CERTES NETWORKS

eBook:

CRITICAL INFRASTRUCTURE CYBERSECURITY DEPENDS ON STRONG ENCRYPTION

Collaboration between Government and ICS Technology

OVERVIEW

Increasingly, critical infrastructure relies on internet-connected industrial control systems (ICS) and internet-enabled distributed operations. Industrial control systems, such as Supervisory Control and Data Acquisition (SCADA) are central to the operation of infrastructure in electricity, transportation, oil and gas, water, manufacturer, and other critical infrastructure sectors.

And, as automation continues to evolve and become more important worldwide, the use of ICS/SCADA systems are going to become even more frequent.

INDUSTRIAL CONTROL SYSTEMS (ICS)

ICS are devices, systems networks and controls used to operate and/or automate industrial processes. These devices are often found in nearly any industry from vehicle manufacturing and transportation to the energy and water treatment segment.

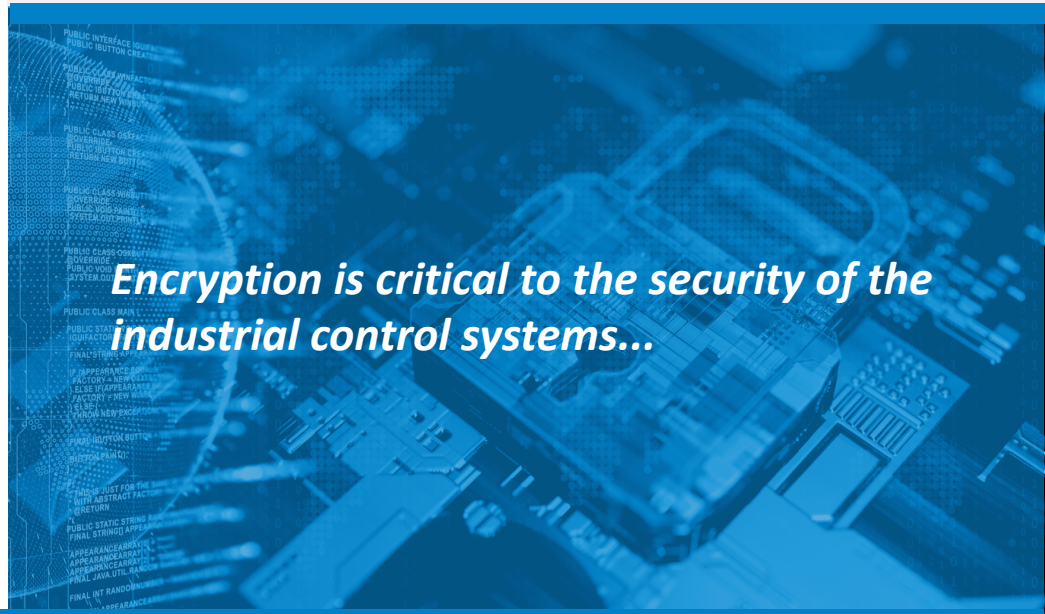
SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

SCADA networks are systems and/or networks that communicate with ICS to provide data to operators for supervisory purposes as well as control capabilities for process management.

These systems and other technologies communicate constantly with sensors, meters and enterprise devices through network channels, that if compromised, can lead to catastrophic disruptions to essential services.

ENCRYPTION IS A CRITICAL SAFEGUARD AGAINST CYBER ATTACKS

Encryption is critical to the security of the industrial control systems and the communication channels through which they send/receive sensitive data to keep critical infrastructure functioning. It protects the integrity of data in transit, enables visibility of communications channels through which data is sent and received, and enables secure authorization to defend against compromise by malicious actors. For example, encryption is used to protect data in transit across the electricity grid, including communications to and from operations centers, power generation systems, distribution substations, and home “smart grid” networks.



CYBER SECURITY OVERVIEW OF U.S. CRITICAL INFRASTRUCTURE

According to the U.S. Department of Homeland Security (DHS), critical infrastructure is at a very vulnerable stage for risk of malicious cyber-attacks. In March 2018, DHS warned that a nation-state actor had "targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors" for sophistical cyber-attacks.[1]

The potential disruption of such attacks has already been demonstrated when, in two separate occasions, hackers shut off power for hundreds of thousands of citizens in Ukraine.[2]

NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Because encryption is among the most important safeguards for managing the risk of data breaches, it is widely mandated by government and critical infrastructure organizations. Strong encryption is recommended by NIST Framework for Improving Critical Infrastructure Cybersecurity, now mandatory for US Government agencies. It is also directed for financial sector entities and ***Smart Grid operators.***[3]

Cybersecurity is critical for national and economic security," said Secretary of Commerce Wilbur Ross (2018). "The voluntary NIST Cybersecurity Framework should be every company's first line of defense. Adopting version 1.1 is a must do for all CTO's."

The U.S. framework was developed with a focus on industries vital to national and economic security, including energy, banking, communications and the defense industrial base. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state and local governments.

Weakening encryption would increase the risk of data breaches, threatening individuals, critical infrastructure, the economy, and ultimately national security. Instead, policymakers should defend the integrity of encryption technologies while working to expand its use across public and private stakeholders.

CHALLENGES

Joe Stuntz, vice president of cybersecurity at One World Identity, said the ICS issue is key, partly due to older technology on the grid. The power sector "must deal with legacy technology and challenges around upgrading" which means security enhancements may be difficult, Stuntz wrote in an email.

Depending on the ICS, there are only so many options that will be interoperable with the rest of the systems. DOE's report finds ICS technology has been a boon to reliability and resilience for utilities, but also offers up a new swath of vulnerabilities.

The U.S. Department of Energy (DOE) cybersecurity report revealed seven “gaps” in power sector defense capabilities. The assessment warns of restoration following a cyber-attack could be more challenging than previously understood, in part due to the unprecedented nature of such an incident.

> The power sector "must deal with legacy technology and challenges around upgrading” which means security enhancements may be difficult.
>
> **- Joe Stuntz – VP of Cybersecurity at One World Identity**

To date, a power outage due to a cyber attack has never happened in the United States, but hacking attempts are on the rise with a recent focus on ICS by cyber intruders.

The challenges at first glance seem overwhelming from staffing problems to supply chain coordination, and security shortfalls that represent potential weaknesses against a growing threat.

Some of the key challenges facing the power sector are:

- Cyber situational awareness and incident impact analysis
- Rules and responsibilities under cyber response frameworks
- Cybersecurity integration into state energy assurance planning
- Electric cybersecurity workforce and expertise
- Supply chain and trusted partners
- Public-private cybersecurity information sharing
- And, resources for national cybersecurity preparedness

However, experts all agree that staffing and supply chain vulnerabilities are the top concerns due to issues of communications between energy companies and subsidiaries.

IN SUMMARY

Wherever that attack comes from, there is a growing focus on industrial control systems (ICS). Malicious actors are taking advantage of older networks and the challenge in guarding the grid against these types of attacks in paramount.

Moreover, it is evident that the supply chain gap includes a call for more collaboration between industry, the federal government and vendors of industrial control systems (ICS) to enhance vulnerability awareness and response.

According to DOE, the systems, which utilize two-way flows -- automation and centralized controls -- have resulted in new vulnerabilities related to cybersecurity, even as utilities adopt increasing levels of protection for their businesses and operations networks.

Compounding the issue, the electric subsector faces challenges in recruiting and maintaining cybersecurity experts with strong knowledge of cybersecurity practices and the requisite knowledge of ICS used to operate the electric grid. According to experts, the workforce issue is likely to have the greatest impact on the ability to strengthen cyber security efforts in the power sector, with a current shortage of almost 1.5 million cybersecurity subject matter experts.[3]

In closing, strengthening the cybersecurity for public and private critical infrastructure must be a collaborative directive for those corporations, organizations and countries around the world to adopt a framework to safeguard our most precious public services. The cyber-attacks will not stop but only increase over the next one to three years; and, for those who do not heed the warning, indeed they could experience consequences that would be catastrophic for the U.S. and our worldwide neighbors.

REFERENCES

[1] Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (March 16, 2018.

[2] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab For Cyberwar," *Wired* (June 20,2017), available at https://www.wired.com/story/russian-hackers-attack-ukraine/.

[3] NIST V1.1 Framework for Improving Critical Infrastructure Cybersecurity, April 2018.

WHY CUSTOMERS CHOOSE CERTES NETWORKS

While competitors offer encryption methods that are often disruptive and complex, the Certes Layer 4 solution enables encryption of data in transit independent of applications and without having to move, replace or disrupt the network infrastructure.

The Certes Layer 4 solution encrypts data in transit and allows for secured masked encryption of only the payload, and not the entire data packet. By applying the Certes Layer 4 solution, network visibility is maintained along with network functionality.

HOW CUSTOMERS USE CERTES NETWORKS

As companies and government agencies seek to secure sensitive data and adhere to compliance regulations, Certes Networks offers an encryption management solution that can be applied to any network, application or user.

The Certes Layer 4 solution encrypts data in transit regardless of the disaggregation of network systems – Legacy networks, 3rd party networks or multiple sites in different locations – Certes Networks has got you covered.

"Our customers understand the value of their Data as a treasured commodity. Therefore, securing that data is priceless. Certes Networks enables customers to deploy our technology in the most mission critical of environments, where uptime is imperative and the security of data must be robust."

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1 (888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com

We offer an encryption solution that is simple, scalable and uncomplicated.