DATASHEET

appdome

MITM PREVENTION

Prevent man-in-the-middle (MiTM) attacks on Android & iOS Apps quickly and easily, no code or coding required.

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." Mobile users 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 user information, harvest transaction 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 recording 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.

ACTIVE MITM DEFENSE IN APPS

Appdome ensures a trusted session 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 Trusted Session enforces, initiates and monitors the SSL handshake, to prevent attackers from gaining control over the session even before the TLS handshake completes. When the app starts the SSL Handshake with the server, Appdome's Trusted Session inspects the traffic for anything that looks suspicious. When triggered, Trusted Session will automatically notify the user of the compromise and drop the connection.

ADVANCED SESSION HARDENING

In addition to Trusted Session, Appdome provides multi-layered mobile session hardening with Mobile Connection Control™. Mobile Connection Control gives developers several tools to safeguard and secure the connection between the mobile app and the back-end server, including URL whitelisting, enforcing SSL/TLS, TLS versions, ensuring approved cipher suites, and enforcing certificate roles, including certificate signatures using SHA256, ECC, RSA Signatures and more.

SERVER PINNING & CLIENT CERTIFICATES

Appdome's MiTM Prevention also ensures valid mobile hosts and client apps, further protecting the connection between the app and backend. SecureCertificate™ server pinning lets the mobile client app validate a legitimate host before a connection is established. If there is a certificate mismatch the app will drop the connection request. SecureCertificate™ client certificates protect the integrity of mobile backends, safeguarding mobile networks from illegitimate clients like bots and other automated attacks. SecureCertificate pinning and client certificates ensures mutual validation between the client app and the mobile host as soon as the connection is established and through the mobile session.

NO-CODE SECURE COMMUNICATION

Appdome MiTM Prevention is the fastest, easiest and most comprehensive way to secure mobile data in transit, including active MiTM defense, session hardening, and SecureCertificate pinning and client certificates.

Simply upload any app binary (.ipa, .apk or .aab) to your account and click Build my App. Appdome is compatible with all mobile apps; native, non-native and hybrid. And because Appdome doesn't require source code access, customers can protect all mobile apps - internally developed as well as 3rd party apps.

TRUSTED SESSION FEATURES

Appdome's Trusted Sessions to provide MiTM protection, prevent stale sessions, proxy detection and more to all API calls. This ensures that the API is communicating securely with the backend server, without depending on the security of the API vendor.

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

Detect and prevent connections to unknown, untrusted or malicious proxies or other intermediary devices.

Prohibit Stale Sessions

Prevent unauthorized reuse of stale or expired Sessions and SessionID reclaiming.

Trust World Wide Public CAs

If a certificate was installed on the device but not uploaded to the app via Trusted Certificate Authority (CA) Pinning feature, the CA(s) will not be trusted and the connection will close.

SECURE PINNING & CLIENT CERTIFICATES

SecureCertificate™ pinning and client certificates can also be used to establish an enhanced security between the app and the backend. These features leverage mutual validation between the app and backend servers.

As a result, the app will always communicate with a secure point inside the secure infrastructure of the API vendor, and from there it will establish the final communication link with the API backend server.

ADVANCED SESSION HARDENING

Enforce Cypher Suites

Connections established using a non-approved cipher specification are regarded as compromised and dropped.

Enforce TLS Version

Enforce network connections use up to date versions of TLS which are free of known security flaws.

Enforce Certificate Roles

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

Enforce Strong RSA Signature

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

Enforce Strong ECC Signature

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

Enforce SHA256 Digest

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

IP Address Visibility

Make real IP addresses visible to the built application.

Static Client Pinning

Pin a static client certificate to the app and to the backend server to authenticate client-to-server and server-to-client connections.

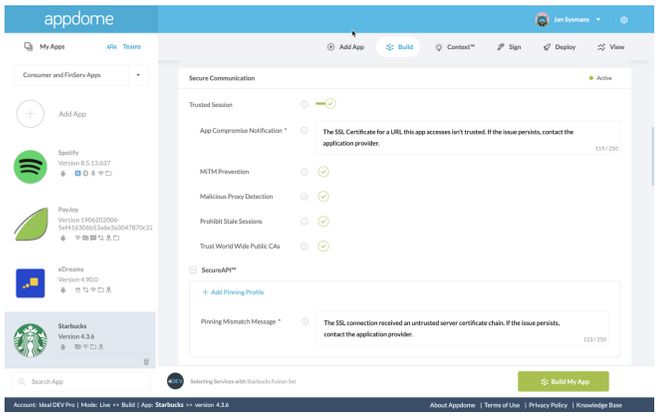

Image: Appdome Trusted Session and SecureAPI.

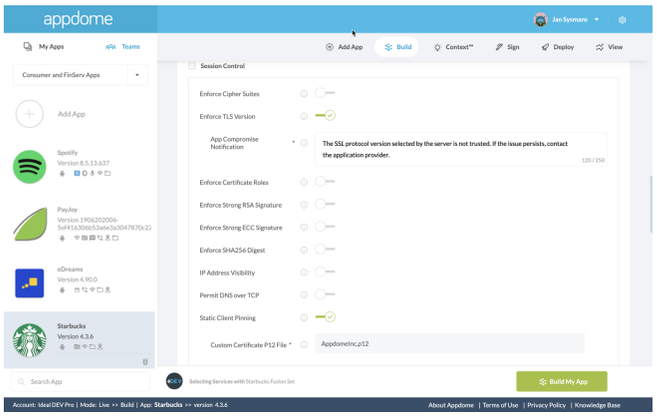

Image: Appdome Session Control.

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.