SSL/TLS Decryption: An Enterprise Network Service

Date: February 2016  Author: Jon Oltsik, Senior Principal Analyst

Abstract: ESG research points to a growing trend: Large organizations are encrypting more network traffic. Yes, this can protect data communication’s confidentiality and integrity, but it also creates blind spots around network monitoring and security analytics. This is troubling as cyber-adversaries regularly use encrypted network channels for malware distribution, command-and-control communications, and data exfiltration. SSL/TLS termination devices can help, but a tactical approach based upon appliances alone often leads to performance problems, network modifications, and operational overhead. So what’s needed? An SSL/TLS decryption “service” built into the network itself. An SSL decryption service centralizes the overhead of SSL decryption and policy while feeding network traffic to security monitoring tools for further analysis. Organizations looking for a more strategic approach to SSL/TLS decryption may benefit from reaching out to Gigamon for help.

Overview

According to ESG research, one-third of enterprise cybersecurity professionals (i.e., more than 1,000 employees) say that between 26% and 50% of their organization’s network traffic is encrypted today. Furthermore, 88% of organizations believe that they will increase their use of network encryption in the next 24 months.

Network encryption is a bit of a mixed blessing: It protects data confidentiality and integrity of network traffic, but it can also impede an organization’s security defense because:

- **Cyber-adversaries use encrypted channels to camouflage attacks.** Recognizing the growing use of network encryption, sophisticated hackers are using SSL/TLS to obfuscate cyber-attacks. For example, when a malware downloader dubbed “Uptare” was revised in 2015, it adopted SSL/TLS over port 443 as a means for hiding communications between compromised clients and command-and-control (C2) servers. Other researchers have noted similar trends with SSL/TLS communications used for malware distribution and data exfiltration.

- **SOC teams become blind to encrypted network traffic.** Security analysts and operations staff depend on a myriad of network forensic and analytics tools that can help them prevent, detect, and respond to cyber-attacks. However, as more cyber-attackers embrace network encryption, these high-end network security monitoring tools become far less effective.

---

Cybersecurity professionals recognize that these issues can greatly increase IT risk. According to ESG research, 22% of organizations say they are extremely vulnerable to cyber-attacks that use SSL/TLS channels while another 40% believe that their organizations are somewhat vulnerable to cyber-attacks that use SSL/TLS channels (see Figure 1).²

FIGURE 1. Organizations’ Level of Vulnerability to Cybersecurity Attacks Using SSL/TLS Encryption

In your opinion, is your organization vulnerable to some type of cybersecurity attack (e.g., APT, data exfiltration, insider threat, etc.) that uses SSL/TLS encryption as a cloaking technique to circumvent your existing security controls? (Percent of respondents, N=150)

- Extremely vulnerable, 22%
- Somewhat vulnerable, 40%
- Not very vulnerable, 31%
- Not at all vulnerable, 6%
- Don’t know, 1%

Source: Enterprise Strategy Group, 2016

Network Encryption and Security

Recognizing their vulnerability to cybersecurity attacks that use SSL/TLS encryption, security and network operations teams often utilize SSL/TLS decryption capabilities on next-generation firewalls or implement SSL decryption appliances at the network perimeter. These approaches can decrypt traffic, providing some relief, but often come with an assortment of issues including:

- **Performance problems.** Cryptographic processing is notorious for its hardware consumption. Many security professionals complain that SSL/TLS decryption operations can “bring the firewall to its knees,” slowing down all other network security operations. This approach can’t scale to accommodate the growing use of network encryption.

- **Certificate and key management.** SSL/TLS decryption acts as a proxy for applications and client browsers. This “man-in-the-middle” approach requires a number of management tasks for digital certificate and encryption key management that can be complex and time-consuming. Human error is common, leaving organizations vulnerable to certificate theft, credentials harvesting, and service outages.

- **Operations overhead.** Deploying and operating an army of SSL decryption appliances demands staff time and focus. Overwhelmed network and security groups may not have ample resources for these additional tasks. While firewalls

² Source: ibid.
and proxies do have native SSL decryption, this approach can lead to repeated encryption and decryption of SSL streams, slowing down network speeds apart from the obvious management issues. Customers are looking for the “decrypt once, feed many security appliances” approach where traffic is decrypted, inspected, and re-encrypted, causing minimal network performance overhead.

What’s Needed?

Rather than approach SSL/TLS decryption on an as-needed basis, CISOs should work with the network operations team on a more strategic approach as today’s requirements will only increase in the future. ESG believes that a strategic approach to SSL/TLS encryption includes:

- **An SSL/TLS decryption “service” everywhere on the network.** Rather than a series of network boxes, large organizations should think in terms of a distributed and ubiquitous SSL/TLS decryption “service” deployed across the entire network. This service should be built with a combination of central management (i.e., policy management, certificate management, configuration management, reporting, etc.) and distributed decryption capabilities at the network perimeter, SOC, data centers, remote offices, etc. The SSL/TLS decryption service must also be easy to deploy and provide for today’s virtual networks and cloud-based workloads.

- **Advanced processing and network traffic management for integration with security tools.** Once traffic is decrypted, an SSL/TLS decryption service should be able to process and forward traffic to various security tools (e.g., NGFW, IDS/IPS, malware analysis, and security analytics) for further content inspection. Again, these operations should be centrally managed and allow for customization. For example, certain network sessions may be trusted and thus precluded from further inspection, while other traffic may require inspection from a myriad of security tools simultaneously. These rule sets must be easy to configure and operate.

- **Minimal performance and architectural impact on the network.** Production networks are built for transporting Ethernet frames and IP packets from source to destination as quickly as possible. Any “bump on the wire” can impact throughput—and user productivity. An SSL/TLS decryption service can’t get in the way of network throughput; rather, it must offload cryptographic operations and traffic forwarding to dedicated processors that can decrypt, process, and route network traffic across a dedicated and non-intrusive channel.

Enter Gigamon

Gigamon is one of few vendors that can help organizations build an SSL/TLS service with the standards described. Gigamon provides products and services for improving visibility into IT infrastructure and thus enhances application performance, network performance, and security protection. As part of its portfolio, Gigamon addresses SSL/TLS decryption with its infrastructure and applications such as:

- **Security Delivery Platform.** Gigamon provides products and services for pervasive visibility into traffic flowing among devices, users, and applications as well as physical and virtual SDN/NFV environments, and cloud-based workloads. This can enable organizations to deploy SSL/TLS decryption services in the right places on the network.

- **GigaSMART traffic intelligence.** GigaSMART applications can be used to help organizations optimize how network traffic is sent to security monitoring and threat detection tools. GigaSMART functions, for instance, can deduplicate packets, isolate applications, remove headers that hamper interoperability, and generally ensure that the right traffic and network metadata is sent to the right tools. SOC staff can develop service chains for traffic visibility needs such as deduplicating packet data, stripping VLAN headers, and generating NetFlow data. Further, with Application Session
Filtering, security teams can identify SSL streams across any port (not just well-known ports such as 443) for inspection. With SSL being used increasingly for VoIP and email, this becomes more important.

All of these Gigamon services roll up to GigaSECURE, a platform designed to provide end-to-end visibility of network traffic, users, applications, and suspicious activities to numerous security tools like IPSs, anti-malware gateways, and security analytics systems. SSL/TLS decryption is a core service of GigaSECURE. In this way, Gigamon can help enable an SSL/TLS decryption service that aligns with today’s enterprise requirements.

The Bigger Truth

As the old saying goes, “Security is a process not a product.” In other words, strong security demands coordination, defined workflows, and constant orchestration across cross-domain processes and a variety of security controls.

Rather than thinking of SSL/TLS decryption as a network appliance, cybersecurity professionals should view it as a service that should be tightly coupled to security monitoring and analytics. Organizations that understand this distinction should take the next step by making SSL/TLS decryption a part of an end-to-end network infrastructure. By doing so, CISOs can improve security visibility and gain the real-time intelligence needed to improve risk management decisions and incident response for their organizations.