GENIVI®

cloakware™
for connected transport

TECHNOLOGY BRIEF

FEBRUARY 2018

Category: Security

Certificate Pinning

Summary

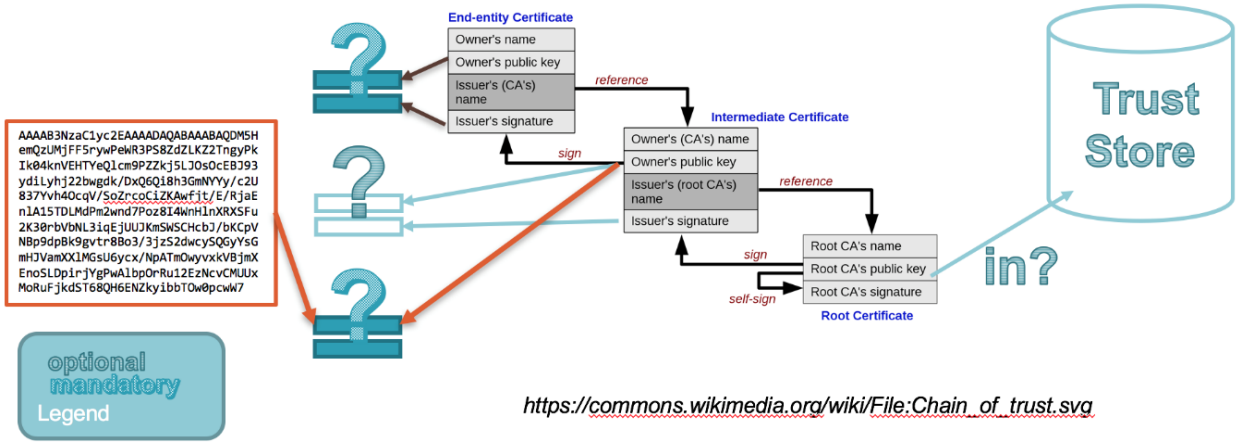
Recommended for ensuring that applications built to perform secure communications to a trusted server continue to do so even in the presence of attached with physical access; where they can easily interpose between the app and server.

Key Characteristics

- Mitigates MITM
- Protects communications from PII disclosure
- Protects communications from reverse-engineering

Description

Attackers have many means available to them to intercept and potentially modify communications. One of the powerful ways they can do this is to use MITM proxies that can dynamically issue new, fake, SSL/TLS certificates. This way, these proxies can impersonate the expected servers to an application. Unless an application is developed with specific checks against the presence of an MITM proxy, the results could be compromised by PII or reverse engineering of the protocol. The latter could begin a further series of attacks into the remote services of the application.



https://commons.wikimedia.org/wiki/File:Chain_of_trust.svg

Certificate Pinning Implementation Example

A typical certificate pinning implementation will confirm that the certificate provided by the server is the expected certificate on first connect. 'Expected' is either (1) having a known public key value (or hash), or (2) being signed by a known public key value (or hash). This check must be performed 'in-code' to be robust. Option (2) is a more flexible solution, permitting multiple server deployments and rolling keys over time.

Second order mitigations against attackers tampering the app to disable or bypass the certificate pinning should be considered in cases where attackers can also control the device execution environment; i.e., where it is straightforward for attackers to execute the target app in their own emulation environment. e.g., an android application or a Linux userspace application.

Alternatives & Related Technologies

Related: Browser Certificate Pinning, *HSTS*.

References & Additional Reading

Attacker Tools

- mitmproxy
  https://mitmproxy.org/
- burp
  https://portswigger.net/burp
- OWASP Zap
  https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- JustTrustMe (Fuzion24/JustTrustMe)
- Frida universal (pcipolloni/universal-android-ssl-pinning-bypass-with-Frida)

Certificate Pinning Example Implementations

ikust/hello-pinnedcerts

Certificate Pinning Testing

OWASP MSTG Section
https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05g-Testing-Network-Communication.md#testing-custom-certificate-stores-and-certificate-pinning

Authors

Ben Gardiner, Irdeto
ben.gardiner@irdeto.com