GALLAGHER PR

A New Way to Secure SSL/TLS Traffic

Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are the primary means of securing traffic between web browsers and web servers. Organizations need to detect and prevent network-based compromises that can be carried through SSL/TLS traffic, but many legacy solutions present problems. SSL/TLS interception is usually achieved by proxying the encrypted sessions through an in-line security device or software daemon which terminates the SSL/TLS session, decrypts the content and re-encrypts it before communicating with the intended recipient. Some issues associated with such in-line architecture include the need for an in-line device and the related cost, latency increases, decreased network availability and potential security exposure. In this article, we'll look at a new way to inspect SSL/TLS traffic that does not require an in-line device and thus overcomes traditional challenges.

The SSL/TLS Attack Vector

Any exploit that can be carried out in regular traffic can be carried out over SSL/TLS. Because the session is encrypted, it makes exploits harder to detect. Sometimes, the same exploit can be carried out over SSL and non-SSL. SSL can hide applications that the enterprise doesn't want, such as peer-to-peer systems or instant messaging apps. Most organizations have policies in place that prevent certain content from being posted to public sites, and they want to be able to enforce these policies about what can travel on the network. But SSL-encrypted traffic makes it difficult to enforce those policies.

In terms of malware, a network analyst can't find virus exploits or other attacks that use SSL/TLS to communicate. The alternative is to monitor endpoint addresses, but endpoint addresses change frequently, leading to false positives and false negatives. In addition, users may use SSL/TLS to download executables, and it's difficult to block that traffic if it can't be detected. For example, most phishing and pharming attacks occur in SSL/TLS traffic.

Traditional SSL/TLS Monitoring

The traditional method of dealing with this challenge is to buy an in-line device that decrypts SSL/TLS traffic, inspects it, and then re-encrypts it. There are several issues with this approach.

In the first place, many organizations don't own their own networks anymore, and it's not possible to deploy an in-line device in the cloud. Networks are increasingly virtualized.

Even when such a device is used in an in-house network, it causes problems. One issue is increased latency: because there's a box in the middle of the traffic that has to decrypt, inspect, and encrypt the data stream before passing it onto the server, the user will experience higher latency in the connection. SSL/TLS inspection device manufacturers try to mitigate latency by adding processing power to their systems, but this increases the cost of the device. In-line inspection devices can cost from $20,000 to $150,000, depending on processing capacity.

Reliability is another issue. If the in-line device goes down, so does access to the network. And the in-line device needn't fail to interrupt network access. Browser-server configurations change frequently, and these devices aren't always up to date, so they can deny legitimate traffic.

In addition, the in-line device is responsible for the cryptographic keys that enforce security on the connection. These cryptographic keys may not be configured correctly, and misconfigurations can also interfere with network access.

From a broader perspective, the in-line device essentially becomes the arbiter of what the user can and can't see, thereby violating the end-to-end relationship between the user and the website.

For more information on these issues, see the Carnegie Mellon blog by Will Dormann, "The Risks of SSL Inspection," and CISA Alert number TA17-075A, "HTTPS Interception Weakens TLS Security."

In virtualized networks, users need to implement SSL/TLS interception functionality in software. The problem with this approach is that software and the server CPU don't have the capacity to handle real-time traffic flows between the client and the server. Decryption and encryption are very CPU-intensive, and the traffic can overwhelm the software and CPU when the software is inspecting traffic from multiple endpoints to multiple servers.

Endpoint SSL/TLS Monitoring

Because in-line SSL/TLS inspection has so many drawbacks, there's a need for a different approach. Instead of running the inspection capability in the network, it can be run in the endpoints. This is accomplished by running an agent on each endpoint to collect traffic in clear text (before it is encrypted for transmission over the network), and by sending those results to a server-based or virtual machine-based sensor for inspection and correlation.

Basically, the agent is a transparent tap into the endpoint's traffic, and it makes a memory copy. This passive SSL/TLS inspection occurs on the endpoints before the traffic is encrypted and sent to the server, so it doesn't interfere with traffic between the client and server at all (see Figure 1).

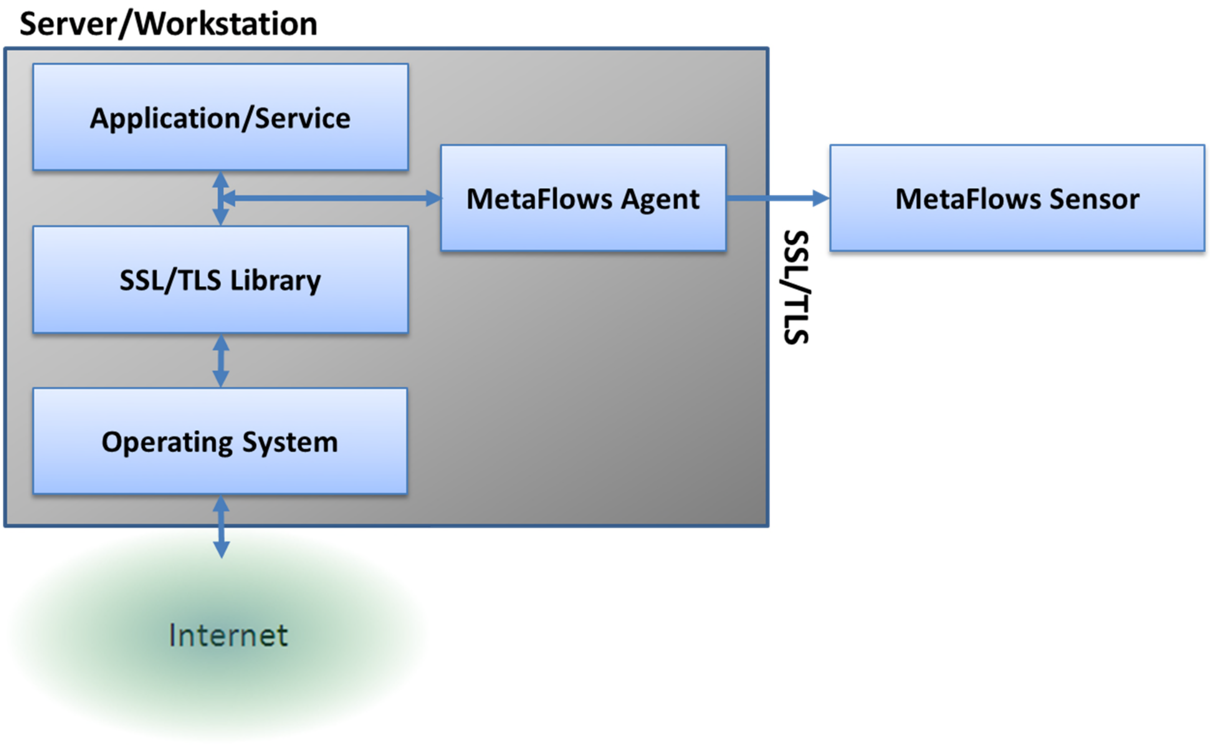

Figure 1: Endpoint traffic monitoring.

This approach has several advantages. There's no increased latency because the agent doesn't interfere with the network traffic. If the agent stops working for some reason, it doesn't interfere with the endpoint user's activity. The agent also has nothing to do with the cryptographic keys, so there are no security or configuration issues. Finally, the endpoint software agent can do full packet mirroring (which may or not be a requirement, especially on physical networks). Some cloud vendors now have mirroring functions as well.

To produce an overall picture of traffic going to or from endpoints, the network sensor receives all the traffic from the endpoints and analyzes it to look for problems. The sensor could also double as a configuration management system, so end users don't have to configure endpoints manually.

Passive SSL/TLS inspection addresses the major problems of in-line inspection, maintains the one-to-one relationship between the endpoint and the server, and enables network analysts to see what's being transmitted over secure sessions. As networks become increasingly virtualized, endpoint SSL/TLS inspection will be the only way to see and react to network exploits conducted via encrypted tunnels between browsers and web servers.