Certificate Pinning in Android & iOS Apps

Talha Paracha, Amogh Pradeep, Protick Bhowmick, Ali Davanian, Abbas Razaghpanah,
Taejoong Chung, Martina Lindorfer, Narseo Vallina-Rodriguez, Dave Levin, David Choffnes

Background

Mobile applications transmit sensitive user data over the Internet.

These apps mainly rely on **TLS** for network security and privacy.

TLS ***does not*** protect against certain class of attacks (e.g., malicious root CA).

Certificate Pinning

- Pinning is an advanced technique to further increase security of TLS connections.

- Hardcodes the certificate that ***must*** be used to establish a given TLS connection.

- Certificates can be pinned in either raw *or* hashed format in the app code:

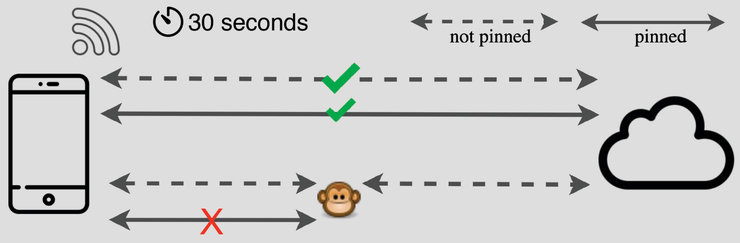
```
<domain>BankOfAmerica.com</domain>
<pin-set expiration="2023-01-01">
 <pin digest="SHA-256">
   7HIpsctkIAq4Y49orFOOQKuKjN3Y=
 </pin>
</pin-set>
```

Methodology

Google Play Apple Store

1000 **Popular** apps, 1000 **Random** apps
& 575 **Common** apps

.PEM .CRT .CER file extensions
sha(1|256)/[a-zA-Z0-9+/=]{28,64}
Statically find evidence of pinning



Dynamically trigger traffic & filter pinned TLS connections using MITM analysis

Key Findings

- **How prevalent is certificate pinning in the mobile ecosystem?**

  Pinning found in **11.4%** of popular iOS apps and **6.7%** of popular Android apps.

- **What are characteristics of apps that pin?**

  Pinning most prevalent in **Finance, Social & Shopping** apps. Only 5 apps on Android, and 4 apps on iOS pin all domains they contact.

- **How consistently do developers use pinning in Android *vs* iOS versions of their apps?**

  Of the **27** apps that pin on both Android & iOS, only **13** do so consistently across platforms.

- **Do apps pin connections to hide data collection from auditors?**

  No evidence that pinned connections have higher prevalence of **user PII** as opposed to non-pinned connections.

Publication

Please refer to our **IMC'22** paper for complete details.

ProperData Frontier 2nd Annual Symposium
Dec 1-2, 2022 | Irvine, California

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]