What is SSL Pinning? – A Quick Walk Through

In today's IT environment, technology keeps evolving, and endpoint devices like smartphones and tablets are sharing the similar kind of connection with the network infrastructure as web browsers do. Like web applications, mobile apps also involve a client-server relationship that relies on information being communicated back and forth between the senders and receivers. This same interplay between sending and receiving nodes provides attackers with an opportunity for intercepting privileged communications. Therefore, it becomes vital for businesses to adopt precautionary measures to protect their communication. One way of doing this is by using security protocols: SSL/TLS.

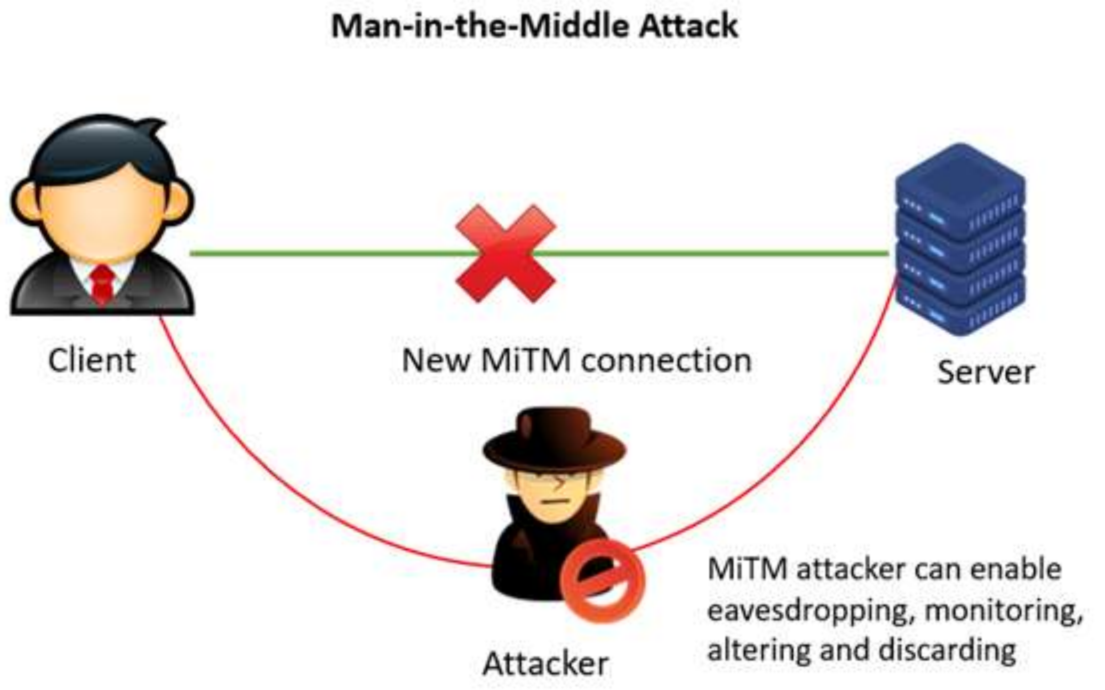
However, the increasing number of fraudulent CAs issuing fake SSL certificates triggers the bar for security, which necessitates SSL Pinning. In the remaining section of this blog, we will disclose what is SSL pinning and how it enhances the security of your business.

Security Protocols and Man-In-The-Middle Attack

Secure Socket Layer (SSL) and Transport Layer Security (TLS) ensure encrypted communication over the internet – specified as HTTPS. The security factors of SSL are based on the security certificates' "Chain of Trust." When a sender sent a message, the client checks the server's SSL certificate to confirm whether the certificate is issued by Trusted CA.

Although SSL/TLS communications are secure as well as unbreakable, the MITM (Man-in-the-Middle) attack still causes a threat to secure communication.

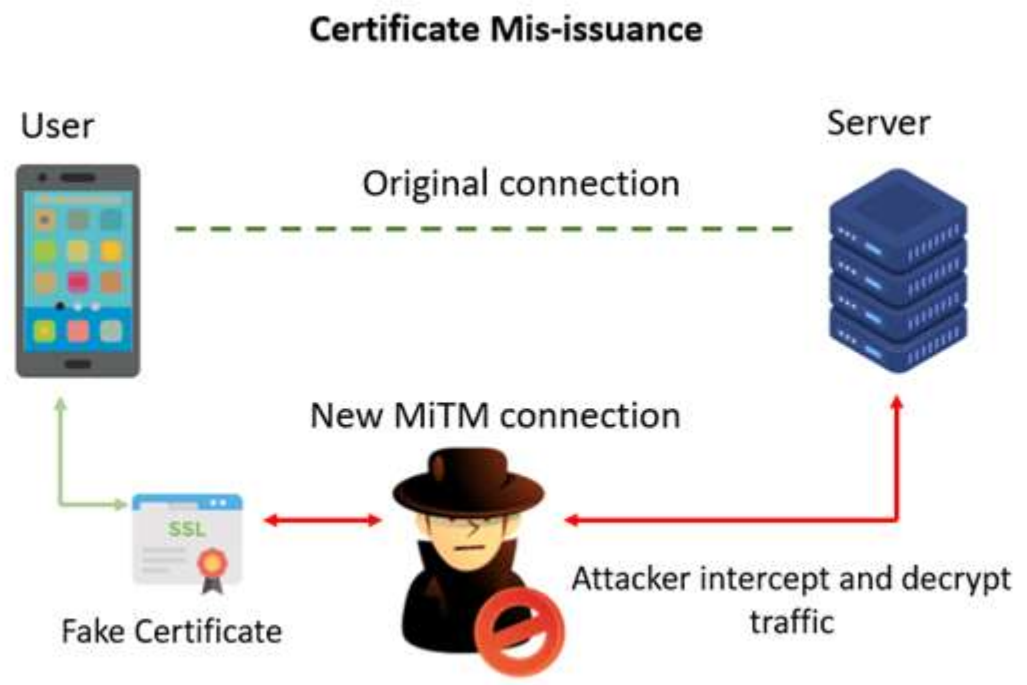
In MITM attacks, hackers managed to discover a loophole in the network communication and seek to be in the middle of communication between the app and the backend server with malicious intentions. The MITM attacks are dangerous since the hacker can read, alter, or even misuse the message between communicating parties. Hackers try various methods, including DNS spoofing and ARP cache poisoning to grab information.


Man-in-the-Middle Attack
Client
New MiTM connection
Server
Attacker
MiTM attacker can enable eavesdropping, monitoring, altering and discarding

Further, the HTTPs traffic can be seized by establishing malicious CA certificates employing tools like Burp, OWASP ZAP, and mitmproxy auto-generate CAs.

In this digital eavesdropping, cybercriminals enter as a proxy and begin communicating between two parties. Neither of them aware that a third person is in between them, who can communicate, or change or remove communication-based on their intention.

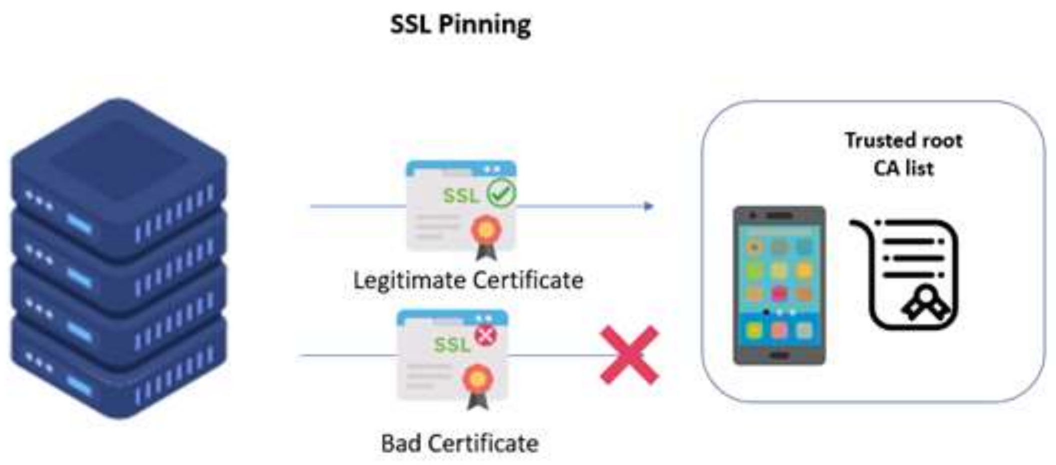
Certificate Mis-issuance was taking place in multiple forms. For example, the Dutch CS Diginotar experienced the largest public CA compromise in 2011. The attacker gained access to their internal systems and was able to provide security certificates for any domain.



When you are unable to discover these threats, your apps become vulnerable to Man-in-the-middle attacks. For example, your app handles credit card details of your customers for a purchase, the man in the middle can misuse the credit card numbers. Here, SSL Pinning plays its role.

What is SSL Pinning?

SSL certificate pinning is a technique designed to prevent dangerous and complex security attacks. This security measure pins the identity of trustworthy certificates on mobile apps and blocks unknown documents from the suspicious servers. Applications with pinned SSL certificates relies on its stored certificates instead of relying on certificate authority stores licenses. With this technique, you can pin SSL certificate host – list of trustful certificates to your application during development and further compare the server certificates against the list during runtime.



As the app validates the server certificates yet again after SSL handshaking, it ensures an extra layer of protection. If there is any mismatch found between the local certificate copy and the server, the connection will be ignored.
As a result, even if you're deceived into installing a malicious certificate on your app, SSL pinning refuses to communicate data in such conditions, therefore keeping your sensitive data secure.

Advantages of SSL Pinning

- Enhanced user privacy and in-app data security
- Cost reduction
- Reduces threat of compromised certificates
- Reduces exposure of user device malware and eavesdropping
- Reports Man-in-the-middle attacks

Limitations of SSL Pinning

Besides the advantages we've examined above, SSL certificate pinning also includes some limitations.

- Less flexibility to change certificates – By pinning an app, it becomes cumbersome to change the security certificate. You must update an android app and send it again to Google play for your users to reinstall it.
- Further, when the app having a pinned SSL certificate, it is hard to introduce any additional security solutions, which functions on reverse proxy technology due to SSL termination.

Explore, how AppTrana cloud WAF provides flexibility to configure the SSL settings, which can make SSL pinned applications fully compatible with a WAF.

Two Approaches to Pin SSL Certificate

- You can directly pin the SSL certificate by binding the certificate in your applications. However, it is significant to implement the transition plan before the certificate expires, else older applications will provide errors.

- The next method for SSL certificate pinning is pinning the certificate’s public key. With this method, you no need to worry about the expiry of the certificate.

Types of SSL Certificate Pinning

You can choose any one of these three SSL pinning types based on the level of security protection you require.

- **Leaf Certificate** – Pinning to the Leaf certificate guarantees that your certificate and chain is 100 % valid. However, this type comes with very less expiry time.
- **Intermediate Certificate** – Signing of the intermediate certificate denotes that you are trusting your CA. If you want to keep your CA, this is the most recommended SSL pinning type.
- **Root Certificate** – It is also known as self-signed certificates and you can employ this type to sign other documents. You should have a strong certificate validation to ensure your CA won’t be compromised.

Conclusion

All internet communications must be secure with SSL certificates. Since these kinds of attacks are complex to execute, SSL pinning is of utmost priority. Though this process is tedious and complex, the pinning SSL certificate is worth the effort as it decreases the risk of data leaks and servers as countermeasures against MITM attack