ARTICLE

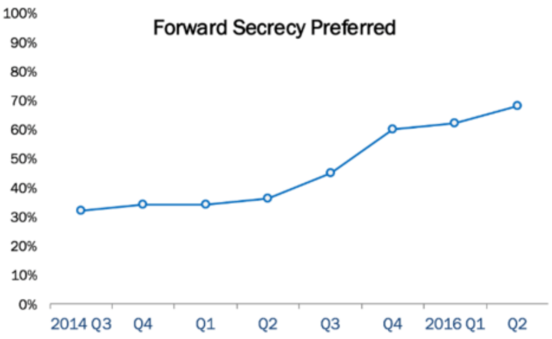
The Expectation of SSL Everywhere

Written by: David Holmes

Date: July 2014

***Author update: July 2016** — My lifelong fascination with cryptography inspired this story, which I had the pleasure of writing two years ago. That's a long time in "Internet" years, yet the story is still as relevant today as it was then. The data I've continued to collect since 2014 indicates a strong preference for Forward Secrecy—a double SSL encryption technique that prevents snooping forward in time. In fact, its use has more than doubled, from 32% to 69%.*

—David Holmes



The security of data in transit has traditionally been the purview of nation states. Now, the global adoption of the World Wide Web is bringing cryptography to the common man. But the forces of malicious actors and eavesdroppers are moving nearly all significant communication and commerce into a single cryptographic protocol: SSL.

SSL is the set of cryptographic protocols that secure data in transit. Today SSL is often the only tool standing between an eavesdropper and a target, or a thief and a merchant. The stakes around SSL have been up-leveled to the limit. Whether or not it's convenient to admit, it's time for organizations to up-level their overall security posture to protect this last line of defense.

BRINGING CRYPTOGRAPHY TO THE COMMON MAN

Long before the digital age, those in power used cryptography to defend their interests—or to inflict damage on their enemies. The Roman ruler Julius Caesar was known to use ciphers to protect messages of military significance. In the Common Era, embedded ambassadors used ciphers to protect their communications with their sovereigns at home. Mary, Queen of Scots, was implicated in a regicide attempt via cryptanalysis. From Victorian England throughout the World Wars, cryptography remained in the hands of the agencies that used it in the same way it had been used before: for intelligence purposes toward the protection of the Church or the State.

Then a strange thing happened with the global adoption of the World Wide Web. Suddenly, people around the world gained the ability to freely communicate with each other. At first, discussions centered on technical concepts related to the building of the infrastructure itself, and then around images of kittens. Now, wherever civic dialogue is taking place, people are using social media to communicate. But the public nature of social media allows interested agencies to monitor those communications. Right-to-privacy advocates looked to cryptography to solve this problem.

For the first time in history, cryptography—in the form of SSL—is now being used to protect not just the interests of the powerful, but the communications of the common man, as well. The common man is starting to expect the use of SSL everywhere (see Figure 1), not only to protect privacy but, of course, also to prevent common larceny via cyber theft. To meet these expectations, global organizations must embrace a broader, higher security posture to protect SSL, the last line of defense for communication and commerce.

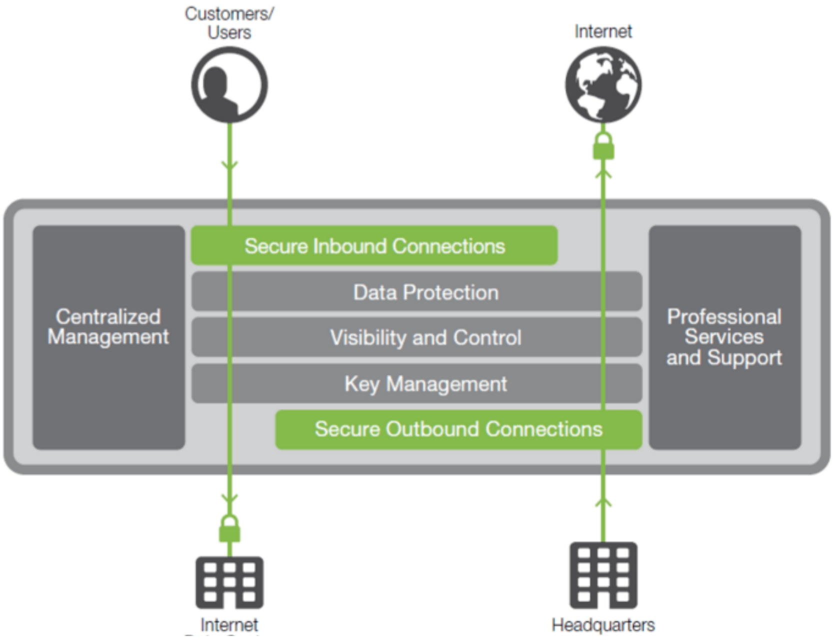


Figure 1: The F5 SSL Everywhere solution

ELEVATING SECURITY POSTURE

The proper deployment of SSL can be daunting, even for seasoned administrators. The good news is that there are groups that can provide guidelines (beyond those recommended in this paper) to assist in the deployment and evaluation of a proper SSL security posture. The Open Web Application Security Project (OWASP) maintains a best practices guide for SSL. The SSL Labs project provides a comprehensive test tool that can assist administrators in evaluating their site's security posture. Among the practices recommended are methods for future-proofing ciphertext, achieving optimal key storage, and refactoring for resilient security architecture.

COUNTER PASSIVE SURVEILLANCE WITH FORWARD SECRECY

In 2013, allegations were raised that state intelligence agencies may have been performing broad-spectrum data collection against citizens in the United States, Europe and, indeed, throughout the world. The target data was alleged to include metadata about mobile phone calls, the text for the SMS messages, and even the collection of encrypted data (ciphertext) of email and other conversations.

Even if an organization lies outside the jurisdiction of a state agency, that agency may be able to tap and record the organization's ciphertext and metadata for years. In the future, the agency may gain access to the key material that enables it to finally decrypt the millions of messages it has saved. This problem of long-term key compromise means messages that are safe today may not remain so in the future.

SSL has a passive surveillance countermeasure called Perfect Forward Secrecy (PFS) protection that adds an additional exchange to the key establishment protocol between the two sides of the SSL connection. When PFS is enabled, an attacker or eavesdropper cannot simply recover a single key to decrypt millions of previously recorded conversations. Because PFS can be achieved by simply activating an additional cryptographic cipher (which is built into the SSL termination device itself), social media providers and other privacy-concerned organizations are quickly adopting it around the world.

PROTECT KEY MATERIAL WITH ADVANCED STORAGE ARCHITECTURE

In the spring of 2014, the world was horrified to learn that a pernicious software error (since named

Heartbleed) in the popular OpenSSL library had been available to exploit in millions of websites for more than two years. Heartbleed, so named because of the code's location in the "heartbeat" code of the library, had a devastating effect—it would quietly leak the contents of the device's memory to the attacker. If anyone had known about Heartbleed before it was officially discovered in 2014, they could have been probing much of the Internet, collecting the most high-profile assets (such as private keys and server administrator passwords) without activating alerts or leaving traces in any instrumentation. Heartbleed will likely be recorded as one of the most severe Internet vulnerabilities of all time.

In the Heartbleed incident, one class of SSL users could be confident that they were not vulnerable: users of FIPS 140-2 hardware security modules (HSMs). An HSM is a separate software and hardware security boundary around a cryptographic core and key store. Keys are typically generated inside the store and never leave it. Because the keys are never transferred into the memory of the network host, they could not be leaked to Heartbleed.

HSM devices follow the strict FIPS 140-2 cryptographic design guidelines, and they can be costly. Financial and federal institutions have been using them for years and have found ways to increase their value in terms of both management and cost-efficiency. Organizations are using HSM devices as centralized key stores (for example, one pair per data center), meaning that the amount of interface training and operational overhead is centralized as well. The centralized HSMs are accessible over the internal network to services that need key decryption (see Figure 2), so the organization saves on capital and operational costs, as well.

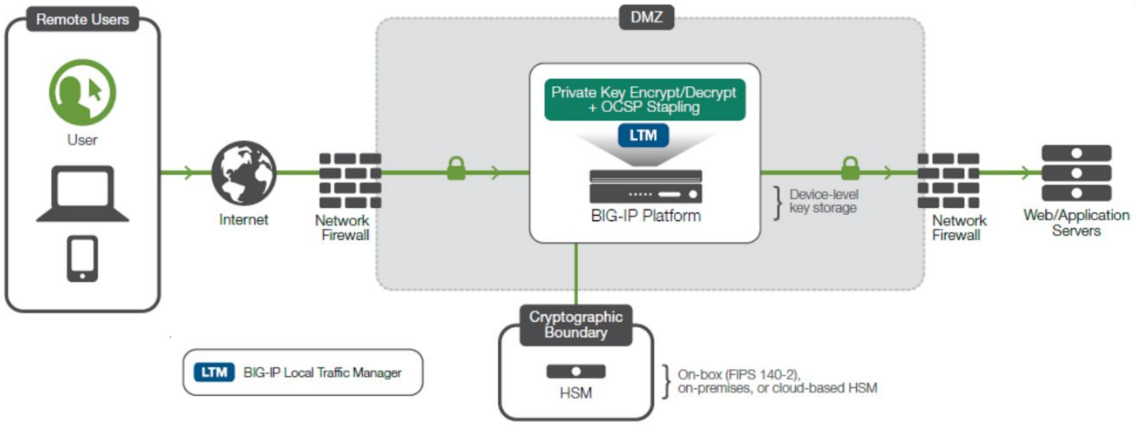


Figure 2: Advanced key storage is enabling cloud security

Network-attached HSMs (netHSMs) are appearing within remote data centers and private clouds. They make it possible for enterprise operations from one data center to request decryption services from a remote data center. NetHSMs are even appearing in public clouds. Organizations pair these public netHSM (so-called CloudHSM) devices with sister devices within the enterprise data center and then use centralized security controls, such as Application Delivery Controllers, to meter requests between them. The HSM devices (in private, network, or cloud configuration), along with forward secrecy, are becoming part of the fabric of the new SSL security posture.

PROTECT EVERYTHING WITH "ALWAYS-ON" SSL EVERYWHERE

Forrester Research security analyst John Kindervag writes of an approach to security called the Zero Trust Model (ZTM). The premise of ZTM is that architecture is much more robust with regards to security if every component in the network distrusts every other component and treats all inter-device traffic as if it had already bypassed other security measures. There is adoption around this model in many network architectures, especially ones where security boundaries are particularly porous, such as enterprise-to-cloud and business-to-business-to-cloud.

Embracing a model where sources are always untrustworthy means protecting data in transit, even within the organization itself. The Forrester model centers on a "network segmentation gateway" that provides security and availability services over multiple high-speed links into each network zone (see Figure 3). The device in question must have a lot more insight into packet data, including into the application layer. In order to operate on application layer data, the device must decrypt it first and then, to adhere to the tenets of ZTM, re-encrypt when done. For years, re-encryption of SSL data after security analysis was a practice found only in the financial sector, as driven by organizations' internal security policies, but it is now gaining wider adoption.

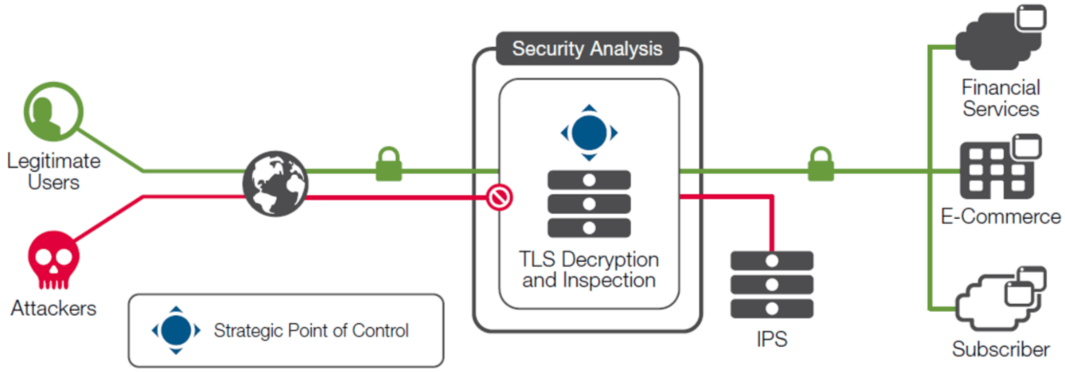


Figure 3: The Zero Trust Model may require re-encryption within the enterprise data center

The re-encryption of data within the organization aligns exactly with ZTM as it protects data from hosts within the network that may be compromised by attackers or surveillance agencies. However, it may also hide data from security analysis devices such as intrusion detection systems, flow monitors, and web application firewalls.

CONCLUSION

Whether the world wants to admit it or not, the stakes around Internet security have been raised into the same spheres as human rights, freedom of speech, and free commerce. Yet, IT directors may look at PFS, HSMs, and ZTM and grumble that these are non-trivial investments that do not appear to add value to the bottom line of a commercial organization. And, if done improperly, wrapping data within SSL sessions throughout the network may protect the data from prying eyes at the cost of creating blind spots for the organization.

The good news is that these concerns are not insurmountable. Many organizations are solving these security challenges today with innovative architecture that meets the new security posture required by the perilous world that we now live in.

ABOUT F5 LABS

F5 Labs combines the threat intelligence data we collect with the expertise of our security researchers to provide global, actionable intelligence on current cyber threats—and to identify future trends. We look at everything from threat actors, to the nature and source of attacks, to post-attack analysis of significant incidents to create a comprehensive view of the threat landscape. From the newest malware variants to zero-day exploits and attack trends, F5 Labs is where you'll find the latest insights from F5's threat intelligence team.

F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com