Experience. Outcomes.

APPLICATION NOTE

Securing Critical Infrastructure

Network Encryption for Utilities

Cyber security poses problems that only stand to become increasingly frequent, complex, and challenging. According to Michael Mullen, former Chairman of the U.S. Joint Chiefs of Staff, "The cyber threat is the single biggest existential threat that's out there" because "cyber, actually more than theoretically, can attack our infrastructure, our financial systems."[1]

Power utilities face elevated cyber challenges since they are considered critical national infrastructure, which is defined as "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health, or safety."[2]

To illustrate the ongoing cyber challenges utilities face, a 2014 Unisys survey with the Ponemon Institute showed that nearly 70 percent of critical infrastructure providers surveyed—utilities responsible for the world's power, water, and other critical functions—have reported at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months.[3]

Security is essential to establishing and holding the public's trust in national power grids. Encryption, one of the key tools in the cybersecurity toolkit, makes information unreadable to anyone except those who possess the correct key to decipher the message.

Most organizations protect data at rest, securing servers, databases, routers, and switches by managing user access and credentialing. However, in today's utility networks, large amounts of critical data are transmitted as high-bandwidth communications beyond the walls of the utility substation or data center, traversing regional and national networks. Therefore, a comprehensive IT security approach must encompass a robust in-flight encryption solution as part of its holistic security

1 CNN: "Admiral Michael Mullen: Farewell and thank you" by Micah Zenko, Nov. 11, 2011; http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/
2 Cornell University Law School, Legal Information Institute: U.S. Code 5195c – Critical infrastructures protection; http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/
3 Ponemon Institute: "Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year", July 10, 2014; http://www.unisys.com/offerings/security-solutions/News%20Release/Unisys-Survey-Reveals-Critical-Infrastructure-Providers-Breached

Benefits

- Safeguards utility in-flight data from data breach and keeps critical systems secure
- Protects valued reputations and avoids costly fines, public media exposure, and customer churn by meeting expectations for information protection
- Meets NERC-CIP security requirements for the utility industry

strategy. By encrypting data as it leaves the security of the private cloud, utilities can ensure this data is protected from unauthorized intercept as it traverses the network, crossing varying security levels as it reaches its destination.

Why utility CIOs do not encrypt in-flight data

Many utility CIOs do not fully appreciate the fact that, once data leaves the substation or datacenter, it is basically outside of their control. Given all the efforts to lock down data at rest with firewalls, anti-virus software, and intrusion detection, cyber criminals are increasingly turning their attention to intercepting the data as it travels across the network. Cyber security firms are reporting increasing numbers of cyber incidents focused on corporate and internal networks.

Another reason for the lack of focus on in-flight encryption is that many CIOs have been lulled into believing their fiber optic networks are inherently immune to breaches. The reality is that a mid-range hacker armed with low-cost equipment and software can intercept utility data undetected for days, months, or even years. Anyone with Internet access can easily shop online for a fiber coupling tool and, after watching a few YouTube videos that guide you through the tapping process, can quickly learn how to steal sensitive data from a fiber optic cable. Numerous videos depicting the ease with which hackers can breach a fiber network can be found on YouTube. A single fiber strand can carry an enormous amount of data, and since fiber optic cables are surprisingly accessible, they have become valuable targets for attackers.

Hacking an Optical Fiber Line in Minutes
Watch video

One more reason utility CIOs have been reluctant to deploy in-flight data encryption is a concern about decreased network performance and cost. In an industry where margins are thinning and network latency can mean the difference between containing or propagating a power outage, their concern is understandable, although unfounded. These concerns may stem from experience with Layer 2 and higher network encryption solutions. For example, Layer 3 encryption devices are designed for IPSec encryption (standard Internet encryption). IPSec uses a process that 'tunnels' the original IP packet to encrypt an IP 'header.' However, tunnels can result in increased overhead, complexity, and network performance speed and processing.

The ideal in-flight network encryption solution

Whether network encryption is part of a private optical network or offered by a service provider as part of a managed service, key points to consider include:

Regulatory compliance. Utilities are very cognizant of regulations that may apply to the applications carried by their networks. The utility industry established a series of security specifications under the North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP) standards. These include everything from protecting physical assets to securing their supply chain and IT assets. The chosen solution must meet NERC-CIP compliance requirements for the utility industry.

Latency. Specifications for latency in the utility market are more stringent than other verticals, as a power surge must be acted on with a delay of less than 10 ms to avoid propagating a power outage. State-of-the-art encryption solutions meet the requirements of utilities by delivering hardware-based latencies on the order of several microseconds.

Management. Whether the utility or a service provider manages the encrypted links, the 'owner' of the data—the utility—should maintain control of the encryption keys, issue new keys as needed, and have visibility into security alarms and logs associated with their encrypted links. This is accomplished by separating the network management from encryption key management. If the encrypted service is purchased from a service provider, the provider will manage the links and their provisioning, administration, and performance monitoring, but will not have control of key distribution or maintenance. Depending on the utility's security policies, key distribution can be performed manually or automatically over secure, encrypted tunnels.

A comprehensive security approach must encompass not just 'data at rest' including data residing in databases, files, and storage systems, but also in-flight encryption, to ensure data is protected from unauthorized discovery as it traverses the network. Today's in-flight encryption techniques can camouflage traffic so it cannot be read or manipulated, and even disguise the fact that there is traffic flowing at all.

In-flight encryption at the optical layer

Optical-layer encryption addresses all these issues and more. While it is true that technologies like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are used increasingly

to secure connections to servers, the only way to secure everything on the communications link in and out of a facility is to encrypt at the physical layer. This is particularly true when one considers the amount of 'meta-data' generated by various services on a network that is not necessarily encrypted, even when using application-layer encryption such as TLS/SSL. IP and MAC addresses, protocol types in use, and other network information are exchanged in the clear, even when the actual user data is encrypted. This meta-data can be used by adversaries to map out a network and plan attacks, even without access to the encrypted application layer data. A Layer 1, bulk encryption approach renders all utility data and meta-data undecipherable to any hacker that taps into the fiber strand.

Utility key encryption use cases and applications:

(1) Power grid communications

a. Tele-protection
b. SCADA

(2) Data center interconnect

a. Disaster avoidance/recovery
b. Data center consolidation/optimization
c. Workload mobility

(3) Video transport

a. Video surveillance

Ciena's WaveLogic Encryption solution

WaveLogic Encryption delivers a simple-to-implement, wire-speed optical encryption solution that integrates directly into the transport network. With its set-and-forget approach, encryption is always on, ensuring the highest level of security and eliminating human error that can result in sensitive data being sent over the network unencrypted. As is shown in Figure 1, WaveLogic Encryption ensures all critical utility data and meta data traveling across the utility network is always secure.

The solution is validated externally, and independently certified by a third party to ensure it is implemented using industry-standard algorithms and advanced security features. It provides a FIPS-certified AES-256 encryption engine with standards-based authentication mechanisms (such as X.509 certificates), enabling seamless integration into existing enterprise PKIs, as well as support for the latest public key cryptography algorithms including Elliptic Curve Cryptography (ECC). Additionally, the hardware and software components of the cryptographic modules are compliant with FIPS 140-2, offering the assurance that the encryption solution complies with all aspects covered by this comprehensive evaluation, including encryption algorithms, key exchange mechanisms, and user authentication.

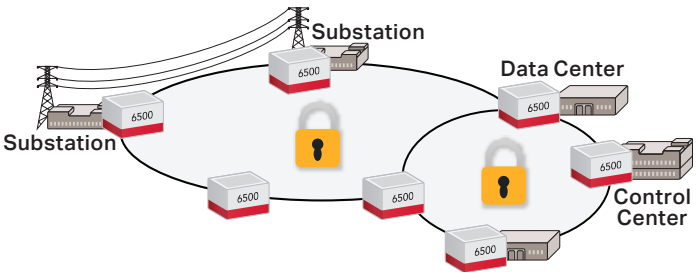

Figure 1. Ciena's WaveLogic Encryption

Ciena's WaveLogic Encryption solution allows utilities to:

- Seamlessly converge utility OT/IT networks and meet compliance requirements over a single, converged, highly-secure infrastructure
- Comply with NERC-CIP requirements for protecting utility networks through FIPS-certified encryption of all in-flight data 24/7
- Leverage flexible bandwidth offerings with protocol-agnostic 10G, 100G, or 200G wire-speed encryption without impact on utility application performance
- Benefit from a simple, integrated encryption management approach that partitions encryption management from transport management. This allows the utility organization networking team to manage the network while the security team maintains full control of the encryption security parameters associated with their critical utility data, issuing new keys or certificates as required by their security policies

WaveLogic Encryption Solution
Download application note

Encryption of data at rest and in flight is not mutually exclusive. They typically are implemented in conjunction with and complement each other as part of a holistic security strategy. When deploying an in-depth, multi-tiered data security strategy, utilities must understand the use case, application, and compliance requirements. In addition, the chosen software or the technology must adhere to the highest level of encryption standards and algorithms. Ciena's WaveLogic Encryption solution combines a high degree of flexibility and security with ease of operation and administration to enable a cost-effective, ultra-low-latency, wire-speed encryption solution for the utility market.

Connect with Ciena now