Old Systems and New Threats: Securing Industrial Control Systems for Utilities

Industrial control systems are hard to secure and highly attractive to sophisticated adversaries. Thinking differently about security can shed light on how to protect what matters most in critical infrastructure environments.

Recent events have put utilities such as electricity, water, oil and gas, and transportation in the crosshairs, providing a painful lesson in how a cybersecurity breach in those environments affects the lives of ordinary people. Industry leaders are asking what more they can do – despite their investments in the latest cybersecurity solutions, FBI and CISA bulletins continue to flow while everyone keeps their fingers crossed that their business isn't the next one in the headlines.

It's time to think about security differently. Instead of focusing on the perimeter, which doesn't really exist in a digitally transformed, cloud-connected organization, and instead of focusing on individual assets and least-privilege, as is accomplished with Zero Trust, it's time to focus on securing the internet itself.

Mining, quarrying, and oil and gas extractions + utilities had 546 incidents with 355 confirmed data disclosures in 2020.

-Verizon Data Breach Investigation Report 2021

Can't live with it, can't live without it: The risks of legacy ICS.

The technological world has changed, but a lot of the technology used by critical infrastructure has not. Many organizations have connected their ICS systems to the internet, but legacy ICS wasn't designed for that level of exposure and is now vulnerable to even simple attacks. Many legacy systems are beyond their support lifecycle, so patches aren't offered when new vulnerabilities are discovered, and even when patches are available, the systems cannot be taken offline for patching.

Top ICS Cybersecurity Challenges

- Legacy technology that was not designed to operate securely in today's hyper-connected environments
- Practical inability to shut down in order to patch or replace vulnerable assets
- A unique environment not well-served by traditional security solutions
- Massive amounts of IoT and mobile devices that may not be covered by policies or meet security standards

Downtime is not an option.

When the choice for ICS is between availability and security, availability will always win. Keeping goods moving and processes flowing overrules the threat of a breach that may or may not happen. ICS systems run for years with known vulnerabilities that go unpatched until a shutdown occurs. Right now, for instance, many facilities are running with certain ethernet/IP stacks that expose them to denial-of-service attacks, data leaks, and remote code execution, despite FBI bulletins warning of the dangers.

Traditional cybersecurity doesn't work for critical infrastructure.

These organizations face a double challenge in cybersecurity: they have complex, dynamic IT networks and they have diverse, distributed production and delivery environments. Security solutions that rely on vulnerability scanning can harm sensitive devices like plant equipment controllers and disrupt their operation. Agent-based solutions only protect the machines they are installed on. Log readers can be modified by attackers. A rise in innovative attacks, such as side-channel attacks, has rendered critical infrastructure extremely vulnerable due to its unique, expansive attack surface.

54%

of industrial sites have at least one remotely accessible device.

-CyberX 2020 Global IoT/ICS Risk Report

71%

of ICS disclosed vulnerabilities were remotely exploitable through network attack vectors.

-ICS Risk & Vulnerability Report

If no one can find you, no one can hack you. Stay available and invisible with Telos Ghost®.

Your controllers may be vintage and traditional cybersecurity may not make sense in your environment. But you can secure your ICS with a method that has been proven in military and intelligence communities for years. You can use Telos Ghost network obfuscation to make your assets invisible to the internet.

Telos Ghost is a robust, scalable, secure network-as-a-service that privatizes the public internet to hide network resources and mask the identity and location of users to ensure total protection as they interact with the operator's network.

Telos Ghost uses network obfuscation, multiple layers of encryption, and proprietary mesh algorithms to dynamically route IP traffic among cloud transit nodes. Advanced managed attribution makes users and their locations completely anonymous, which is a particularly compelling case for critical infrastructure operators conducting exploration, interacting with third-party suppliers and distributors, or communicating with remote workers.

Which sectors do cybersecurity professionals identify as "Most Vulnerable?"

Electric: **46%**

Oil & Gas: **18%**

Transportation: **13%**

-Security Magazine

How network obfuscation works.

Network obfuscation hides servers, applications, and unified mobile communications from the public internet and erases digital footprints so attackers can't follow them back to a targeted organization, device, or person.

With Telos Ghost, you can conceal SCADA and DCS DMZs in a cloak of invisibility to make them undiscoverable by adversaries, and protect PLCs and PACs from unauthorized access or reprogramming by hiding their control networks from view. Telos Ghost can also augment enhanced network segmentation with advanced obfuscation and encryption techniques.

Ransomware attacks are frequently delivered via phishing attacks that target unwary personnel. Telos Ghost can mitigate these risks by preventing adversaries from discovering and targeting devices on the enterprise network and keeping any successful intrusion from spreading horizontally across the IT or OT network by hiding those attack vectors as well.

This is a different approach from traditional cybersecurity, which focuses on protecting the enterprise edge and its endpoints. Instead, network obfuscation focuses on the internet itself. The Telos Ghost virtual obfuscation network protects traffic with multiple layers of encryption, eliminates source IP addresses and network component IP address at the destination, sends traffic through complicated routes, and masks details associated with users, devices, files, locations, network pathways, and more.

With no way to see internet-connected resources, unauthorized users cannot identify a target based on network-defined or static identity information and they cannot understand the nature of the organization's communications. Your most critical resources remain concealed, even to those who are hunting you specifically.

Discover how Telos Ghost can protect your ICS systems and networks.

Telos Ghost hides the crown jewels of your organization from the public internet making them invisible and inaccessible to adversaries by cordoning them off from your enterprise network. To learn more, please contact us.

KTT

Ken Michaels
ken.michaels@kttechnologies.net
https://www.kttechnologies.net

publication number: 5690-0624-B