FPKIPA

Federal Public Key Infastructure Policy Authority

SSL/TLS Inspection and Mutually Authenticated SSL/TLS

Version 1.0.0

November 20, 2009

Summary

Mutually authenticated SSL/TLS technology is commonly used within the Federal Government to attain strong authentication of users to web sites using their PKI credentials (e.g., PIV authentication certificates). This document is intended to inform the Federal PKI community regarding a technical issue that arises when web proxies attempt to inspect mutually authenticated SSL/TLS communication.

Web proxies (or HTTP proxies) that provide SSL/TLS inspection enable organizations to enforce Internet usage policies and monitor web traffic that would otherwise be encrypted between the web site and the user (i.e., user's web browser). However, an error occurs when these proxies attempt to insert themselves into traffic where the user needs to perform mutually authenticated SSL/TLS (i.e., certificate-based authentication) with the web site. This error is caused by the proxy altering packets that are signed by the user's private key. As a result, sites that require mutual SSL/TLS cannot be proxied successfully. The technical issue is explained below along with one approach to circumventing the issue.

Overview of Web Proxies with SSL/TLS inspection

Web proxies have proven themselves valuable for enforcing online usage policies and protecting against harmful content (i.e., monitoring and filtering web browser content). Benefits of filtering web traffic include:

- Managing online productivity of employees
- Blocking the exchange of proprietary, sensitive, or inappropriate content
- Preventing the transmission of viruses and malware

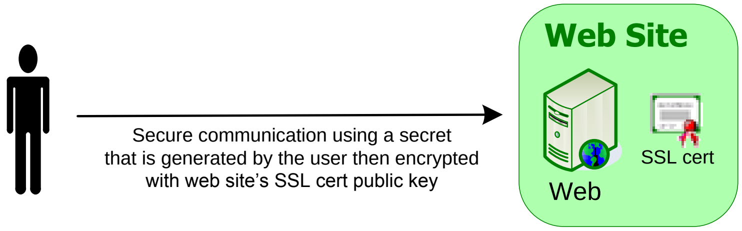
In the past, the benefits of web proxies could not be realized if the user connected to a web site over SSL/TLS. Now, web proxies that include SSL/TLS inspection functionality make it possible to realize these benefits even when SSL/TLS is used (mutually authenticated SSL/TLS is an exception that is discussed below).

To understand how SSL/TLS inspection works, one should understand that SSL/TLS establishes secure point-to-point communication between a client and a server using encryption. Normally, the two connection points consist of the user (client) and the target web site (server). Additionally, most SSL/TLS web traffic relies only on server authentication. That is, only the server presents a certificate and proves possession of the corresponding private key. During server authenticated SSL/TLS, the user generates a secret and encrypts it using the public key from the web site's certificate[1]. Thus, the secret is only shared between the user that generated it and the web site that can decrypt

[1] In actuality only part of the secret used to generate the symmetric key is generated by the client, but it is both common and helpful to leave this detail out for high-level discussions.

it. The shared secret is then used to generate a symmetric key that is used to encrypt the communication session.

Figure 1 - Server Authenticated SSL/TLS


Web Site
Secure communication using a secret that is generated by the user then encrypted with web site's SSL cert public key
SSL cert
Web

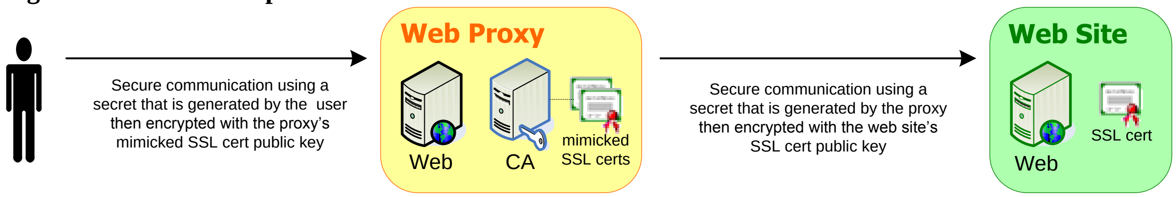
In order to monitor SSL/TLS traffic, the proxy must insert itself between the user and the target web site. To insert itself, the proxy establishes two point-to-point communication sessions. One point-to-point communication session is between the user and the proxy. The other communication session is between the proxy and the target web site. The user establishes an SSL/TLS connection with the proxy, and the proxy establishes its own SSL/TLS connection with the target web site.

It is important to note that web browsers are programmed not to connect to a web site whose certificate (a) is not trusted, and (b) does not match that of the web site[2]. In order to get the user's browser to connect, the web proxy uses a certificate authority that is trusted by the user's browser to generate a certificate mimicking that of the target web site. The certificate authority is usually contained within the proxy (i.e., the proxy acts as a CA) and is only trusted within the organization monitoring the web traffic. When the user attempts to connect to the target web site, the proxy:

1. intercepts the transmission;
2. establishes an SSL/TLS connection between itself and the target web site;
3. generates a certificate that mimics the target web site's certificate;
4. presents the mimicked certificate to the user's browser; and
5. establishes the SSL/TLS connection with the user.

As a result, the user's browser believes that it has connected directly to the target web site. Furthermore, the user is typically unaware that of the proxy's involvement as well.

Figure 2 - SSL/TLS inspection


Secure communication using a secret that is generated by the user then encrypted with the proxy's mimicked SSL cert public key
Web Proxy
Web
CA
mimicked SSL certs
Secure communication using a secret that is generated by the proxy then encrypted with the web site's SSL cert public key
Web Site
SSL cert
Web

[2] Typically, the certificate matches the web site when the web site's hostname is found in the Subject DN or the Subject Alternative Name of the certificate.

SSL/TLS inspection works for most SSL/TLS web traffic because most SSL/TLS web traffic only uses server authentication. However, mutually authenticated SSL/TLS is a clear case where SSL/TLS inspection fails.

Mutual Authentication Issue

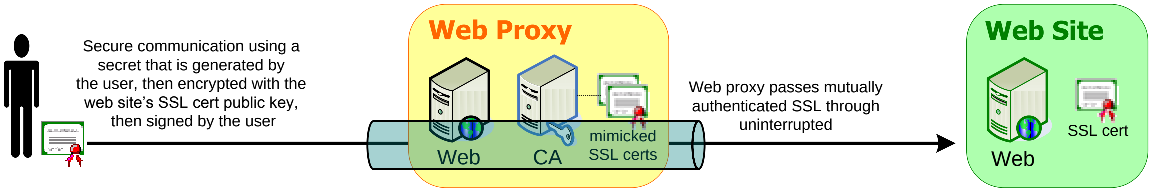
Mutually authenticated SSL/TLS is used for strong authentication of the user to the web site. It is designed to provide secure point-to-point communication where both the server and the client (i.e., user's browser) authenticate to one another. During mutually authenticated SSL/TSL, the client:

1. presents its certificate to the server;
2. generates a secret;
3. encrypts the secret using the web server's public key; and
4. digitally signs the secret that is encrypted for the server.

The client certificate and subsequent signature provide the server with the means to authenticate the user. In addition, by signing the secret, the client guarantees that it generated the secret and that it has not changed. Since we know that the client generated the secret and that only the server can decrypt it, we can be sure that the secure communication is point-to-point between the client and the server. As a result, a web proxy cannot insert itself between the user and the target web site successfully. Because the user signs the secret in mutually authenticated SSL/TLS a web proxy cannot alter the secret. Likewise, if the proxy signs a secret that it generates itself, then the web site cannot authenticate the user by matching the signature with the user's certificate. Simply put, at this time there is no way to perform SSL/TLS inspection of mutually authenticated SSL/TLS that does not interrupt the strong authentication process, which is the purpose of mutually authenticated SSL/TLS.

One solution is to not proxy SSL/TLS traffic to approved sites. Most web proxies can be configured to allow specific traffic to pass through uninterrupted. For example, at least one Federal Agency using SSL/TLS inspection opted not to proxy traffic to any web sites that end in ".gov" or ".mil". Similarly, if there are specific sites that are known to require mutually authenticated SSL/TLS, an organization could elect not to proxy those communications on a site-by-site basis.

Figure 3 – Uninspected Mutually Authenticated SSL/TLS


Secure communication using a secret that is generated by the user, then encrypted with the web site's SSL cert public key, then signed by the user
Web Proxy
Web
CA
mimicked SSL certs
Web proxy passes mutually authenticated SSL through uninterrupted
Web Site
SSL cert
Web