www.pipelinepub.com
Volume 19, Issue 1

Stealth Networking for Critical Infrastructure and 5G Defense-in-Depth Protection

By: Rajiv Pimplaskar

Several critical infrastructure sectors utilize industrial control system (ICS) and supervisory control and data acquisition (SCADA) systems and IoT devices, which can often present appealing soft targets for threat actors. There is a significant percentage of such devices that can have inherent vulnerabilities and, unfortunately, many of these systems are operated outside the purview of the security teams that manage the Common Vulnerabilities and Exposures (CVEs) and the Cybersecurity and Infrastructure Security Agency (CISA) advisories.

The complexities of adhering to the National Institute of Standards and Technology (NIST) standards and the Purdue model has become even more challenging with the advent of 5G. While 5G does have built-in security—as specified by the 3rd Generation Partnership Project (3GPP)—it poses a new danger of expanding the attack surface with smaller cell sizes, shift to Open Radio Access Network (O-RAN) and more business-centric use cases. A key strategy to safeguard 5G critical infrastructure is to augment its security framework with "stealth networking." This approach was first developed by special forces and the intelligence community and is now also popular within law enforcement and the digital forensics world. Source and destination relationships as well as sensitive data flows across the public cloud and the Internet are obfuscated with a next-gen virtual private network (VPN). Stealth networking adds "defense in depth," making it virtually impossible for a bad actor to detect—let alone target—the operational technology (OT) estate in the first place. Stealth networking is also capable of complementing

conventional cyber safeguards and control assertions as specified by NIST, the Purdue Model and IEC 62443 standards, which can typically kick in later along the kill chain.

Critical infrastructure security and 5G implications

As critical infrastructures have come under persistent and nation-state motivated attacks around the world, cybersecurity for ICS SCADA systems is undeniably paramount. NIST guidelines, the Purdue Model and IEC 62443 standards establish best practices for IT and OT networks as well as addressing use cases where the boundary needs to be crossed. These models delineate the need for network segmentation and communication control as well as the use of perimeter firewalls.

5G has security built into the standards itself and could represent a new era of transformation for critical infrastructures, offering significant improvements over previous generations like 3G, 4G or LTE. The industry body that sets standards for mobile communications, 3GPP, has added new capabilities for 5G via the Service and System Aspects working groups that include enhanced subscriber privacy and authentication, greater interface protection, and enhanced integrity protection of user traffic. While they are more secure, 5G rollouts are characterized by small cell deployments due to outdated regulations, excessive fees, prolonged processes to obtain permits, and lengthy procurement cycles. Private 5G adoption is accelerating within the U.S. in part due to the availability of Citizens Broadband Radio Service (CBRS) frequency band which enables organizations to use the 3.5 GHz to 3.7 GHz radio spectrum to build wireless networks based on 4G LTE and 5G cellular technologies. However, this unrestricted capability does not exist worldwide, and several sovereign countries consider radio spectrum as a national asset necessitating bureaucratic carrier negotiations and fees.

These issues, coupled with a massive increase in numbers of IoT devices, vulnerabilities within the public fiber infrastructure, and higher use of virtualization and cloud services, have dramatically expanded the attack surface and intensified the need for advanced security.

5G use cases within critical infrastructures span multiple sectors including manufacturing, retail, healthcare, utilities, agriculture, mining, and oil and gas. 5G capabilities can revolutionize warehousing, distribution, supply chain, asset management, and transport as well as smart city planning. These varied use cases range from real-time data collection to digital twin, AR-guided work instructions, predictive maintenance, connected and automated guided vehicles, connected workers, and worker safety.

3GPP's open interoperability also facilitates the rise of O-RAN, where multiple vendors come together at the edges of the network in a virtualized and disaggregated manner. This disaggregation facilitates time to market for 5G buildouts worldwide. However, security remains a key concern due to the inherent expansion of the threat surface, as

is being actively addressed within the O-RAN Alliance. Zero-trust architectures will play a crucial role in helping secure the new frontier of 5G critical infrastructure. These architectures will help organizations meet the latest security requirements and keep pace with challenges associated with the expanded attack surface in the context of NIST 800-82 and IEC 62443 standards.

Nation-state threats can overwhelm conventional defenses

According to research by Venafi, 64 percent of businesses suspect they have been targeted or impacted by nation-state attacks and 63 percent doubt they would ever know if their organization was hacked by a nation-state. Internet Protocol Security (IPsec) using Internet Key Exchange (IKE) and Transport Layer Security (TLS) cryptographic protocols operate at the session layer (layer 5) of the OSI model and are designed to provide communications security over a computer network. Once the client and server have agreed to use IKE (or TLS), they negotiate a stateful connection by using a "handshaking procedure" with an asymmetric cipher to establish not only cipher settings but also a session-specific shared key with which further communication is encrypted using a symmetric cipher. Applications generally use TLS as if it were a transport layer, even though applications using TLS must actively control initiating TLS handshakes and handling of exchanged authentication certificates.

IPsec and other underlying protocols operate at the session layer (layer 5) of the OSI stack. This means that the Network and Transport layer (layers 3 and 4) have to be set up before encryption is set up. This opens the door for an adversary to eavesdrop as source and destination relationships of the traffic and flows of interest can be reverse engineered across conventional networking providing deep insight into the public cloud setup, identifying privileged users, and organizational IT and OT relationships. Those adversaries can then intercept, harvest, or even disrupt those flows with a Man in The Middle Attack (MiTM).

Nation-state actors can exploit host nation ISPs and public cloud to run sophisticated MiTM attacks such as Steal Now Decrypt Later (SNDL) or Harvest Now Decrypt Later (HNDL). Traditional zero-trust approaches stop at the network and are largely ineffective against such nation-state actors.

Defense-in-depth with stealth networking

The deployment of a "stealth networking" strategy will be an important step in providing an effective and enhanced defense against future cyber-intrusions. Stealth networking builds upon the concept of managed attribution, which is utilized extensively within the intelligence community. As its name implies, attribution is the assigning of an identity to some visible entity or activity. Managed attribution is the active process for shaping online identifiers. It's what allows you to control what conclusions others draw about the identity of a user or online resource. In other words, it's the active process of creating visible information that will lead the adversary to the desired conclusions.

Stealth networking can enable communication across the public cloud and Internet with private IP addresses. Firewall architectures can be secured by enabling outbound access and provide only a "silent fail" to port scans or "TCP Listen" calls deployed by threat actors. Finally, the source and

destination will not be known by either side, leading to traffic obfuscation and concealing information and flows of value.

Stealth networking can be expanded to also enhance protection of data in transit with dynamic virtual active/active multipath networks with rolling encryption keys and granular access controls. In addition, orchestration, control, and data planes can be separated, thereby further protecting data flows from potential interception and future analysis. This can protect against advanced MiTM nation-state attacks like SNDL or HNDL. Proper micro-segmentation, access control and device posture checking can also be implemented to prevent unauthorized access.

The types of next-gen networks I've discussed here can enhance resiliency and performance even within a contested or congested environment, enabling service providers to offer better SLAs. The network can finally become automated and self-healing with dynamic routing and management capability with smart deflection and redirection of traffic from impacted resources and network nodes to mitigate against availability issues and distributed denial of service (DDoS) attacks. Importantly, performance can be enhanced, even across high latency, low bandwidth environments, enabling alternative communication pathways such as mobile hotspot, ADSL, broadband, satellite, MPLS, LTE, and others to maintain business continuity—even in the face of primary network disruption.