DATASHEET

appdome

SECURE COMMUNICATION

Prevent Man-in-the-Middle (MitM) attacks on mobile apps.
Protect Android & iOS apps with secure certificate pinning.

MOBILE MITM RISKS & REALITIES

Appdome's annual state of mobile app security revealed more than 75% of mobile apps are susceptible to Man-in-the-Middle (MitM) attacks and other methods of session hijacking. Dark Reading defines mobile MitM attacks as "interception by cyber-criminals of the communications between a mobile user and server the user attempts to reach." People use Android and iOS apps 100s of times a day for critical banking, commerce and social needs, to send, receive and discover information and to complete transactions.

Hackers use MitM attacks to intercept insecure mobile connections to steal user information, harvest data and impersonate legitimate hosts and clients as part of larger attacks. MitM attacks can be passive, in which the attacker engages in reconnaissance, credential harvesting or capturing user data such as PII. MitM attacks can also be active, in which the attacker alters payloads, modifies certificates, redirects users to malicious proxies or servers, or injects malware into what the user or server believes is a safe session.

SECURE COMMUNICATION FOR MOBILE APPS

Appdome ensures a secure communication channel between the mobile app and the backend by validating all elements of the session and chain of trust and actively protecting against MitM attacks, malicious proxies, compromised digital certificates or CAs and more. Appdome's MitM prevention enforces, initiates and monitors the SSL/TLS handshake, to prevent attackers from gaining control over the session even before the SSL/TLS handshake completes.

When the app starts the SSL/TLS handshake with the server, Appdome inspects the traffic for anything that looks suspicious. When triggered, the Appdome-secured app will automatically notify the user of the compromise and drop the connection.

MITM PREVENTION

Appdome's MitM prevention for Android and iOS apps validates the authenticity of the SSL certificate used by the destination server to ensure that the certificate has not been forged or compromised. This prevents mobile apps from connecting to untrusted, unknown or malicious destinations.

In addition, Appdome offers advanced session control settings such as enforcing Cipher suites and TLS version to prevent the use of weak or outdated encryption and to prevent hackers from exploiting weaknesses in the app's encryption model.

SECURE CERTIFICATE PINNING

Appdome's Secure Certificate Pinning prevents mobile apps from connecting to compromised servers or endpoints. It encrypts and securely stores the certificate(s) of known trusted servers in the app and validates the certificate before the connection is established. If there is a certificate mismatch, the session is denied or dropped.

BOT DEFENSE

Appdome's Bot Defense prevents bot attacks against the app and the mobile backend.

SECURE COMMUNICATION FEATURES

With Appdome's Secure Communication solution, mobile apps get Man-in-the-Middle prevention, Secure Certificate Pinning and Bot Defense.

ANDROID AND IOS MITM PREVENTION

Appdome's Secure Communication provides Android and iOS apps with comprehensive protection against passive & active MitM attacks.

MiTM Prevention

Validates the authenticity of the SSL certificate used by the destination server. Protects the app from connecting to untrusted, unknown, or malicious destinations or websites.

Malicious Proxy Detection

Detects and prevents connections to unknown, untrusted or malicious proxies or other intermediary devices.

Prohibit Stale Sessions

Prevents unauthorized reuse of stale or expired sessions and SessionID reclaiming.

Trust World Wide Public CAs

Validates the certificates of OEM public CAs to ensure that they have not been compromised or altered.

Enforce Cipher Suites

Ensures that only secure or trusted cipher suites are used before allowing TLS sessions to be established with the mobile app.

Enforce TLS Version

Ensures that only secure and up-to-date versions of TLS are used when the mobile app established a TLS session.

SECURE CERTIFICATE PINNING

Embeds the server certificates for known trusted domains inside the mobile app to ensure that the app only connects to valid and trusted servers. This will prevent hackers from presenting modified fraudulent certificates to the mobile app in an attempt to redirect the mobile user to a malicious site.

Enforce Certificate Roles

Enforces network connections to verify 'basicConstraints' extension in the certificate chain.

Enforce Strong RSA Signature

Enforces server certificate signatures to use a Rivest-Shamir-Adleman (RSA) key with a length of at least 2048 bits.

Enforce Strong ECC Signature

Enforces server certificate signatures to use Elliptic-Curve Cryptography (ECC) key with a size of at least 256 bits.

Enforce SHA256 Digest

Enforces server certificate signatures to use at least a SHA256 certificate hashing algorithm.

BOT DEFENSE

Mobile Client Certificates

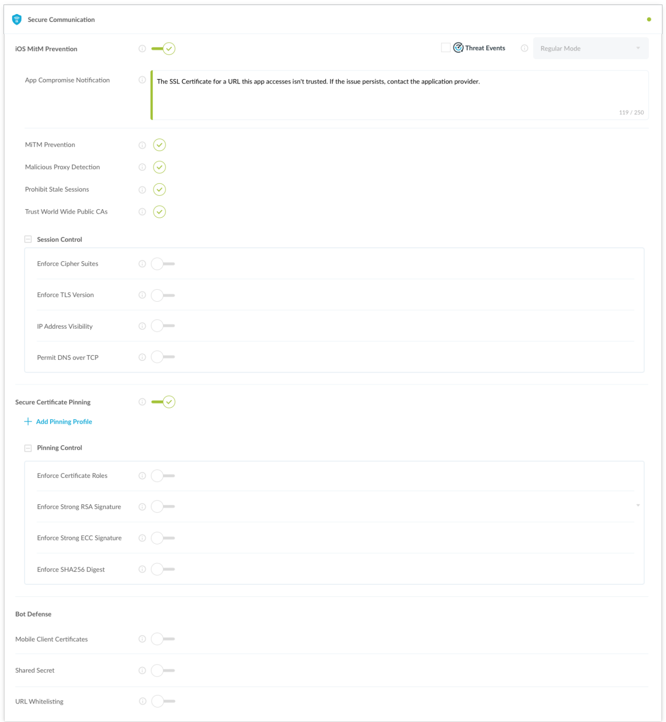
Pin a static client certificate to the Appdome-secured to authenticate client connections on a MicroVPN gateway. Protects mobile backend from connections originating from compromised hosts.

Shared Secret

Specify a secret that will be included in every URL request made by the application. This secret can be verified by the server to identify and only allow trusted/valid applications.

URL Whitelisting

Ensure that the Appdome-secured app can only connect to a trusted set of destinations or hosts.



Secure Communication

iOS MitM Prevention ✓ □ Threat Events Regular Mode

App Compromise Notification: The SSL Certificate for a URL this app accesses isn't trusted. If the issue persists, contact the application provider. 119 / 250

MiTM Prevention ✓
Malicious Proxy Detection ✓
Prohibit Stale Sessions ✓
Trust World Wide Public CAs ✓

Session Control
Enforce Cipher Suites ○
Enforce TLS Version ○
IP Address Visibility ○
Permit DNS over TCP ○

Secure Certificate Pinning ✓
+ Add Pinning Profile

Pinning Control
Enforce Certificate Roles ○
Enforce Strong RSA Signature ○
Enforce Strong ECC Signature ○
Enforce SHA256 Digest ○

Bot Defense
Mobile Client Certificates ○
Shared Secret ○
URL Whitelisting ○

Learn more about Appdome MitM Prevention at **www.appdome.com**.
Open a free Appdome account at **fusion.appdome.com** and start securing your apps!

ABOUT APPDOME

Appdome changes the way people build mobile apps. Appdome's industry defining no-code mobile development and security platform uses a patented*, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new security, authentication, access, enterprise mobility, mobile threat, analytics and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 150+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.

For more information, visit www.appdome.com

*Yehuda et al. Method and a system for merging several binary executables. U.S. Patent 9,934,017 B2 filed November 15, 2015, and issued April 3, 2018.