ciena
Experience. Outcomes.

WHITE PAPER

Smarter Security for Financial Networks with In-flight Optical Encryption

For the Financial Services Industry (FSI), cyber attacks have become one of the highest risks for regulatory violations and potential loss, exacerbated by the growing volume and sophistication of the attacks FSIs face. Failures in cybersecurity have the potential to impact a bank's operations, core systems, and reputation, and in the extreme can undermine the public's confidence in the individual bank as well as in the financial services industry as a whole. FSIs are increasingly dependent on Information and Communications Technology (ICT) to deliver services to their personal and business customers, which, as evidenced by recently publicized cyber hacking incidents, can place customer-specific information at risk of exposure.

The risk

The FSI finds itself under a seemingly never-ending barrage of cyber attacks on a daily basis. In fact, it holds the dubious honor of experiencing security incidents 300 percent more frequently than any other vertical[1], according to Forcepoint's 2015 Industry Drill-Down Report on Financial Services. More than 66 percent of financial institutions face at least one attack per year, and almost 15 percent face more than 100 per year, according to Help Net Security[2]. With each attack carrying an average annualized cost of approximately $16M USD[3]—the highest cost of any vertical, as reported by Ponemon's 2016 Cost of Cyber Crime study—it is little wonder security is a priority for most banking executives. According to Forbes, this concern is evident in the fact that, in 2015, cybersecurity spending from four of the largest U.S. banks[4]—J.P. Morgan, Bank of America, Citigroup, and Wells Fargo—topped $1.5B[5], with the overall U.S. FSI laying out $9.5B[6].

This huge expense is hardly surprising when Ponemon reports[7] that over half of their respondents had experienced malware, phishing attacks, Web-based attacks, malicious code, botnets, or stolen devices. This rise in the number and effectiveness of attacks is partly driven by the increasing ease and lower cost of staging an attack. There has been a proliferation in the use of increasingly less-costly hacking toolkits, with 64 percent of hackers rating them as 'Effective' or 'Highly Effective.'[8]

Ponemon's report found that more than 60 percent of hackers were deterred if the hack took more than 40 hours. However, as FSIs increase their defenses against these attacks but remain highly desirable targets, hackers will inevitably move to easier points of attack.

Why FSI CIOs do not encrypt in-flight data

Although FSIs have some of the largest deployments of encryption technology, typically these are deployed to protect data at rest, encrypting such caches as databases, data center storage arrays, and laptop hard drives. However, some CIOs do not fully realize the extent to which security has passed beyond their direct control once data leaves the premises.

[1] Forcepoint, *2015 Industry Drill-Down Report – Financial Services* www.forcepoint.com/content/2015-industry-drill-down-report
[2] http://www.helpnetsecurity.com/2016/11/09/financial-institutions-cyber-attacks/
[3] Ponemon, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf
[4] http://www.bankrate.com/finance/banking/americas-biggest-banks-1.aspx
[5] http://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#3cfab741112b
[6] Homeland Security Research Corp, "Banking & Financial Services Cybersecurity: U.S. Market 2015-2020 Report"
[7] Ponemon, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation* http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf
[8] Ponemon/Palo Alto Networks, *Flipping the Economics of Attacks* – January 2016 http://www.ponemon.org/blog/flipping-the-economics-of-attacks

Because of all the money spent to protect data at rest with encryption, firewalls, anti-virus software, and intrusion detection, cyber criminals' traditional routes to attack an FSI are becoming increasingly challenging. As a result, they are turning their attention to intercepting data as it travels across the network. Cybersecurity 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 believe 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 customer data and remain undetected for days, months, or even years. Anyone with Internet access can easily shop online for a fiber-coupling tool and quickly learn from YouTube how to steal sensitive data from a fiber-optic cable. Considering the distances traffic may be traveling via optic fibers, it can be difficult to maintain complete physical security. Optic fibers can carry enormous amounts of data and, since fiber-optic cables are surprisingly accessible, they have become valuable targets for attackers.

When it comes to introducing in-flight encryption to their networks, some CIOs have also expressed concerns about the following areas:

1. **System performance and latency –** This is an industry in which latency can have a major impact on system performance and severely affect the company's profit. 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 an increase in overhead, complexity, and subsequently, network performance speed and processing. Layer 3 encryption also may not be able to support the full range of protocols being deployed.
2. **Policy enforcement –** Many of the network encryption solutions deployed today are designed to protect one stream of data. While this often offers a point solution, it poses its own challenges around management and policy enforcement. Ensuring that all the correct traffic is identified and protected can quickly become a management nightmare in a complex environment. The task of safeguarding all the traffic that should be protected can easily become overwhelming, as sometimes traffic that needs protection is not protected, and vice versa.
3. **Scalability –** While many encryption solutions work well at low traffic levels, as traffic scales—especially if it consists of mainly smaller packets such as credit card transactions—the inability to maintain the encrypted service at wire speed means many solutions will start to drop packets or even lock up. In a web-scale world, with data center-to-data center traffic often measured in multiple 10s or 100s of Gbs, any solution that cannot deliver the full data rate throughput at today's speeds can seriously impact security and business performance.

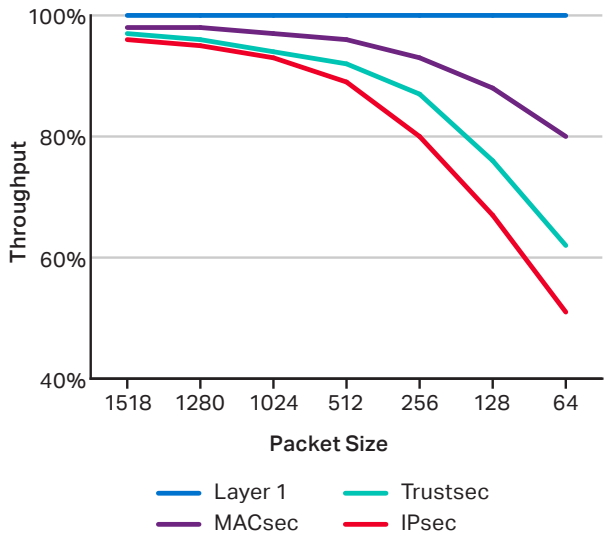

Figure 1. Throughput effects from encrypting at different Network Layers

4. **Key management –** Many security teams welcome the idea of an encryption solution, but are unwilling to delegate or take on responsibility (and accountability) for the management and configuration of the company's encryption keys. Many in-flight encryption solutions offer key management as part of the overall device management platform, which means either the network team or the Managed Service Provider has access to the security management of the device, or the security team must take responsibility for both the security and network management and configuration of the device. The perceived complexity around key management is one of the main reasons cited for not deploying more encryption solutions.
5. **Support for advanced algorithms –** Faced with mounting concerns that previous encryption methods may have been compromised to a greater or lesser degree, many CIOs are looking for solutions that have adopted newer algorithms, such as Elliptical Curve Cryptography (ECC), that are recognized as more secure than some first-generation public key cryptography systems.

Hacking an Optical Fiber Line in Minutes
Watch Video

In-flight encryption at the optical layer

Optical-layer encryption addresses all these issues and more. While technologies like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are increasingly used 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 approach renders data undecipherable to any hacker who taps into the fiber strand.

TLS and SSL solutions also generally rely on third-party certificate authorities that may themselves be compromised, allowing for man-in-the middle attacks. In addition, the traditional operational model for deploying and maintaining protocol-specific encryption solutions can quickly become cumbersome, complex, and costly, with multiple encrypt/decrypt device pairs required to support a multi-protocol environment. At the transport layer, a wide variety of traffic types—such as Ethernet, Fiber Channel, FICON, OTN, SONET, and SDH—can be encrypted simultaneously. Furthermore, optical-layer encryption guarantees transparent encryption at wire speed. In other words, the encryption process does not reduce the traffic throughput of the signal being encrypted, nor does it modify user data in any way. Additionally, encrypting all traffic before it enters the fiber ensures the entire data channel is encrypted, no matter what.

WaveLogic Encryption Solution
Download application note

One major benefit of encrypting in-flight data is the potential exemption from regulatory requirements to report a data breach. Across the world and applying to many verticals, there is an increasing focus on the protection of user data and rapid notification of those affected if their data is stolen. Whether through more general U.S. regulations like the Federal Trade Commission Act, more specific legislation like the Gramm-Leach-Bliley Act or Health Insurance Portability and Accountability Act (HIPAA), or even more international rules such as the EU's General Data Protection Regulation (GDPR), a common theme is the increasing size of penalties for breaches and for failing to notify consumers within stipulated timescales if a breach has occurred. A commonly applied caveat is that, if a data breach occurs but the data is unusable to the hacker—such as encrypted data (usually to a stipulated level such as Federal Information Processing Standards (FIPS) 140-2 standard)—, the requirements for notification and the associated penalties may be waived.

Financial key encryption use cases and applications

1. Data Center Interconnect (DCI)

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

2. Video transport

a. Remote consultation (such as for mortgage or loan advice, wealth management, and pension/insurance)
b. Security cameras
c. Distance learning/training for staff

3. Connectivity services-related applications

a. Trading desks
b. Core banking systems
c. Data analytics and mining/big data
d. Customer portals
e. Account record storage backup and archiving, lifecycle management
f. Connectivity to payment rails
g. Secure connectivity to private, public, or hybrid cloud
h. Secure connectivity to third parties (such as approved ecosystem financial technologies)
i. Email and ERP systems

Ciena's WaveLogic Encryption solution

WaveLogic Encryption combines the proven encryption technology deployed on platforms that have a large global installed base, with the proven reliability of the market-leading 6500 Packet-Optical Platform, which has been deployed by more than 500 operators around the globe. The 6500 underpins much of today's critical communications infrastructure, addressing the requirements of service providers, Internet Content Providers, enterprise, government, healthcare, utility, media, and entertainment, as well as research and education networks.

WaveLogic Encryption delivers a simple-to-implement, ultra-low-latency, wire-speed optical encryption solution that integrates directly into the transport network. With the flexibility of the 6500, providers can select the optimal shelf size to cost-effectively meet their site-specific capacity, space,

and power requirements. 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 customer or business data being sent over the network unencrypted. As illustrated in Figure 2, WaveLogic Encryption ensures all critical data traveling across the network is always secure.

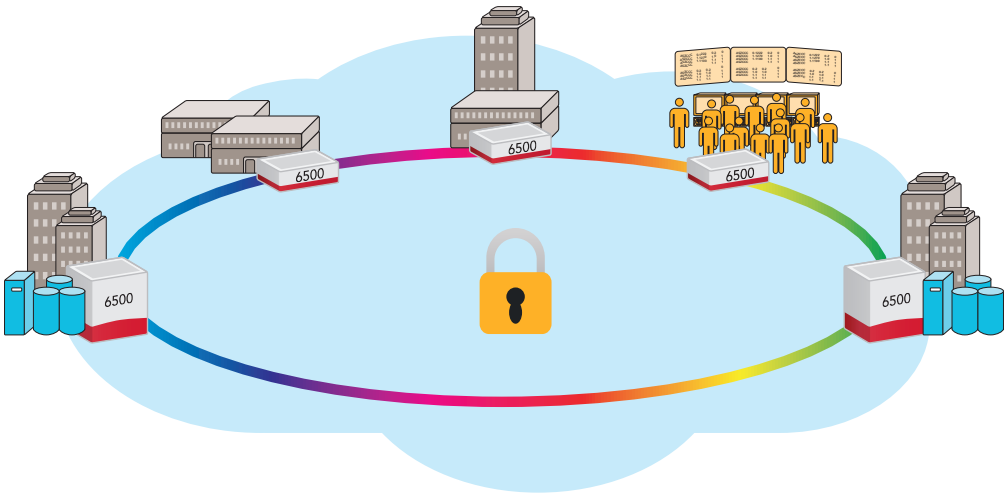

Figure 2. Metropolitan finance network

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 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. For enhanced data protection, two distinct and independent sets of keys are used for authentication and data encryption functions, with a fast encryption key rotation interval of seconds instead of minutes. The AES-256 data encryption session keys are autonomously negotiated and rotated every second, independently, without impacting traffic or throughput, and without user intervention.

WaveLogic Encryption enables deterministic, ultra-low-latency in-flight data encryption that supports the full range of critical financial applications, allowing FSIs to:

- Seamlessly access critical customer data, interconnect resources, transfer trades/data files/records, and meet compliance requirements over one highly secure network
- Comply with regulatory requirements for protecting customer information through FIPS-certified encryption of all in-flight data 24/7
- Leverage flexible bandwidth offerings at wire speed with no impact on financial application performance
- Benefit from a simple, integrated encryption management approach that partitions encryption management from transport management to allow the service provider or FSI networking team to manage the network while the security team maintains full control of the encryption security parameters associated with their critical customer data, issuing new keys or certificates as required by their security policies

Encryption of data at rest and in flight is not mutually exclusive. Both are typically implemented in conjunction and complement each other as part of a holistic security strategy. When deploying an in-depth, multi-tier data security strategy, FSI organizations must understand the use case, application, and compliance requirements. They should also ensure their chosen software or technology adheres to the highest level of encryption standards and algorithms, such as ECC 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 efficient and secure collaboration between financial stakeholders.

Visit the Ciena Community
Get answers to your questions