White Paper

Cyber Security Solutions for Power Utilities

June 2015

RAD

Your Network's Edge

Abstract

This white paper explores the variety of challenges that arise when securing power utility operational technology networks. It addresses the limitations of current solutions and proposes new technologies to deal with numerous vulnerabilities inherent in the communications network.

Contents

1 Introduction

Power utility control networks, also known as operational technology (OT) networks, have always been inherently different from information technology (IT) systems. While a portion of the power utility network is in fact reserved for corporate and traditional data communications, the bulk of its infrastructure is dedicated to communicating with power utility equipment using various SCADA protocols.

From the very beginning, power utility networks were designed solely for control purposes and to provide operators with information on what was happening in the power grid. Cyber security was not even a distant consideration, as at that time cyber attacks were practically unheard of. Even as OT networks evolved to support today's modern power grids, operators continued to maintain minimal security of their operational communications infrastructure.

Finally, the beginning of the twenty-first century brought about a newfound awareness of the potential damage that cyber attacks could cause to critical infrastructure. This in turn resulted in more attention given to the security of critical networks. The first such binding regulation was the North American Electric Reliability Council (NERC) Critical Infrastructure protection (CIP) set of requirements that were introduced in 2008. Still, at the time, cyber security was viewed primarily in terms of its traditional roots – as an IT-type risk – and was treated as such in terms of threat mitigation.

1.1 Traditional Defenses

The traditional doctrine for securing IT devices focuses on two basic elements:

The first is an **anti-virus**, which is simply a software running on a PC. Anti-virus software uses a combination of heuristics patterns, along with other patterns or "signatures". Together, they allow the PC to identify malicious software running on the infected machine.

The second element is the **firewall**. The security mechanism of early firewalls was based on pre-determined knowledge of applications, network relationships between applications and the establishment of an enforcement mechanism for these relationships. As such, it allowed communication only between devices with pre-approved source and destination IP addresses. In more advanced firewalls, a Deep Packet Inspection (DPI) software engine created a firewall/anti-virus hybrid that can check characteristics of the data passing through the firewall.

1.2 New Packet Technology

Over time, traditional SONET/SDH/PDH networks (which utilities have been using for years) are gradually being replaced with new packet technology. The reasons behind this trend are outside the scope of this paper, but it's worth noting that the transition greatly increases the risk of cyber threats directed at critical infrastructure.

Due to their static nature, traditional SONET/SDH networks with dedicated connections are less susceptible than packet technology to cyber attacks. In the latter, traffic is capable of dynamically reaching any point in the network using IP addressing.

1.3 Security by Obscurity

Industrial equipment vendors have long shared the common philosophy that systems would remain immune to cyber attacks as long as they kept secret the interface and communication protocol that composed their equipment. They confidently reasoned that without a detailed specification, attackers would be unable to communicate with the equipment (and most likely, would not even bother to try). Many agreed that this approach would block any possibility of cyber attacks on devices or networks. While this may partially be true, the growing use of standard hardware, software and protocols has rendered this approach ineffective.

2 Vulnerabilities of the Industrial Control Network

As noted in the Introduction, the main distinction of the power utility OT network lays in its use of Supervisory Control and Data Acquisition (SCADA) protocols. Loss of communications between remote sites and the SCADA control center could quickly trigger an event with widespread consequences for days, weeks or possibly months. For this and many other reasons, the security of the communications network is critical. The following section examines the main vulnerabilities of such networks, as well as the current defenses being employed to protect them.

2.1 Vulnerabilities of RTUs and SCADA Equipment

Industrial devices and protocols were designed primarily with operational safety and reliability in mind. Security was not considered a top priority and the type of defense employed was, at best, "Security by Obscurity". Consequently, earlier versions of the leading SCADA protocols (DNP3 in North America and IEC-60870-5-101 in Europe) did not have robust mechanisms for source address authentication or validation of message integrity. The 2010 discovery of the STUXNET virus was a painful reminder of this particular vulnerability. The STUXNET malware code sent erroneous and malicious commands to a Siemens PLC, which eventually caused a SCADA system malfunction, resulting in significant damage to the centrifuge equipment. Due to the critical nature of the industrial operations, maintenance managers often refrain from making modifications, such as upgrading an older-generation operating system, updating an anti-virus, or keeping it current with updated security patches. As a result, there are many known security holes that are not patched or otherwise addressed in RTUs, other industrial equipment and SCADA servers that are based on standard operating systems.

2.2 Vulnerabilities of the OT Network

One rarely discussed aspect of security vulnerability analysis is the underlying network technology. Since legacy networks were seldom attacked and more modern networks are mostly protected only to a small degree – the OT network was not well defended against cyber threats. There are two major vulnerabilities that can be associated with the network layer:

- **Attacks on the network control plane** – the control plane (also known as "signaling plane") is the set of functionalities that prepare and maintain the data plane, including finding paths through the network (routing), setup and release of connections, protection switching, etc. Some of today's packet networks have a control plane intended by protocol designers as a way to streamline circuit provisioning. While this aspect of the network succeeds in making circuit design part of the network, it also introduces a huge vulnerability. The ability to dynamically assign destinations with protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) creates the opportunity to both corrupt and disable the network. By simply disseminating malicious information, an attacker can create routing rings or other harmful actions, which could result in the entire network crashing. In protocols such as IP, Multiprotocol Label Switching (MPLS) and MPLS-TP, a single unsecured node can essentially bring down the network.
- **Attacks on the data plane** – the data plane (also known as "forwarding plane") is the set of functionalities responsible for forwarding packets through the network from source to destination. Denial of Service (DoS) attacks are a classic example of threats that originate in the data plane. Typically, DoS attacks bombard a victim with multiple bogus requests for connection, severely limiting the recipient's resources for handling legitimate requests. DoS attacks are relatively simple to create, and target the very essence of the OT network. Loss of visibility to its RTUs could very quickly result in loss of control of the network and a significant outage. For this reason, DoS attacks are especially dangerous in the internal OT network. Though arguably the most common, DoS attacks aren't the only data plane attacks to represent significant danger. Others involve snooping around network resources and attacking unpatched control stations.

Combined, these two planes of attack represent a major vulnerability. They are dependent on the design and implementation of the network overlay and can be either enhanced or mitigated as a result of network design considerations.

3 Approaches in Defending Against Cyber Security Threats

Several tactics have been employed to mitigate the vulnerabilities of OT networks. As mentioned in the introduction, the current approaches vary, but tend to focus on the IT nature of the network.

3.1 Perimeter Protection

The first set of perimeter defenses aims to separate the OT network from any outside contact. This includes:

- Network firewalls – designed to regulate the exchange of information by allowing contact only between approved entities, network firewalls can approve or reject connection requests as well as check remote users for credentials. Their effectivity is limited, however, since once they permit a connection, they have no notion of the data that passes through. As a result, malware or invalid data can potentially penetrate the system.
- Unidirectional security gateways – these appliances are designed to separate the OT network from incoming requests originating in the corporate network. They allow only a one-way flow of information – from the OT network outward – and eliminate possible exposure of mission critical components to external control.
- Encrypted VPNs – this measure is typically used in conjunction with network firewalls and allows secure communications between system elements residing in the electronic security perimeter (ESP) and the control center. In essence, a secure VPN mitigates "Man in the Middle" attacks.

The limitations of perimeter protection are typically tied to the ease of physical security breaches. While IT networks guard their critical equipment in well-protected locations such as central offices, the control equipment relied upon by utilities often resides in unmanned, lightly protected locations. Here, it's relatively easy to circumvent the network's perimeter security and gain unauthorized access to the equipment within it.

3.2 Network Protection

The underlying architecture for interconnecting locations in the communications network is also a source for potential vulnerabilities in the OT network. While often overlooked, the underlying network technology can have wide ranging implications on the stability and susceptibility of the OT network to cyber attacks. As outlined in the previous chapter, there are several ways to breach network security, including attacks to both the control plane and data plane. There are also several ways in which such threats could be mitigated or limited in a way that would improve network security and resiliency, without affecting its performance.

3.3 Minimizing Control Plane Attacks

Network designs that include a control plane, such as MPLS and IP networks, are highly susceptible to these attacks. While mitigation is possible to an extent, the threat remains as long as control planes exist. Networks technologies operating without a control plane will always be more secure. These include SONET/SDH and Carrier Ethernet networks. Neither SONET/SDH nor Carrier Ethernet offer a means to attack their control plane, and both require a management station to provision them. Once that management station is secured, no control plane attacks are possible.

3.4 Minimizing Data Plane Attacks

Attacks on the data plane are also a potential source of cyber threats. Although these tend to be more specific (e.g. DoS attacks targeting a particular host), the potential loss of connectivity between the SCADA sever and

RTUs can interrupt the control process. Similarly to attacks centered on the control plane, data plane attacks can be mitigated by proper design relating to the OT network.

Where strict connection-oriented networks are involved (as with SONET/SDH or Carrier Ethernet), it is more difficult for an attacker to gain visibility into network elements. In such cases, only the minimum necessary parts of the network are exposed and other, more vulnerable parts are shielded. In routed networks (such as MPLS and IP), an attacker can first collect information by snooping and scouting the network from the outside, and then use spoofed addresses to perpetrate an attack.

Another way to increase security and avoid masquerading or spoofing is through the use of source authentication protocols. The most prominent of these is the Ethernet-based IEEE 802.1X, which validates each newly connected device through a centrally managed database. It uses encryption to verify the identity and ensure the new device is a truly one. This ensures that all devices connected to the network are valid, authenticated network devices and not hacker-inserted ones.

3.5 Internal Application Protection (Malware Protection)

Among the most difficult attacks to detect are those that originate from inside the network. Insider attacks pose a hazard from a number of perspectives. First, it is extremely challenging to determine whether a particular command is valid or malicious. Some commands (e.g. decommissioning of an old RTU) may be valid when issued by authorized personnel, but can be harmful when initiated without permission.

Second, since attacks travel through diverse paths, it is necessary to track all possible paths to secure the entire network. Some utilities use a location-based firewall to mitigate the risk of one site controlling another, as well as to contain cyber threats at their general point of origin.

Finally, it is tough for standard "firewall" equipment to inspect commands. While standard DPI-enabled firewalls can check the message payload to determine if a previously isolated "signature" is present, and flag potential matches, it has no way to evaluate whether a particular command is valid or malicious. All of these limitations present an obstacle when it comes to internal threats, as the NERC CIP expects power utilities to detect and block occurrences where malware has taken over equipment – whether an RTU or a control console – and be able to stop it from performing its malicious task.

In order for a network to cope with all the limitations posed by internal threats, defense solutions must "understand" the ICS protocol and intelligently determine whether a particular command is valid or out of bounds. The distributed ICS-aware firewall, with its ability to determine the validity of SCADA commands, can be integrated into the fabric of the network. It can also block and detect insider threats or threats stemming from the introduction of malware to the network.

Application awareness as a requirement stems from the difficulty associated with detecting malware attacks. Malware typically piggybacks on real control stations and verifiable hosts, and only changes the content of control messages. In order to detect this type of tampering, an external unaffected element must then verify the

content of those communications. The intelligence to read and verify each command is required to enable this functionality, necessitating the use of application aware equipment.

4 Layered Defenses for ICS

As discussed previously, OT networks face a plethora of potential cyber threats. These threats span several vectors of attacks, and each defense strategy comes with its own vulnerabilities. As there is no silver bullet to completely protect the system, a network can be truly secure only when multiple defenses at multiple layers are employed, covering the vulnerabilities introduced by each single defense strategy.

The multi-layering of defense process is called Defense-In-Depth. It focuses not on building a single impervious single wall, but on building multiple defenses. These defenses utilize a mix of measures and tactics to impede the advancement of an attacker and allow the defender to detect and block them. Relative to cyber security, this approach has been used in various contexts. In power utility operational networks, it must be employed at all layers and attack vectors that are relevant to the OT network.

4.1 Defense-in-Depth for ICS Systems

IT infrastructure protection in the form of standard network firewalls and anti-virus software is simply not enough to qualify as a defense-in-depth strategy for ICS. Such an approach addresses only one vector of defense and might be useless if the network is breached, or when an attacker uses malware to issue malicious commands. This is why a multilayered defense strategy is deployed to protect against all attack vectors – especially in a mission critical environment managed by the OT protection network. Within the ICS network, each layer of defense-in-depth protection has both advantages and vulnerabilities. Working together, the combined solution successfully provides protection against:

- Remote attacks from another location. This is achieved by a networking firewall and inter-site encryption. They prevent hackers from gaining “logical” access to the internal networks.
- Man-in-the-middle attacks. This is achieved by inter-site encryption and prevents corruption or tampering of data.
- Network control plane attacks. This is achieved by selecting a security-robust infrastructure like Carrier Ethernet or SONET/SDH in lieu of MPLS or MPLS-TP.
- Masquerading attacks. The defense is achieved through source authentication protocols such as IEEE 802.1X. It verifies that a particular host has not been replaced by another machine that can in turn issue malicious data or attacks.
- Snooping and scouting. This is achieved by using network technology with rigid path definition and universal address space – like Carrier Ethernet.

- Malware attacks from RTUs, control stations or HMIs. This is achieved by the use of distributed application-aware firewalls. These firewalls can review the SCADA protocol to verify that commands are within the bounds of the control or monitoring system, not just that the devices are members of the automation network.

4.2 Multiple Layers

A properly designed ICS network is surrounded by multiple layers of defense, whereby each layer addresses a different type of attack. When one layer filters some of the attack, the next layer protects its vulnerabilities. The underlying ICS network can only be fully secured when all layers function together. Otherwise, each can be attacked and defeated relatively easily.

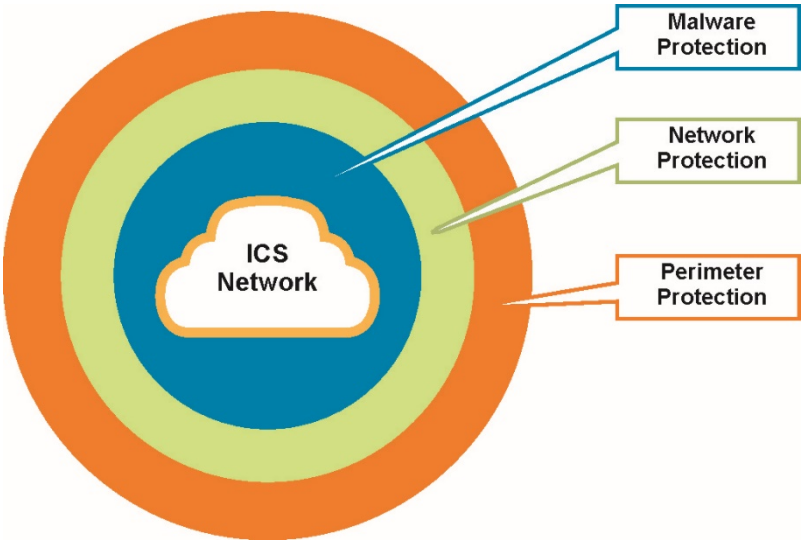

Diagram 1 – Defense-in-Depth of ICS Power Networks

5 Summary

ICS networks are vulnerable to cyber attacks. Not only are they susceptible to the traditional threats common in IT and enterprise networks, they are also exposed to attacks that do not have prevalent defenses. These include malware attacks centered on the ICS control layer. The unsecure physical nature of the OT network, coupled with the existence of unmanned substations, also lends itself to attacks on the underlying network technology.

Most of these attacks can be mitigated and constrained to their initial intrusion vectors by the technique known as Defense-in-Depth. Defense-in-Depth layers a variety of security defenses to protect the different vulnerabilities in the OT network. The multiple layers include the prevalent perimeter defenses along with

network protection and malware protection. The design of the network also plays a critical role in determining that network's vulnerability. A technology such as Carrier Ethernet that is inherently more secure can mitigate major network vulnerabilities. By contrast, technologies such as MPLS can actually amplify existing network vulnerabilities in the current network and permit an attacker to topple the entire network.

Malware protection must be part of a distributed application-aware firewall that can block internal attacks. This final layer of defense can protect against situations where an attacker is able to breach the perimeter network, but unable to attack the network directly.

Ultimately, network security must be seriously considered at every stage of the design, and not only as an afterthought. Such diligent planning can dramatically improve the resilience of the network and reduce expenses tied to securing it.

For information on RAD's cyber security defense-in-depth solutions for power utilities, visit www.rad.com.

www.rad.com

International Headquarters
RAD Data Communications Ltd.
24 Raoul Wallenberg St.
Tel Aviv 6971923 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com
http://www.rad.com

North America Headquarters
RAD Data Communications Inc.
900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100
Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com
www.radusa.com

Your Network's Edge