White Paper

Cyber Security for Power Utilities

A defense primer for the operational network

Motty Anavi
VP of Business Development
RAD
December 2013

RAD

Abstract

This white paper explores the variety of challenges that arise when securing Industrial Control Protocol (ICP) networks in a power utility environment. 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 networks have always been inherently different from traditional corporate networks. While a portion of the power utility network is in fact reserved for corporate and traditional communications, the bulk of its infrastructure is dedicated to communicating with industrial equipment using various SCADA protocols.

From the very beginning, power utility networks were designed solely around the need to provide operators with a picture of what was happening in the power network. Cyber security was not even a distant consideration. In fact, cyber attacks were practically unheard of in the twentieth century industrial environment. Even as networks evolved into today's modern 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 wreak on computers. This in turn resulted in more attention given to the security of critical networks. The first such binding regulation was the NERC CIP set of requirements that were only approved in 2008.

Still, cyber security was viewed primarily in terms of its traditional roots – as an IT-type danger – and was treated similarly in terms of threat mitigation.

1.1 Traditional Defenses

Traditional doctrine for securing IT devices focuses on two basic elements:

The first is "anti-virus", which is simply a type of software running on a PC. Anti-virus software uses a combination of behavior patterns known as "heuristics" along with other patterns or "signatures". Together, they help the PC identify malicious software running on the infected machine.

Second 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 only approved hosts and approved applications to communicate. In later firewall versions, a Deep Packet Inspection (DPI) software engine was added, creating a firewall/anti-virus hybrid that can check characteristics of the data passing through the firewall.

1.2 New Packet Technology

The advent of the twentieth century was also marked by a shift towards replacing traditional SONET/SDH/PDH networks (which utilities had been using for years) with new packet technology. The reasons behind this trend are many and outside the context of this paper, but it's worth noting that the transition greatly increased the risk of cyber threats among power utility networks.

While traditional SONET/SDH technology is not impervious to cyber attacks, it is categorically less susceptible than packet technology, thanks to the static nature of SONET/SDH and the absence of a signaling plane. Plus, the static reach of the network hampers the ability of attackers to traverse between different locations at will.

Packet technology, on the other hand, introduces a myriad of threats by nature. For one, it is capable of dynamically reaching any point in the network through the use of addressing. In addition, some packet protocols and technologies provide a signaling plane that renders them especially susceptible to cyber attacks.

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 communications structures 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 tight-lipped approach would thereby block any possibility of cyber attacks on devices or networks.

2 Vulnerabilities of the Industrial Control Network

As noted in the Introduction, the main distinction of the power utility network lays in its use of Industrial Control Protocols (commonly known as SCADA) in addition to standard corporate communications. While SCADA is not unique to the power industry, it is employed throughout the power network to control mission critical equipment. Loss of communications to that equipment, or even minor tampering in the communications, can quickly trigger a catastrophic event with wide spread power outages lasting days, weeks or possibly months. For this reason, the security of the communications network is critical.

Considering how little thought was put into securing the power utility network in its original design phases, the fact that it's currently riddled with vulnerabilities is no surprise. This section will examine the vulnerabilities inherent in the original, design as well as in the current defenses being employed to protect the network.

2.1 Vulnerabilities of RTUs and SCADA Equipment

Industrial devices and protocols were never designed with security in mind. At best, they employed "Security by Obscurity"-type defenses. Currently, neither of the leading SCADA protocols (DNP3 in North America and IEC-101 in Europe) have mechanisms for source authentication or validation of any of the commands they receive. This vulnerability was demonstrated in Project Aurora, performed in 2007 at the Idaho National Laboratories, in which a group of hackers was challenged to damage a mock power station. The hackers successfully penetrated the mock substation and caused a generator to self-destruct. The 2010 discovery of the STUXNET virus was another painful reminder of this particular vulnerability. Through multiple undocumented security holes in the control console and dedicated PLCs, STUXNET sent erroneous and malicious commands to a Siemens PLC, resulting in its breakdown.

The proprietary characteristics of RTUs and SCADA equipment also pose challenges. Due to the sensitive nature of the industrial equipment's software code, utility operators are often prohibited from making modifications, such as upgrading an older-generation operating system, or keeping it current with updated security patches. As a result, there are many documented security holes that are not patched or otherwise addressed in RTUs or industrial equipment that is based on standard operating systems.

In conclusion, the "Security by Obscurity" approach was debunked many times, not only in the incidents mentioned above, but also more recently in Black Hat conference demonstrations involving remote control of vehicle command systems and insulin pumps.

2.2 Vulnerabilities of the Power Network Communications

One rarely discussed aspect of cyber security vulnerability analysis is the underlying network technology. Since legacy networks were seldom attacked and more modern networks are protected to a small degree – the network was not well-studied in the context of the power utility network.

There are two major vulnerabilities that can be associated with the network layer:

- Attacks on the network control plane – 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 BGP and OSPF creates the opportunity to both corrupt and disable the network. By simply disseminating malicious information, an attacker can cause a network to send its traffic into nowhere, create routing rings, or other harmful actions. Essentially, it gives a single interface the ability to crash the entire network. In protocols that use these signaling protocols, such as IP, MPLS and MPLS-TP, a single unsecured node can essentially bring down the network.

  This is exactly what happened in late 2010 when erroneous routing information from a Chinese ISP caused the Internet to come crashing down. Contributing to the problem was the fact that for power utility networks, the number of physically unsecure locations is usually quite large. An attacker can easily overcome the physical barrier of an unmanned substation, inject malicious information into the network, and bring it completely down.

- Attacks on the data plane –Denial of Service (DoS) attacks are a classic example of threats that originate on the data plane. Typically, DoS attacks bombard a victim with multiple bogus requests for connection, causing the recipient to waste resources and struggle to handle legitimate requests. Sometimes, all resources are exhausted and fail completely. DoS attacks are relatively simple to create, and target the very essence of the power utility network – connectivity. For a power utility, loss of visibility to its RTUs or Teleprotection equipment can very quickly translate into loss of control of the power network and a significant power outage. For this reason, DoS attacks are especially dangerous in the internal operational 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 that can be inherent in the network. 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 operational 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 defenses aims to separate the power operational network from any outside contact. Perimeter defenses include:

- Network Firewalls – Designed to regulate the exchange of information by only allowing contact between approved entities, network firewalls can approve or reject connection requests as well as check remote users for credentials. They are limited in effectiveness, however, since once they permit a connection, they have no notion of the data that passes through. As such, malware or invalid data can potentially penetrate.
- One-Way Network Firewalls – These appliances are designed to provide a "physical" separation of the operational network from user monitoring requests. They allow only a one-way flow of information – from the operational network outward – and minimize the exposure of mission critical components to possible outward control.
- Encrypted VPNs – This measure is typically used in conjunction with network firewalls and allows secure communications between different elements of the Electronic Security Perimeter (ESP). In essence, it prevents "Man in the Middle" attacks and compromises of control information.

The majority of security measures today are derived from the concept of perimeter protection. The limitations of such defenses are typically tied to the ease of physical security breaches. While some networks (e.g. carrier networks) house their equipment in well-protected locations such as central offices, the communications equipment relied upon by utilities often resides in unmanned, lightly protected locations. Here, it's relatively easy to breach physical security and circumvent all of the network's perimeter security. In such cases, it's essential to contain and mitigate the break-in. This is where additional security measures are required.

3.2 Network Protection

The underlying architecture and protocols for interconnection of locations in the communications network are also a source for potential vulnerabilities to the power utility network. While often not considered, the underlying network technology that's selected can have wide ranging implications on the stability and susceptibility of the 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 the data plane. There are also several ways in which such threats could be mitigated or limited in a way that would improve security and resiliency, yet not impact network performance.

3.3 Minimizing Control Plane Attacks

One of the more dangerous types of attacks is one on the control plane, where the attacker either corrupts or crashes it. In either case, the ultimate result is the complete collapse of the network. This type of attack is especially alarming because the breach of just a single location has potential to crash the entire network. Essentially, the entire network is only as secure as its weakest link, and power utility networks are at the mercy of their least protected substation.

Network designs that include a control plane or signaling protocol are therefore highly susceptible to these types of attacks. These include MPLS and IP type networks. Control plane vulnerabilities have been demonstrated multiple times in both standardization bodies (see IETF's RFCs 4272, 5920 and 6941) and hacker conferences. In fact, a technique to bring down an MPLS network via the control plane was demonstrated live at the 2011 Black Hat conference.

While mitigation is possible to an extent, the threat of danger remains as long as control planes exist. Networks that are based on technology devoid of a control plane will always be much more secure. These include SONET/SDH and Carrier Ethernet networks. Neither SONET/SDH nor Carrier Ethernet offers a means to attack their signaling 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 peril. Although these tend to be more focused (e.g. DoS attacks focus on a particular host), the potential loss of connectivity between the HMI station and RTUs can interrupt control of the electrical grid. As with attacks that are centered on the control plane, data plane attacks can be mitigated as a result of design decisions relating to the operational network.

In scenarios where rigid connectivity is forced (as with SONET/SDH or Carrier Ethernet), it is much more difficult for an attacker to gain visibility into network elements outside of their direct connection. Such data plane rigidity serves to only expose the minimum necessary parts of each host to the network, and shield other parts that may be more vulnerable. In cases where a routed network exists (such as MPLS and IP), an attacker can first collect

information by snooping and scouting the network from an unsecured location, 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 802.1X, which validates each newly inserted device through a centrally managed database. It uses encryption to verify the identity and ensure the new device is not masquerading as a valid network device. This ensures all devices connected to the network are indeed valid authentic 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 elements inside the network. Insider attacks pose hazards from a number of perspectives.

First, it is extremely challenging to make a determination as to whether a particular command is valid or malicious. Some commands (e.g. decommissioning of an old RTU) may have a valid use when issued by authorized personnel, but can be harmful when initiated by others without permission.

Second, since attacks travel through diverse paths, a system that's omnipresent and able to track all possible paths is necessary to secure the entire network. Some utilities use a location firewall to mitigate the risk of one site controlling another, as well as to contain cyber threats at their general point of origin. Still, this can cause a wider than desired blockage or outage, and the larger the substation, the greater the risk of damage.

Finally, it is tough for standard "firewall" equipment to inspect commands. While standard DPI-enabled firewalls with can check software 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 a seemingly insurmountable obstacle when it comes to internal threats. The problem is, NERC CIP expects power utilities to deal with them. Specifically, NERC CIP expects power companies to detect and block occurrences where malware has taken over a piece of equipment – whether it be an RTU or 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, a few deductions must be made. The distributed nature of possible attacks renders a centralized or transitional solution inadequate. In addition, solutions must "understand" the ICS protocol and make an intelligent determination of whether a particular command is valid or out of bounds.

Hence, the ideal solution must be a distributed ICS-aware firewall. This type of solution can be omnipresent, as it is integrated into the fabric of the network (made part of the network switching equipment). Plus, the ability of an ICS-aware firewall to determine the validity of different SCADA commands can be used to block and detect insider threats or threats stemming from the introduction of malware to the network.

Two primary elements of this solution, omnipresence and application awareness, derive from the inherent characteristics of attacks. The distributed nature of power utility networks, plus the fact that most elements of the network can be placed in areas that are not highly secure – makes an omnipresent distributed approach preferable to a central solution. The only way of implementing this without having all traffic home-runned to the central gateway and incurring excessive delay, is by distributing the intelligence.

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 A Cyber Security Framework for Layered Networking Defenses in Industrial Control Systems

As discussed previously, operational power utility networks face a plethora of potential cyber threats. These threats span several vectors of attacks, and each defense strategy comes with its own vulnerabilities. Therefore, a network can only be truly protected when multiple defenses at multiple layers are employed. In short, it's the only way to protect from every one of the attack vectors and cover the vulnerabilities introduced by each single defense strategy.

The multi-layering of defenses is called **Defense-In-Depth**. Defense-In-Depth strategy focuses not on building an impervious single wall, but on building multiple defenses. These defenses utilize a mix of tactics to impede the advancement of an attacker and allow the defender to detect and block him. 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 relevant to the operational network.

4.1 Defense-in-Depth of Power ICS Systems

For power networks, 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. Such an approach addresses only one vector of defense, and will be rendered useless if an attacker can either breach the network or use malware to issue malicious commands. This is why a multilayered defense strategy is deployed to protect against all attack vectors – especially in the mission critical environment of the operational or automation and 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:

1. **Remote attacks originating at another location.** This is achieved by a networking firewall and inter-site encryption. They prevent hackers from gaining access to the internal networks "logically".

2. **Man-in-the-middle attacks.** This is achieved by inter-site encryption and prevents corruption or tampering of data.

3. **Network control plane attacks.** This is achieved via the design of the underlying network. For example, selecting a security-robust infrastructure like Carrier Ethernet or SONET/SDH in lieu of MPLS or MPLS-TP.

4. **Masquerading attacks**. This is achieved through source authentication protocols such as IEEE802.1X, which verifies that a particular host has not been replaced by another machine that can in turn issue malicious data or attacks.

5. **Snooping and scouting.** This is achieved by using network technology with rigid path definition and universal address space – like Carrier Ethernet.

6. **Malware attacks from RTUs, control stations or HMIs**. This is achieved by the use of distributed application-aware firewalls. These firewalls can dive into the SCADA protocols to verify that commands are within the bounds of the control or monitoring automation solution – 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.

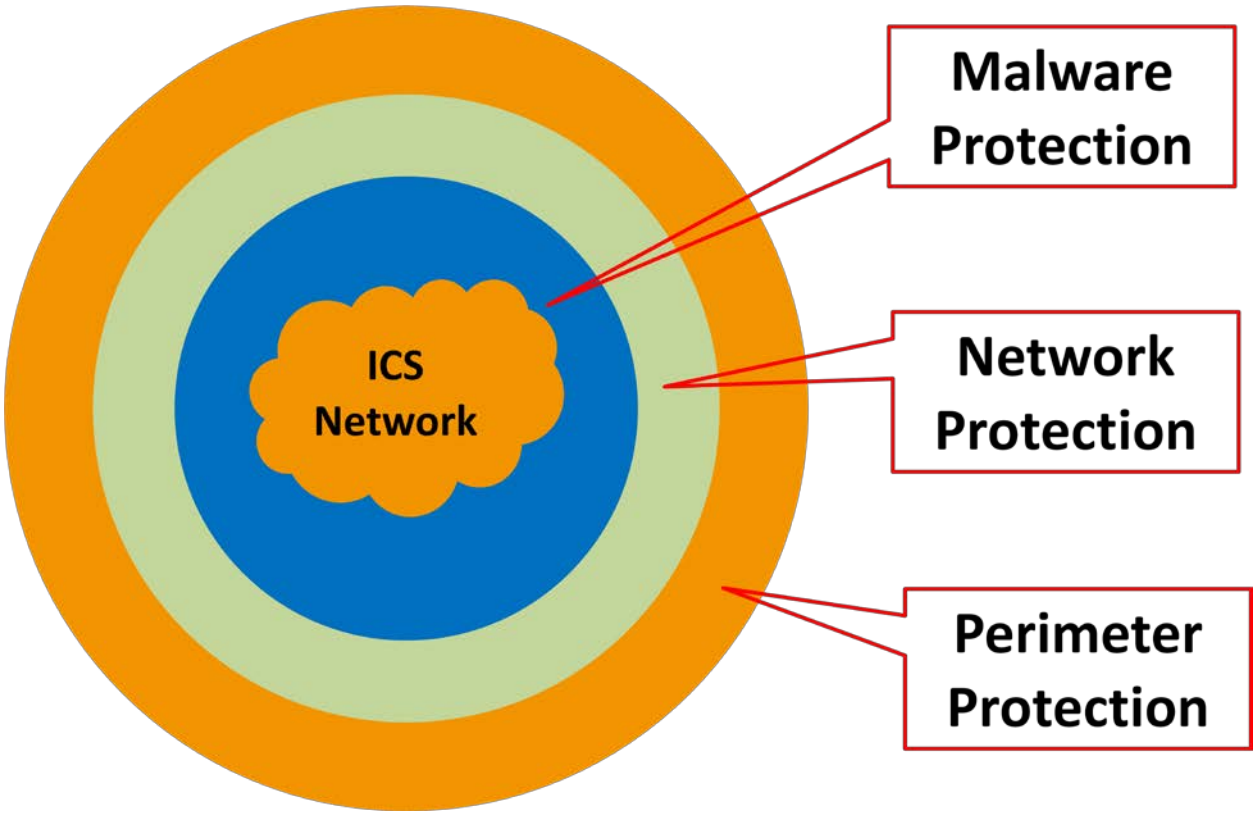

Diagram 1 – Defense-in-Depth of ICS Power Networks

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

5 Summary

ICS networks are extremely 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 power utility operational network – coupled with the existence of unmanned substations – also lends itself to attacks on the underlying network technology selected by the power utility.

All 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 power utility network. The multiple layers include the prevalent perimeter defenses along with network protection and malware protection.

The design of the underlying 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 potentially permit an attacker to topple the entire network through a simple breach of the physical security.

Malware protection must be part of an omnipresent 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 for the power utility network 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.

www.pulsesupply.com