, this is a necessary evil, as the mechanism of state must be known to both the sender and the receiver to correctly reassemble packets to ensure that application data is correct and consistent. One of the two protocols used for movement of applications and data in the TCP/IP protocol suite is the Transmission Control Protocol (TCP), which is known as the "stateful" protocol; the other being the User Datagram Protocol, which is state-less.

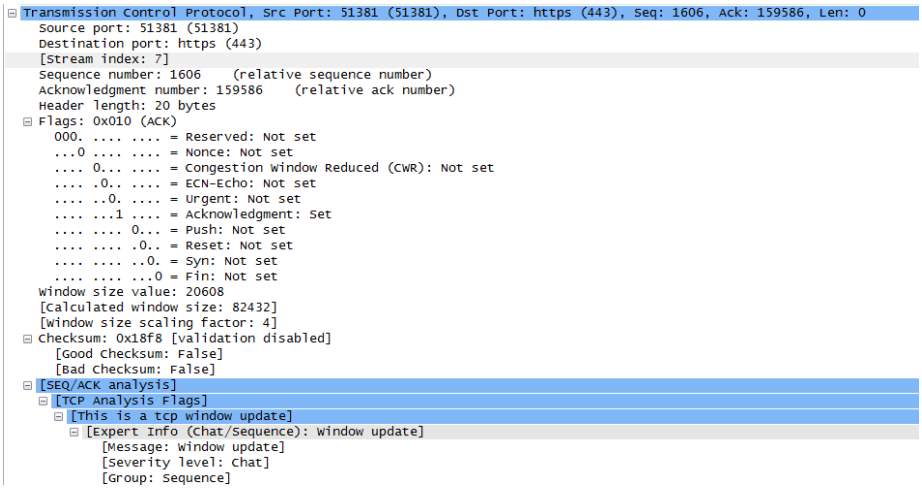
The control information maintained in TCP is used by software (such as security software and network firewalls), and is relied upon to determine the *state* of a session. Due to the process of TCP's "three-way-handshake", it is necessary for security software and network firewalls to maintain a table indicating whether a connection through the software or device is active. The "three-way-handshake" consists of the initial set-up of a TCP connection, including the three-step communication in which the SYN, SYN and ACK and ACK flags are set between the sender and receiver. Other parameters necessary to the communication include the Maximum Transmission Unit (MTU) size of the network path, and the "window" size of data transmitted and received by both systems. The session negotiation sequence validates the stateful connection between the two network end-points. An initial TCP connection is shown in Figure 1, below. [1] [2]



TCP Example

Fig. 1

Just as the flags and window sizes are vital to TCP connections, so is the manner of recognizing the loss of data and determining a mechanism for restoring it for the receiving device. This mechanism is accomplished by the use of TCP source and destination ports, as well as sequence and acknowledgement numbers, which are stored in state tables, or routing tables (also known as translation, or XLATE, tables.) The information in these tables varies with the type of device, however, stateful firewalls use all four datagram fields to determine the state of TCP traffic. So-called "Next Generation" firewalls also introduce varying levels of application-layer analysis, depending on the individual product.



TCP Datagram State Information

Fig. 2

This does not mean that as a state-less protocol, the User Datagram Protocol (UDP) can't be used in attacks. In the following example, a sample rule in the Snort intrusion detection system was posted on the SANS ISC InfoSec Forum, as the initial attack probe utilized UDP [3]:

```
alert udp any 4000:5000 -> any any (msg:"Witty Initial Traffic";

content:"|29202020202020696e73657274207769747479206d6573736167652068657265|";rev:1;)
```

Real-World Exploitable Vulnerabilities

The vulnerability of statefulness in network firewalls mirrors that of TCP/IP itself. The venerable communications protocol is now nearly ubiquitous, even being adopted by control system developers as a replacement, or at least as an augmentation, to existing control protocols. The very mechanism used to provide statefulness becomes a vulnerability, as software can potentially execute Man-in-The-Middle (MITM) attacks based upon known state conditions. The following provides a short list of observed vulnerabilities in the control system space based upon the implemented TCP/IP protocol stack.

IP forwarding vulnerability

Advisory ICSA-15-244-01 illustrates the potential for Virtual Local Area Network (VLAN) isolation to be circumvented, permitting communications with devices in another VLAN if the same IP addresses are configured on both VLANs. [4]

TCP predictability vulnerability

Advisory ICSA-15-169-01A contains a TCP predictability vulnerability in ICS Devices that exists through the use of a real-time operating system used in various vendors' remote transmission units, or RTUs. [5]

TCP initial sequence vulnerability

In advisory ICSA-15-153-01, researchers identify a TCP initial sequence number vulnerability in two digital voltage regulator controllers. In response to the reported vulnerability, the manufacturer also identified four similarly affected devices with this vulnerability. Successful exploitation of this vulnerability could result in a denial-of-service condition, or session hijacking. [6]

Predictable TCP initial sequence vulnerability

In advisory ICSA-15-041-02, researchers identify a predictable TCP sequence vulnerability in a manufacturer's device. Successful exploitation of this vulnerability could result in manipulation or spoofing of TCP connections, and could result in a denial-of-service condition for the device, or transmission of inaccurate data regarding developing fault conditions in equipment, such as transformers. [7]

Additionally, in Internet CERT Vulnerability Note VU#498440, researchers posit that "As of 2015, predictable TCP ISN generation is still somewhat common, particularly in low-power/low-bandwidth, embedded, and IoT devices that use older operating systems and networking code." [8]

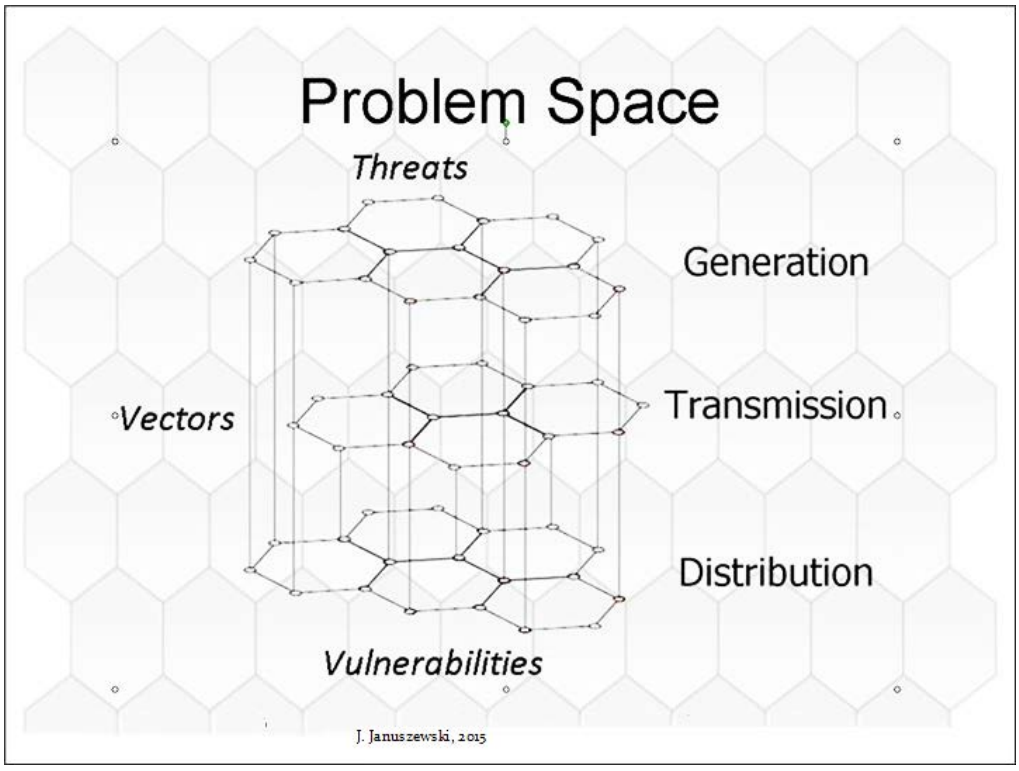
Holistic Network Security

Based upon the inherent vulnerabilities and design flaws of the current TCP/IP Internet protocol suite, looking beyond simply adding more firewall rules to limit outbound network traffic, entities in all sectors must do a better job at building a multi-layer defense-in-depth posture inside the network border and within the interior of the network.

In February 2015, the ICSJWG reported the following most common methods used by attackers to access control system networks:

- Unauthorized access and exploitation of Internet facing ICS/Supervisory Control and Data Acquisition (SCADA) devices;
- Exploitation of zero-day vulnerabilities in control system devices and software;
- Malware infections within air-gapped control system networks;
- SQL injection via exploitation of web application vulnerabilities;
- Network scanning and probing;
- Lateral movement between network zones;
- Targeted spear-phishing campaigns; and
- Strategic web site compromises (a.k.a., watering hole attacks). [9]

Figure 3 below illustrates the three-dimensional problem space used by the author to demonstrate the various facets of the security model in the electric utility sector. This model also parallels the gas industry space, as well.



Electric Sector Security Problem Space
Fig. 3

Addressing these attack methods requires:

- increased network controls,
- network redesign,
- increased physical controls and authentication mechanisms,
- programmatic controls and sanitization of input data, and
- user education.

Internal network architecture and increased controls relies on using network segmentation with systems located in isolated private VLANs controlled by multiple layers of firewalls. A "flat" network architecture in any type of environment creates a space with contiguous addresses and less control points to mitigate the spread of a malware infection. The use of multiple private VLANs with various address subnets in conjunction with several layers of firewalls creates an environment that is more difficult for malware to traverse and spread. These controls create a logical network defense-in-depth posture that make migration through a network difficult for worms. Used in conjunction with other system-level techniques discussed below, a segmented, hierarchical network architecture creates a more-secure environment.

> Entities in all sectors must do a better job at building a multi-layer defense-in-depth posture inside the network.

Historically, control system and information system (now cyber system) security viewed networks and resources simply as "inside" and "outside". However, separating business and control networks is essential, as the *Microsoft Security Intelligence Report 18* indicates: there are between 5,000 and 6,000 new vulnerabilities reported every year. Many of these vulnerabilities affect not only user applications such as office productivity software, but other more specialized software, as well, and those same vulnerabilities can be used to access control systems. [10]

A better way of viewing network traffic is as *in-bound* and *out-bound* at various control points. This view-point provides a good way of imagining the traffic that enters a subnet through a link or port – sometimes referred to in control networks as "zones" and "conduits". In-bound traffic controls should implement the following:

- network profiling: knowing what type of traffic is "normal",
- host intrusion prevention,
- system-level policy controls,
- intrusion protection systems,
- white-listing and black-listing applications and file signatures: aiding in spear-fishing,
- dynamic file analysis and sandbox technologies, and
- additional application- and file-based controls.

Out-bound traffic controls, likewise, should implement:

- network profiling: knowing what type of traffic is "normal",
- URL controls: preventing access to rogue websites,
- dynamic file analysis and sandboxing: exfiltration tracking and prevention, and
- outbound firewall policies.

Virtual Private Networks (VPNs) must be implemented for remote access control. A single layer of SSL or TLS encryption is no longer enough. Another down-side of encryption is that it can be "weaponized" and used by malware to also blind the network owner; it can also become a form of "Trojan horse" if authentication is inadequate, and user access sessions are high-jacked by attackers.

The viewpoint of many that network firewalls do not belong in control system networks due to latency should be reminded that in internal control networks, firewalls should be sized to the environment. Sometimes, this requires the introduction of telecomm "carrier-grade" equipment. It should also be kept in mind that proper segmentation of control networks away from office and corporate networks will limit superfluous traffic that must be filtered out of control networks to provide a better security posture and should not even reach control system firewalls in the first place. The ISA99 group of the International Society of Automation is responsible for developing the ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) security. Network segmentation is recommended in ISA/IEC 62443-3-2: "Security Risk Assessment and System Design".

Proper segmentation of control networks away from office and corporate networks will limit superfluous traffic.

BlackEnergy 3 and Beyond

The third version of the BlackEnergy malware focuses on ICS, more so than the two previous versions. Nearly a year ago, the DHS ICS-CERT issued ICS-ALERT-14-281-01B Ongoing Sophisticated Malware Campaign Compromising ICS (Update B). [11]

An HMI system should NEVER be permitted to access the outside Internet for configuration or updates. Access should be blocked by network security resources as close to the server as possible, but at the very least, access should be blocked by the border firewall. The reason for this is that if access is permitted to go outside the control system network, the HMI could access, in the instance of BlackEnergy 3, a rogue system to download a hacked version of software, or a control file. Some are of the opinion that the same rule on more than one level of firewall is needlessly redundant. This is the farthest from the truth. Redundancy in security is vital. If an HMI needs to access control systems on a remote network, access should be made through an authenticated, encrypted link such as through a VPN, and not in an unprotected manner over the public Internet. Some have suggested that so-called "air-gaps" are without merit, as shown by the attack vector used by Stuxnet. The concept of defense-in-depth is counter to the implementation of only a single line of defense to stand between the system and the outside world. This is even more evident in terms of physical attacks against distribution and transmission resources. [12] [13] [14]

An HMI system should NEVER be permitted to access the outside Internet for configuration or updates.

Consequences of the "Internet of Things"

It is now commonly known that at some point in the not-too-distant future, advanced wireless devices – both infrastructure and personal mobile devices – will become widely-used in critical infrastructure. As much as the wireless device phenomenon has affected the consumer market, it will also affect the industrial control community, and is already seeing wide acceptance in the freight logistics space. The first application in the energy sector has been in the use of Automated Metering Infrastructure (AMI). This new networking paradigm has caused some to proclaim that "the firewall is dead". The security of devices (such as those on poles and towers) in the distribution and transmission systems has always been viewed as a physical security issue. Added intelligence and communications capabilities have the potential to make them even higher-value targets; and the need for encryption and advanced physical protection methods to protect command and communications operations and traffic has never been greater. The industrial community must be ready to respond to these threats and protect itself accordingly.

Conclusion

Exfiltration of data and the potential to pull down rogue configurations from outside a control network are major concerns in today's environment. By using existing network security resources, these threats can be greatly reduced by employing outbound policies, not only at border firewalls, but also on internal firewalls. Architecting a control system network requires the elimination of the fallacious border-only, "hard-and-crunchy-on-the-outside, soft-and-chewy-on-the-inside" network security posture.

The position in many areas of security that pose the question: "Do we have a firewall?" is typically met with the answer "Yes", and a check is placed on a security form. Complex security policies, network segmentation and in-depth inspection of applications, files and protocols are required to meet the security of complex operations of control systems and the servers that they depend on for control, HMI and historian functions. Firewall policy configuration can be viewed as drudgery. But, the simple truth is that denying paths into - and out of - a control system network can prevent some of the most damaging examples of network intrusion.

While threats such as zero-day attacks, rootkits specifically-designed for control systems, and rogue software containing an ID signed by a trusted authority pose hazards; and since patch management has too long of a horizon, compensating controls are the next best alternative. While a worm like Stuxnet showed that air-gapped networks are not absolutely secure, better managing the control system environment, and realizing that there is no such thing as "absolute security" is paramount. This also highlights that the most effective defense for social engineering attacks, such as spear-fishing, is still user education. [15]

The way to succeed is in using the full spectrum of available security technologies. There is no success in half-measures. As Winston Churchill said: "The era of procrastination, of half-measures . . . is coming to its close. In its place we are entering a period of consequences."

Author's Note: This article is provided as an informed opinion, and is not intended to provide procedural guidance under NERC policies.

References

[1] Comer, Douglas E., Internetworking with TCP/IP Volume One, 6th Ed., Pearson, 2013. ISBN-13: 978-0136085300.

[2] Information Sciences Institute, University of Southern California. "RFC 793: TRANSMISSION CONTROL PROTOCOL". September 1981.

[3] https://isc.sans.edu/forums/diary/ALERT+Black+Ice+Worm/144/

[4] https://ics-cert.us-cert.gov/advisories/ICSA-15-244-01

[5] https://ics-cert.us-cert.gov/advisories/ICSA-15-169-01

[6] https://ics-cert.us-cert.gov/advisories/ICSA-15-153-01

[7] https://ics-cert.us-cert.gov/advisories/ICSA-15-041-02

[8] "Multiple TCP/IP implementations may use statistically predictable initial sequence numbers". Vulnerability Note VU#498440. CERT, Software Engineering Institute, Carnegie Mellon University. Original Release date: 13 Mar 2001, Last revised: 20 Oct 2015. Retrieved 14 Nov 2015 https://www.kb.cert.org/vuls/id/498440

[9] https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

[10] http://download.microsoft.com/download/7/1/A/71ABB4EC-E255-4DAF-9496-A46D67D875CD/Microsoft_Security_Intelligence_Report_Volume_18_English.pdf

[11] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

[12] http://cyberx-labs.com/wp-content/uploads/2015/05/BlackEnergy-CyberX-Report_27_May_2015_FINAL.pdf

[13] http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-134508.pdf

[14] http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

[15] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf