CASE STUDY

AppTrana Managed WAF Compatibility with Mobile Apps Configured with SSL Pinning

ABSTRACT

- What is SSL pinning, and why do application developers use it?
- The application developers use the SSL pinning technique as an additional security layer for application traffic, which can avoid man-in-the-middle attacks and further prevents attackers from analyzing the functionality of the app and the way it communicates with the server.
- SSL pinning enforces the client to trust the valid or pre-defined server certificate or public key, ensuring that the user devices communicate only to the dedicated trustful servers.
- How does it work?
- The developers embed (or pin) a list of trustful certificates to the client application during development and use them to compare against the server certificates during runtime. If there is a mismatch between the server and the local copy of certificates, the connection will be disrupted, and no further user data will even be sent to that server.
- There are two ways to achieve SSL pinning in client applications. Pin either the whole certificate or its hashed public key.

KEY CHALLENGES

- When the applications (Mobile apps/APIs/web apps) have SSL pinning enabled, it is difficult for customers to introduce security solutions/ in-path devices that work on reverse proxy technology because of SSL termination.
- As soon as any reverse proxy solution has been introduced between client and server, the SSL handshake getting established between application clients and reverse proxy solution, and the client will receive the SSL certificate, which is installed at the reverse proxy solution, due to which the client rejects the connection considering untrusted server connection.

STRATEGY & RECOMMENDED SOLUTION

- To protect the applications (Mobile App/APIs/ Web apps, etc.) enabled with SSL pinning, AppTrana customers can upload their own SSL certificate or choose our free SSL installation.

1. AppTrana Web Application Firewall seamlessly integrates with Let's Encrypt, enabling the generation, signing, installation, and renewal of certificates for domains hosted on the AppTrana platform.

   If customers select our free Let's Encrypt certificate while onboarding AppTrana, they will require adding the Let's Encrypt certificate to the trusted certificate list of the SSL pinning configuration. So that clients can trust the certificate exchanged by AppTrana and establish the connection.

2. Customers can also choose/switch to a custom certificate on AppTrana WAF and upload their own SSL certificate embedded in the client. This way, customers do not require to make any changes on the application side and can activate the WAF protection for their SSL-pinned applications using AppTrana.

NOTE

For a seamless and uninterrupted encryption experience, AppTrana auto-renews the Let's Encrypt certificates every 3 months. In the case of certificate pinning, we recommend uploading a custom certificate to avoid the adjustment required for certificate renewals.