A Better Way to Connect and Protect Industrial Control Systems and Assets

Easily and instantly authorize, connect, cloak, and disconnect any resource, anywhere, anytime

Introduction

Today's industrial control systems (ICS) represent critical operational assets across many organizations and a large cross section of industries and markets, such as utilities, manufacturing, Department of Defense, distribution, retail, and transportation. Provisioning, connecting and protecting these vital networks is critical to improving operational efficiency, and maintaining the safety of our communities, as well as the personnel who work with these ICS systems.

The Security Problem

The most recent SANS Institute survey on network security in March of 2016 states that up to 44% of network endpoints have experienced a security breach within the last two years.

Internet connectivity has become a requirement for all aspects of our lives today—work, home and recreation. This growing reliance on network connectivity only increases an organization's attack surface. Increasingly, it is critical to understand and be more judicious in knowing the things we connect to via the Internet. Decision makers with responsibilities over modern and legacy ICS have to be concerned, not only with ordinary hackers, but also the possibility of foreign espionage attempting to steal intellectual property or disable our vital resources.

Security experts at the U.S. Department of Homeland Security (DHS) have confirmed that principal activities behind many foreign hacks have been targeted at discovering models of ICS-SCADA systems and

"As the perimeter continues to dissolve and end-user technology continues to evolve, more endpoints are being exposed to external threats."

G.W. Ray Davidson
SANS survey author

other key hardware/software components of critical infrastructure. China, Russia, and North Korea have already proven their ability to successfully execute major attacks on critical U.S. systems related to power, public utilities, manufacturing, and other industries.

Unfortunately, the engine that makes our connectivity run is TCP/IP, which was built with openness and connectivity in mind, but not security.

> *"In its early days, the Internet was designed to be a network that combined unprecedented speed, reach, and efficiency. It was a perfect formula … for the dark side."*
>
> ***Leonard Kleinrock***
> *UCLA scientist and pioneer of networking*

One of the most basic attacks a hacker can execute is by spoofing the IP address of an endpoint. Such a misrepresentation is all they need to gain access to your data, your operations, and potentially your reputation as a capable and socially responsible organization.

Connectivity vs Security Trade-off

Complicating the issue of network security is the operational need to keep ICS systems running at peak efficiency. Unfortunately, efficient connectivity is often compromised in favor of bulky layers of added security and prohibitive firewalls as a best effort to properly safeguard critical assets.

Additional challenges regarding optimal connectivity are presented by operational technologies (OT) located in geographically sparse areas, making it time-consuming and costly to get skilled staff members to various sites to effectively authorize vendors and other users. Between the growing connectivity requirements of ICS and the ever-expanding Internet of Things (IOT), which might range from medical devices and smart meters to break room vending machines, securely adding such an influx of connected devices is becoming very challenging.

With such an expanding attack surface for hackers to exploit, security is understandably at the forefront of the mindset of IT decision makers everywhere. However, the need to stay up to speed with operational efficiency is also a growing problem. Not only is the attack surface of your network expanding, but also the overall scope of

Network and Security Policy Controls

100%

Use IP addresses for device identity – the root cause of networking and security complexity failure.

operations. More devices must be added seemingly every day causing more complexity and placing more stress on existing networks. The challenge then becomes how to strike the proper balance between diligent network security practices and expedient operational efficiency.

IT System administrators and operational teams need the ability to easily and instantly authorize, connect, cloak, and disconnect any resource, anywhere, anytime.

Alternative Solutions

Firewalls, including next generation versions, require you to put an inordinate amount of rules and restrictive policies in place, on a nearly continuous basis. Security patches and tighter control over systems by highly skilled personnel add complexity to the network, slow operations, and drive costs sky high. VPNs (virtual private networks) or VLANs (virtual local area networks) have been deployed to support ICS, but these are complex options to deploy, maintain, and troubleshoot, particularly when networked systems and machines are geographically distributed. These types of solutions do not provide adequate security, since they rely on spoofable TCP/IP addresses.

The need for a better way to achieve optimal security along with increased operational efficiency has become obvious to all ICS stakeholders with a watchful eye over the evolving technological landscape. In short, it's time for something better.

The Well-Tempered Solution – a New Identity Paradigm

It's time for a new paradigm whereby an IP address must no longer serve as a device's identity in networking and security. The vast majority of today's complexity and vulnerabilities (DoS, MiTM, Spoofing etc.) can be traced back to this singular flaw. Our unique host identity paradigm fixes this root defect and revolutionizes networking and security.

Tempered Networks' Identity-Defined Network (IDN) is a unified secure networking architecture that significantly reduces IT complexity, is simple to orchestrate, and enables instant provisioning and revocation of networking and security services with minimal, if any, modification to the underlying network, applications, or infrastructure. Tempereds' IDN is built with an "orchestration and

Today's alternatives are not sustainable

No identity, only complexity

VPN access controls for each network

Complex firewall and networking rule sets

Routing policies, VLANs and ACLS overhead

DNS and routing updates for failover

manageability first" mind-set, enabling controlled and predictable self-service by authorized technical teams.

The outcome of a Tempered Networks IDN deployment is a greater than fifty percent reduction in the overall network attack surface. IDN benefits are achieved through better segmentation and isolation of networks and endpoints, device cloaking, simplified multi-homing, and instant fail-over, all within a unified encrypted fabric. Our IDN's Software-Defined Segmentation capability provides effortless and verifiable micro, macro, and cross-boundary segmentation. Devices are natively cloaked and invisible to hacker reconnaissance, and protected against DDOS, MiTM attacks, and IP spoofing.

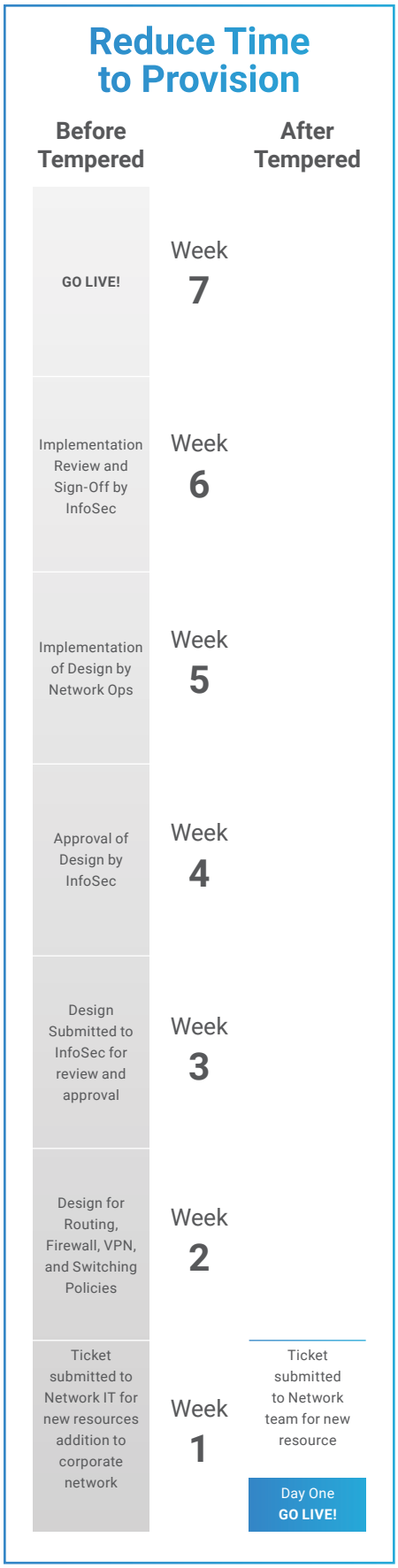
The IDN architecture incorporates a fully encrypted fabric that is centrally managed with a single pane-of-glass console. Unlike traditional IP networking approaches, IDN requires few, if any, changes to the underlying network, significantly reducing complexity, cost, and labor, while optimizing organizational responsiveness.

HIP services are available in a wide variety of versions depending on your individual needs, including virtual or physical appliances, cloud, client, server, and as embedded firmware, to provide you with nearly limitless flexibility. The Conductor enables simple policy-based orchestration with a RESTful API for smooth integration with other networking and security tools.

3-Click Network Design

An intuitive user interface dramatically simplifies the coordination and configuration of security policies, explicit trust relationships, and monitoring and analytics of your Tempered Networks deployment. The Conductor's intuitive user interface dramatically simplifies the coordination and configuration of security policies, explicit trust relationships, and monitoring and analytics of your Tempered Networks deployment. The power of orchestration coupled with ease-of-use enables '3-click network design'.

Reduce Time to Provision



A well-tempered solution features the following benefits:

Rapid Resource Provisioning

Unparalleled deployment speed for connectivity and automatic failover across Ethernet, Wi-Fi, cellular, and radio. Increase operational efficiency and availability with the ability to securely connect devices or systems worldwide, even if no network exists through cellular or Wi-Fi.

Cloaking with Encrypted Fabric

Vital assets and endpoints are invisible and safeguarded from bad actors. Our solution enables proactive security because endpoints are undetectable (no TCP/IP footprint) from the underlying shared network using AES-256 encryption across the elastic IDN fabric.

Effortless Segmentation

Easy micro, macro, or cross-boundary segmentation of devices/systems with the ability to give access or control for self-management to business units for specific network segments. Grant and revoke access to vendors for specific servers or devices from anywhere in the world.

Protect Legacy Systems

Topology and IP protocol-agnostic solution supports serial-over-IP communications for unparalleled flexibility and security for legacy and "unpatchable" systems. For example, most of the ATMs around the world still run Windows XP. Our HIP Services can cloak and protect all those devices with no changes to existing infrastructure needed.

Instant Failover and Quarantine

Effortlessly and instantaneously switch traffic between networks or data centers, in case of a failure, to ensure business continuity and system availability. Or, if a device is compromised with malware, for example, instantly revoke and quarantine it using an API-initiated alert.

The New Identity Networking Paradigm

Simple. Fast. Effective. Secure.

Reduce networking and provisioning time up to

97%

Increase in network and security team productivity

25%

Decrease IT Capex and Opex costs up to:

25%

Make

100%

of your connected IP resources invisible

Conclusion

Today's common practices for security and networking are simply unsustainable. Organizations, from small to enterprise level, require a new approach that ensures networks and people can efficiently scale to keep up with increasing connectivity demands. It is equally important, however, to implement a cost-effective way of protecting any device or system—from today's intricate SCADA systems and PLCs to legacy networks and long-lived systems such as HVAC, fuel pumps, and generators among others. Additionally, there is a vital need to properly safeguard transient and mobile resources such as robots, vehicles, sensors, trains, laptops, and tablets in a rapid and seamless fashion.

Best practice calls for segmenting your network and ICS to significantly reduce an attacker's ability to traverse the network in the event of an intrusion. Until now, however, segmentation has been so difficult and complex with traditional technologies that most organizations have avoided or ignored this approach.

With Tempered Networks' substantial investments and advancements in ease-of-use for secure networking, organizations can now rapidly provision, cloak, and segment any ICS resource down to the device level. Security is "baked in" from the start for a proactive, practical, and entirely sustainable implementation.

Resources

- Whitepapers
  - **The Answer to Next Generation Security Threats**
  - **Identity-Defined Networking Technical Whitepaper**
  - **A Primer on Host Identity Protocol**
- Videos
  - **Identity-Defined Networking solution overview demo**
  - **ESG primer on Internet of Things**
  - **Cloaking overview**
  - **Orchestration overview**

Next Steps

The time for something much more effective is overdue. It's time to learn what a well-tempered network can do for you and your organization. For more information **contact us** for a no obligation demo or visit **http://www.temperednetworks.com/demo/**.

The Tempered Networks Advantage

Integrates networking and identity from the start

Fast deployment, simple policy-based orchestration

Provisions secure networks and resources rapidly

Instantly connect, segment, revoke, quarantine, move or failover