The Energy Sector Under Attack

How to protect smart grid infrastructure from cyber threat

Introduction

Imagine what would happen if a portion of the smart grid was attacked and disabled for a prolonged period of time. Or imagine if all smart meters were reset, turned off, or set to record only half of the electricity consumed. Think of the headache, public outcry, and chaos. The smart grid is under attack and these are only a few of the ways malicious attackers could disrupt smart grid infrastructure.

In this white paper, we look at how to best protect critical infrastructure and provide proper visibility into network threats by taking advantage of the latest technology for industrial control system (ICS) security.

The threat of cyber attack is real

Over the years, the ICS environment has become ripe for successful attacks. Consider these facts.

Large attack surface

There are already 45 million connected SCADA devices and 244 million connected smart grid devices deployed. And these numbers are only expected to grow.

Growing number of disclosed vulnerabilities

Equally alarming is the accelerating number of ICS vulnerabilities disclosed. According to the Department of Homeland Security, ICS vulnerabilities disclosed from 2010 to 2012 increased by 600%. This does not take into consideration the many vulnerabilities kept secret or undiscovered.

Readily available attack tools

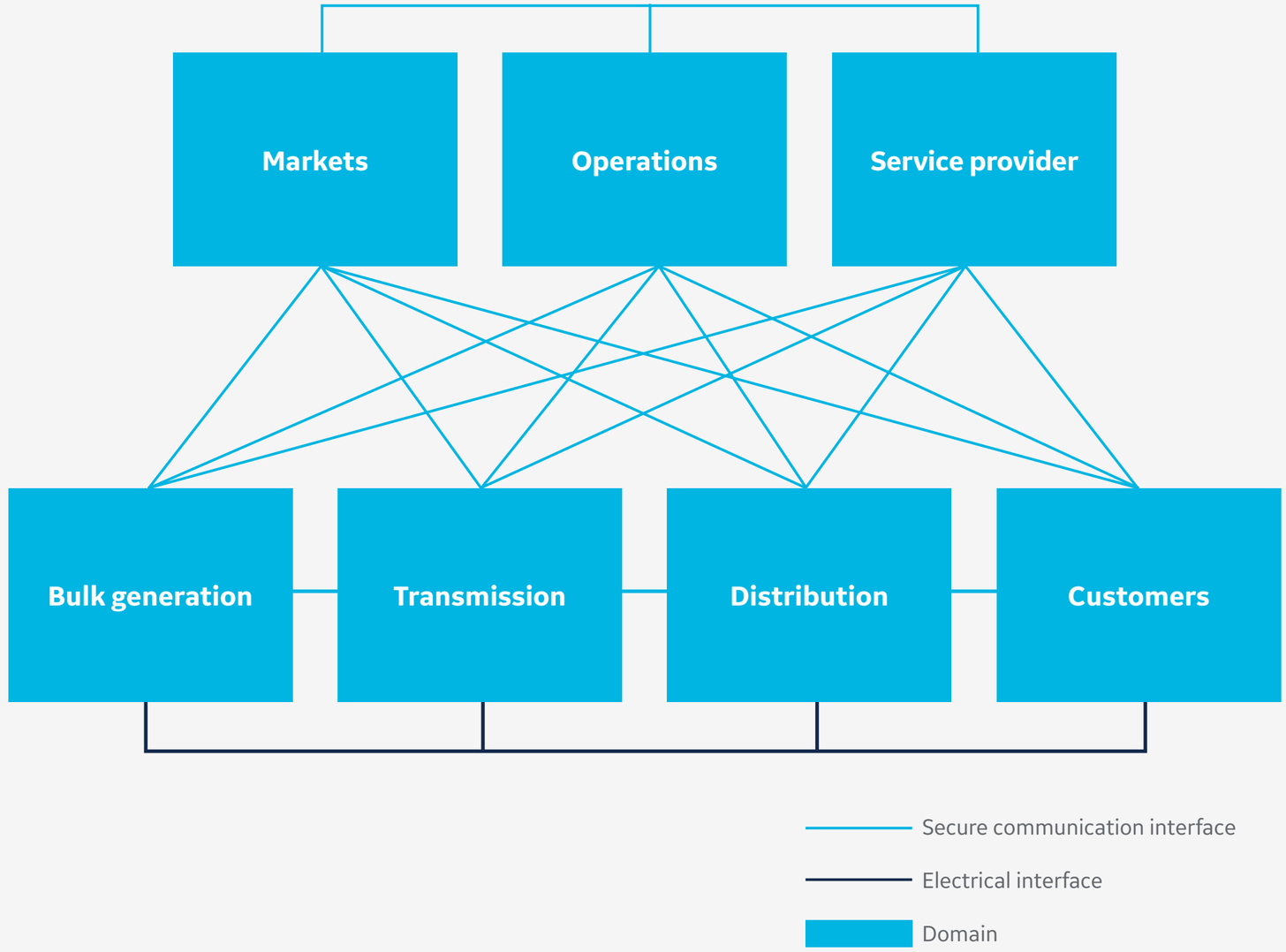
Attackers leverage search tools such as Shodan (shodanhq.com), "the Google for hackers," and Every Routable IP Project (eripp.com) to easily locate vulnerable ICS systems. By using attack tools such as Metasploit ICS modules, attackers can take advantage of publicly disclosed proof of concept code.

With the increasing number of disclosed vulnerabilities and available online tools to exploit them, the smart grid has been and will continue to be attacked. ICS-CERT Monitor recorded 256 reported attacks in 2013 and there are many more that are not disclosed. The number of attacks is trending up, with only 81 reported attacks in 2012. Of the reported attacks, 59% of them target the energy sector, indicating an urgent need to protect the smart grid.

Understanding the evolution of the smart grid enables us to better appreciate its unique security challenges.

Interconnectivity has increased the risk

There is an ever-increasing number of connected devices on the smart grid that require two-way communications. In the 1990s, the Advanced Metering Infrastructure (AMI) required bi-directional communications to share electricity usage information between smart meters in homes and internal systems. In addition, power sources are now more distributed and require bi-directional energy flows. Not only do large power plants supply electricity, but also things such as photovoltaic cells, hydroelectric plants, fuel cells, and wind turbines. Today, there are more meters, substations, and power sources than ever, all requiring more legitimate interconnections between meters and internal systems. Therefore, there are many valid reasons for interconnectivity allowing more network traffic to flow in and out of the network perimeter. Given this environment, it's essential to properly protect all critical information flows.



The National Institute of Standards & Technology (NIST) Smart Grid Conceptual Model

Perimeter protection using segmentation

Before delving into the protection alternatives, we must first clarify the definition of the perimeter so that our protections will be in the proper context. By perimeter, we don't mean a single choke point between the smart grid and the rest of the world. Within the smart grid infrastructure, there are many networks and subnetworks, all with potentially differing levels of security requirements. Many of the connection points are required to connect to other nodes, sometimes across subnetworks. In order to ensure proper protection, segmentation is key.

Information flows must be properly protected. Network nodes sharing common security requirements can be in the same logical zone, so nodes in disparate physical locations can still be grouped together to create a segment. Every zone has a logical perimeter and all information flows and network traffic must cross the perimeter so that the policies enforced on this traffic can secure it.

To properly secure each segment, it's necessary to:

- Create perimeters or network segments
- Put appropriate security controls in place for each zone
- Map proper policies to inspect each information flow

Now that we've determined segmentation can help secure the smart grid, let's look at specific security benefits. They include the following concepts.

- **Least access:** Limits user access and information flows to a "need to know" level, or more accurately, "need to access." Controlling which flows are allowed or not allowed can be done by setting the proper policy. By controlling access, the internal network structure will not be visible from the outside.
- **Containment:** Limits the effects of local failures in a specific segment from impacting other parts of the network. Whether the malicious culprit is a compromised contractor laptop, vendor back door, infected thumb drive, insider threat, or a rogue access point, the attack will be limited to a single segment and will not affect other parts of the smart grid.
- **Defensibility:** Introduces multiple barriers of entry to attackers and implements a defense-in-depth strategy that hinders an attacker from readily penetrating multiple parts of the network.

An additional side benefit of segmentation, beyond security, is improved performance due to fewer hosts per segment, thus minimizing local traffic.

However, segmentation alone is not enough. Network-based exploits, denial of service attacks, and insider attacks all appear to be legitimate traffic. So segmentation may not stop these threats. More information is needed to determine if legitimate traffic contains malicious intent.

The need for deep packet inspection

While investment in new technology or a step-change from current security measures may not be necessary, there are new requirements. The key requirement starts with the ability to control or limit network traffic by allowing or blocking it from a particular segment. With today's technology, that can be as simple as deploying a firewall with the appropriate rules and policies to limit traffic to legitimate traffic only. Since we know that ICS traffic can run on IP, and firewalls understand IP traffic, the firewall can successfully accomplish this important first step. However, attackers can use this legitimate traffic to hide their malicious intent. Let's consider two examples:

- A remote user can reset a smart meter, use an attack command, or even cause the smart meter to give everyone a discount for electricity. All of this can be done to legitimate traffic and today's enterprise firewalls do not have visibility to understand the specific payloads and its malicious intent.
- A user can engage in espionage by accessing and transferring files, data on operations, functions, features, and memory addresses from the compromised device. By reviewing ICS-CERT, one can also find implementation vulnerabilities in industrial protocols to render a device useless until a manual reset can be performed.

Therefore, deep packet inspection is necessary to understand malicious intent at the packet level. In today's enterprise firewalls, some have additional capabilities including content filtering and application control. However, it should be noted that pattern-matching packet contents and filtering/blocking web URL and enterprise applications do not provide the specific protections required for the smart grid. Appropriate and relevant solutions must be able to understand industrial protocols (e.g. DNP3, Modbus, and ZigBee), track industrial application sessions, and make proper "allow" and "block" decisions. This additional protocol insight can help OT managers apply the proper security policy to protect smart grid infrastructure.

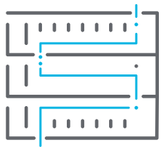
In addition, technology built for the smart grid needs to address performance and management UI needs for OT personnel. ICS network and smart grid infrastructure is not built like an enterprise network, so the latency and performance characteristics must match the operational environment parameters. In addition, since OT staff may not have advanced IT security training, management of the security technology must be easy to deal with, ideally using a graphical UI that provides visibility into the smart grid network, not a complicated command-line interface.

Industrial protocols relevant to the smart grid require deep packet inspection:

Modbus, ZigBee, dnp.

Benefits outweigh costs

Properly segmenting the network with the necessary visibility into industrial control applications and protocols comes with considerations, cost, and perhaps some added complexity. Ultimately, the protections and gains are worth these added steps, but they must be examined and considered carefully. Therefore, when implementing segmentation and industrial protocol inspection, consider these financial and time-related costs.



Additional complexity

Implementation and management of additional firewall devices or, at the very least, the capability to do deep packet inspection of industrial protocols and applications.

Greater change management support

Requires greater support whether from IT or OT staff teams, as there will be further work when making network or configuration changes.

Increased capital equipment cost

More technology requires more allocated budget for new firewalls or deep packet inspection capability for industrial protocols.

Impact on common networking tools

Support for routing, multi-homed networking, multicast in routed environments.

Performance overhead

Some latency increases may result when adding equipment to the network. Although the latency increases shouldn't be a factor, it needs to be considered.

Conclusion

In summary, the smart grid needs proper segmentation. Since traditional approaches have fallen short, organizations today require a firewall with deep packet inspection of industrial protocols for better security and better network visibility. Industry analysts, such as Gartner, always stress the importance of gaining approvals for the security budget upfront. The typical smart grid project has a significant and positive ROI, so earmarking 5–10% of that budget for security would not have a huge impact. By waiting to implement security later, you may find yourself needing to justify a separate budget. This will be a much harder proposition, requiring a cost center or insurance argument vs. an important corporate initiative. Remember to include security as an important line item in your budget when modernizing smart grid infrastructure.

About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive, and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure, and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology, and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

www.ge.com/digital