APP-1 · Mobile Threat Catalogue

Archived: 2026-04-06 00:42:53 UTC

Mobile Threat Catalogue

Man-in-the-middle Attack on Server Authentication

Contribute

Threat Category: Vulnerable Applications

ID: APP-1

Threat Description: Apps that exchange information with a back-end server should strongly authenticate the server before attemtping to establish a secure connection. If the authentication mechanism used by the app is weak, such as not validating a server certificate, an attacker can readily impersonate the back-end server to the app and achieve a man-in-the-middle (MITM) attack. This would provide an attacker with unauthorized access to all unencrypted transmitted data, including modification of data-in-transit. A successful MITM greatly facilitates further attacks against the client app, the back-end server, and all parties of a compromised session.

Threat Origin

Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices [1]

Exploit Examples

Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security [2]

SMV-HUNTER: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps [3]

How We Discovered Thousands of Vulnerable Android Apps in One Day [4]

CVE Examples

- CVE-2016-3664
- CVE-2014-5618

Possible Countermeasures

Mobile App Developer

Use fail-safe logic when establishing a connection to the back-end server; if server certificate validation fails, do not continue to negotiate a secure session or fall back to an unencrypted communication protocol, and warn the app user.

On Android devices, use the Android Network Security Policy feature, Certificate Pinning.

To reduce the impact of a successful MiTM attack on your application, consider the use of public key cryptography to protect sensitive data destined for back-end servers prior to transmission off the device.

Enterprise

App vetting tools/services or pen testing to detect MiTM vulnerabilities in mobile apps.

References

1. L. Neely, Mobile Threat Protection: A Holistic Approach to Securing Mobile Data and Devices, SANS Institute, 2016; www.sans.org/reading-room/whitepapers/analyst/mobile-threat-protection-holistic-approach-securing-mobile-data-devices-36715 [accessed 8/25/2016] ↩

2. S. Fahl et al., “Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security”, in Proceedings of the 2012 ACM conference on Computer and Communications Security, 2012, pp. 50-61; http://dl.acm.org/citation.cfm?id=2382205 [accessed 8/25/2016] ↩

3. D. Sounthiraraj et al., “SMV-HUNTER: Large Scale, Automated Detection of SSL/TLS Man-in-the-Middle Vulnerabilities in Android Apps”, in Proceedings of the 2014 Network and Distributed System Security Symposium, 2014; www.internetsociety.org/sites/default/files/10_3_1.pdf [accessed 8/25/2016] ↩

4. J. Montelibano and W. Dormann, How We Discovered Thousands of Vulnerable Android Apps in 1 Day, presented at RSA Conference USA 2015, 19 Apr. 2015; www.rsaconference.com/writable/presentations/file_upload/hta-t08-how-we-discovered-thousands-of-vulnerable-android-apps-in-1-day_final.pdf [accessed 8/25/2016] ↩

Source: https://pages.nist.gov/mobile-threat-catalogue/application-threats/APP-1.html