Enterprise Solutions for TLS Offloading, Acceleration, and Termination

What is Transport Layer Security (TLS)?

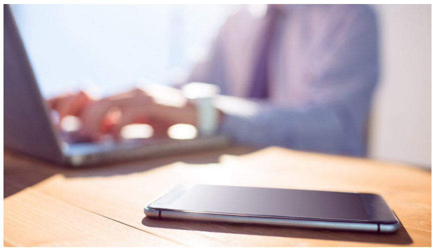
TLS, or Transport Layer Security, is a cryptographic protocol used to prevent eavesdropping on data sent between two points. One of the most common uses of this is to secure the connection between web browsers and web servers that serve content, enable communication, and accept electronic payments. Both TLS and its predecessor Secure Sockets Layer (SSL) rely on public key cryptography. They can be used to secure any number of applications, such as web browsing, e-mail, instant messaging, and more. After establishing an encrypted connection using a process known as a TLS handshake, the endpoint device and server are mutually authenticated and can share information freely.

What is TLS used for?

The purpose of TLS is to add confidentiality and integrity to the exchange of information. TLS is most frequently used to secure web traffic either between a browser and the web server, or between two users. It ensures that communication between users is private by encrypting the connection between each point. Using TLS, secure connections can be established on a one-to-one or one-to-many basis, allowing the secure sharing of information between two parties or large groups.

SSL & TLS: What's the difference?

Over time, both SSL and TLS have served as commonly used industry protocols for encryption. However, SSL is the predecessor of TLS.



SSL was introduced by Netscape Communication Corporation in 1994, for the purpose of securing web transactions. SSL underwent a number of revisions, culminating with the release of SSLv3 in 1996. With the goal of standardizing the protocol, the Internet Engineering Task Force (IETF) released TLS 1.0 in 1999.

Although the differences between TLS 1.0 and SSLv3 are minor, TLS 1.0 uses stronger cryptography and adds protection against certain attacks. In June of 2015, the IETF officially deprecated SSLv3 and recommended organizations move to TLS version 1.2.

Software Vs. Hardware TLS: At-A-Glance Comparison

While software and FIPS 140-2 Level 3 validated hardware solutions for processing TLS traffic are similar in many respects, the following comparisons outline several notable differences between the two types of solutions:

Cryptographic Key Management

Software: When keys used for securing TLS connections are managed in software, a significant risk of compromise by external attackers or malicious insiders is introduced.

Hardware: With a FIPS 140-2 Level 3 validated hardware security module (HSM), the full key management lifecycle is managed within a secure, tamper-responsive device. From initial generation of keys to issuance, modification, revocation, and destruction, the entire process is protected.

Scalability

Software: Scaling software-based TLS processing often requires multiple devices to be added, ranging from web servers to load balancers, firewalls, switches, and more.

Hardware: Purpose-built hardware designed for TLS acceleration means that fewer additional servers are required, resulting in a less complex integration effort.

Processing and Throughput

Software: In the example of website protection, the growing use of TLS to protect generic traffic rather than just login credentials and eCommerce data has dramatically increased the processing burden on web server CPUs.

Hardware: Moving the TLS negotiation, or handshake, into hardware allows dedicated resources to handle the most computationally resource-intensive portion of the process.

Tamper Responsiveness

Software: Able to detect some forms of intrusion attempts, but the ability to respond to physical attacks is limited.

Hardware: FIPS 140-2 Level 3 validated hardware contains physical controls over the integrity of the cryptographic boundary, temperature, voltage, and more to instantly erase sensitive data in the event of an intrusion attempt.

Regulatory Compliance

Software: Additional controls and compliance requirements are often put in place for software-based systems.

Hardware: The scope and cost of compliance can often be reduced, simplifying audits and saving time and money.

Problems with Software-Only Implementations of TLS

Software-only methods of TLS encryption introduce security risks to users by allowing cryptographic keys to reside in clear-text within the server the applications are operated from. Whereas hardware-based solutions protect the full key management lifecycle using a tamper-responsive hardware security module, software offerings leave cryptographic keys relatively unprotected. Through key logging, memory scanning, or even inadvertent misconfiguration by administrators, cryptographic keys can be accessed and used for malicious purpose. With hardware protection, keys are always protected within a dedicated device and any tamper attempt will result in the immediate clearing of the sensitive information.

Saturation of CPU resources is another issue often seen when using software-only models of TLS encryption. The TLS negotiation, or handshake, requires significantly greater processing power than the actual encryption and decryption of the transmitted data. When the task of performing the handshake falls to the web or application server, resources can become strained. This is especially true when considering the increasing percentage of traffic that organizations are choosing to pass through a TLS-encrypted channel.

To analyze the impact of CPU saturation in this scenario, Rice University conducted a comprehensive performance analysis of TLS-enabled web servers. The study found that by offloading TLS responsibilities to a separate CPU, the web server improved processing speeds by 44-61%. By using a dedicated cryptographic device for this, organizations can increase response time for end users and ensure the capability to scale seamlessly over time.

The Growing Use of TLS Encryption

Historically, usernames and passwords, as well as eCommerce data, were the primary areas where TLS encryption was used. TLS encryption was viewed as optional for web pages without high-security data.

Now, many business applications, websites, and social networks are using TLS on all pages by default to ensure user privacy. Across a broad range of devices, TLS encryption has become a standard.

Many large web service providers have announced plans to enable TLS on greater portions of their service offerings.

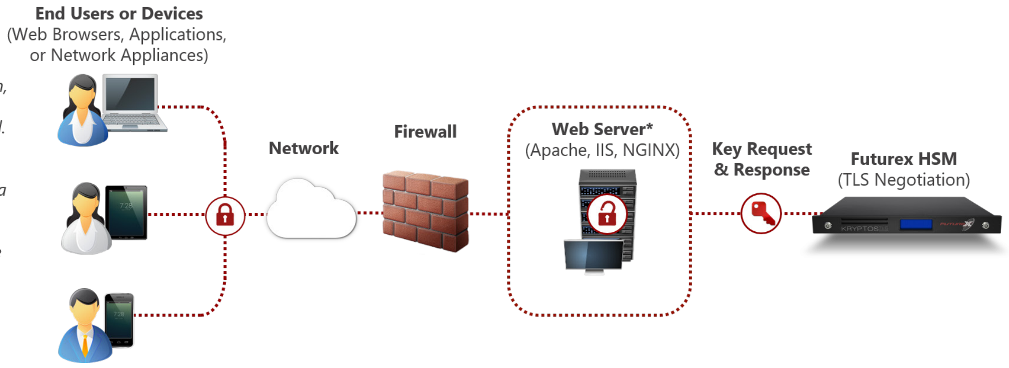
In 2013, Facebook announced the incorporation of TLS encryption for over one billion users. Likewise, Google has pledged to enable TLS encryption on all pages accessed through search. In March of 2014, Google began moving to HTTPS for Gmail. Through these and other similar initiatives, the Internet continues to move towards encrypted connections as the norm, slowly eliminating the practice of unencrypted web traffic.

Use Cases for Offloading TLS Negotiation to a Dedicated, FIPS 140-2 Level 3 Validated Hardware Security Module

There are numerous applications for offloading TLS negotiation to a FIPS 140-2 Level 3 validated hardware security module:

- Private key storage and management of the full key lifecycle for web and application servers.
- Removal of the TLS negotiation burden from resource-limited servers to improve end user response times and provide additional capacity for growth without requiring new hardware purchases.
- Private key storage for network appliances, such as switches, firewalls, and load balancers.
- Host and client-neutral addition of TLS to applications that do not currently support it, or those that use deprecated ciphers.
- Reduction of the scope and cost of compliance audits.

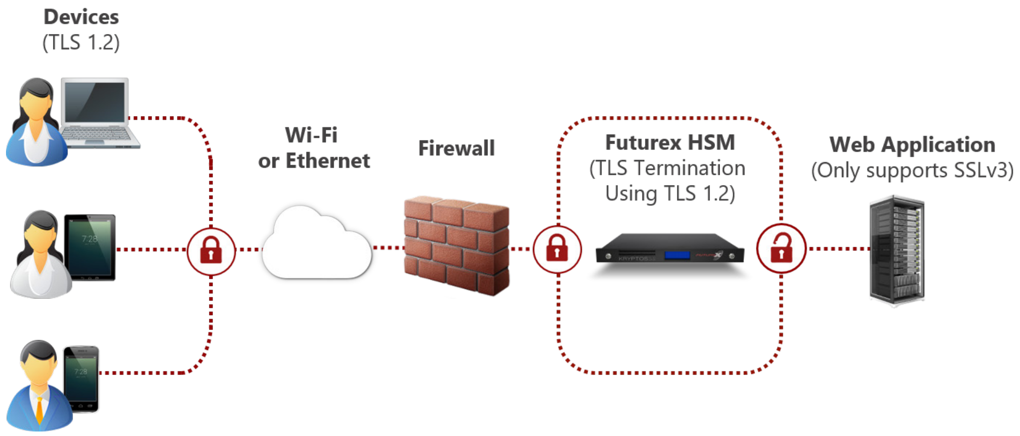
Use Case #1: Private Key Storage for TLS Handshake Offloading (Web Servers, Applications, Network Appliances)



For this simplified diagram, the example of protecting web browser data was used.

The same overall structure applies to protection of data for network appliances, generic web applications, and other uses taking place either over a Wide Area Network or within a Local Area Network.

Use Case #2 TLS Termination for Applications without TLS or only Supporting Deprecated Ciphers



Benefits of TLS Offloading and Acceleration using Hardware

The benefits of using hardware security modules for TLS offloading are far-reaching. By using a secure cryptographic device, organizations leverage greater security, ease of deployment, fulfillment of compliance requirements, and increases in processing power.

Hardened cryptography is used to establish the root of trust in an enterprise IT ecosystem. Without assurance that sensitive data will be kept secure and unmodified, user confidence will remain low and the risk of a data breach will be high. With a hardened cryptographic solution, TLS negotiation is offloaded to a FIPS 140-2 Level 3 validated hardware security module, and keys are never stored in the clear. Customer and end-user data is protected, and the risk of financial and reputation penalty for data breaches is significantly reduced. The full key management lifecycle is always managed within the HSM's secure boundary, giving all stakeholders the confidence that the most rigorous measures are being taken to protect their data.

Futurex's easy-to-implement technology provides solutions for host and client-neutral scenarios involving the protection of TLS traffic. In many scenarios, little or no modifications are required to existing host or client systems. Additionally, multiple applications and clients can connect to the same Futurex devices, streamlining organizational processes, decreasing the time spent configuring devices, and enabling organizations to achieve ROI sooner.

With a designated device to offload TLS negotiation, users remove bottlenecks on web and application servers by handling the most computationally resource-intense portion of the process in hardware. This relieves the servers from performing these tasks, and expedites processing by using hardware that is purpose-built for TLS encryption.

Organizations can also fulfill industry compliance requirements and best practices by offloading cryptographic tasks to hardware security modules. Cryptographic hardware from Futurex is applicable to a wide range of uses outside of the use cases for TLS defined in this document. This allows for a diverse range of functionality to be performed from a single device. In addition to this, organizations can leverage the VirtuCrypt Hardened Enterprise Security Cloud for service-based deployments of this same technology.

As organizations increasingly adopt TLS to protect their most sensitive data for transmission via the web, Futurex will continue expanding the role of the Hardened Enterprise Security Platform to fulfill critical needs within this environment. By managing the most cryptographically sensitive and resource-intensive portions of TLS encryption using hardened, FIPS 140-2 Level 3 validated technology, organizations can ensure the confidentiality and integrity of their data, allowing them to maintain focus on providing the best possible products and services to their end-users.

Sources

Coarfa, Cristian, Peter Druschel, and Dan Wallach. Performance Analysis of TLS Web Servers. Report. Rice University: Department of Computer Science, 2006.

Langley, Adam. "A Roster of TLS Cipher Suites Weaknesses." Google Online Security Blog. November 14, 2013. Accessed October 28, 2016. https://security.googleblog.com/2013/11/a-roster-of-tls-cipher-suites-weaknesses.html.

"Secure Browsing by Default." Facebook. Accessed October 28, 2016. https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920.

"Transparency Report." Google. Accessed October 28, 2016. https://www.google.com/transparencyreport/https/?hl=en.

FUTUREX.COM