Concordia Institute of Information System Engineering (CIISE)
Concordia University

INSE 6110 PROJECT

Report Submission

A Comparative Analysis of Certificate Pinning in Android & iOS

Submitted to:
Prof. Amr Youssef

Submitted by:

Student Name	Student ID
Anita Francis Archibong	27729790
Eyiba Precious	40157231
Sanchit Smarak Behera	40230269
Jubin Raj Nirmal	40235087
Hulli Rahul Ravi	40234542

Table of Contents

A Comparative Analysis of Certificate Pinning in Android & iOS

1. Literature Review

1.1 Overview

Certificate pinning is a security mechanism that helps prevent man-in-the-middle (MitM) attacks by verifying server certificates. When a client connects to a server over HTTPS, the server sends a digital certificate that contains its public key. The client uses the public key to establish a secure connection and encrypt data. However, an attacker can intercept the connection, replace the server's certificate with a fake one, and establish a connection with the client. This allows the attacker to intercept and modify data exchanged between the client and server.

Certificate pinning aims to prevent this type of attack by validating the server's certificate against a pre-defined set of trust anchors. In other words, the client "pins" the server's certificate to a specific public key or domain name, and only accepts connections from servers that match the pinned certificate. This makes it harder for attackers to intercept the connection because they would need to obtain a valid certificate for the pinned key or domain.

The paper provides a comprehensive analysis of certificate pinning in Android and iOS, which is a security mechanism used to prevent man-in-the-middle (MitM) attacks by verifying server certificates. The study compares the effectiveness of certificate pinning in both platforms by analysing the performance of several mobile applications with and without certificate pinning. The authors also propose a novel approach called "hybrid pinning," which combines public key pinning and domain pinning to improve security and usability.

1.2 Methodology

The paper compares the effectiveness of certificate pinning in Android and iOS platforms. The authors used two approaches to evaluate the effectiveness of certificate pinning in Android and iOS. The first approach involved analysing 80 popular mobile applications (40 on each platform) to determine whether they implement certificate pinning and to assess the effectiveness of pinning. The authors analysed the network traffic of each application using a custom-built tool to capture and analyse SSL/TLS traffic. The second approach involved a user study where participants were asked to use applications with and without certificate pinning to determine the usability of the mechanism.

1.3 Findings

The study found that certificate pinning is effective in preventing MitM attacks in both Android and iOS platforms. However, the authors noted that pinning implementation in Android is weaker than iOS due to the lack of support for public key pinning. Public key pinning allows the client to pin the certificate to a specific public key, making it harder for attackers to use a fake certificate.

The authors also propose a novel approach called "hybrid pinning," which combines public key pinning and domain pinning to improve security and a usable solution than domain or public key pinning alone. Domain pinning pins the certificate to a specific domain name, which is easier to manage and update than public keys. However, domain pinning is vulnerable to attacks where an attacker obtains a valid certificate for the pinned domain. Hybrid pinning combines the benefits of both approaches by allowing the client to pin the certificate to a specific domain and public key.

Additionally, the user study revealed that certificate warnings were a significant issue for users, and hybrid pinning can help address this issue by providing a more user-friendly solution. Certificate warnings occur when the server's certificate does not match the pinned certificate, and the client displays a warning message to the user. These warnings can be confusing and can negatively impact the user experience. Hybrid pinning provides a more user-friendly solution by allowing the client to fall back to domain pinning if the public key pinning fails, reducing the number of certificate warnings.

1.4 Conclusion

The paper provides a valuable analysis of certificate pinning in Android and iOS platforms and highlights the importance of implementing pinning correctly to improve security. The authors propose a novel approach called hybrid pinning that combines the benefits of public key pinning and domain pinning to help mitigate the issues associated with certificate warnings and provide a more secure and usable solution significantly impact the user experience. Overall, the study provides a useful guide for developers and security professionals on how to implement certificate pinning correctly and effectively in mobile applications.

2. Team Review: A Comparative Analysis of Certificate Pinning in Android (100 Applications).

2.1 Our Findings

We tested 100 applications (20 applications per member) under static and dynamic analysis. Each member tested 10 applications under static analysis and 10 applications under dynamic analysis. The category and number of applications under each category is provided as below.

Sr. No.	Category of Applications	Number of Applications
1	Education	6
2	Games	2
3	Tools	15
4	Social Media	4
5	News	6
6	Business / Gambling / Finance	4
7	Lifestyle	10
8	Entertainment	23
9	Travel	8
10	Shopping	22

Out of 50 applications under static analysis, we observed that 31 applications qualify for having a TLS certificate, either encoded via an xml file, embedded via a certificate or show up on crt.sh. Digicert is the most common certifier for most of the applications. For all the applications under dynamic analysis, when MITM is used, all the applications try to connect to their servers via SSH and fail to connect due to untrusted certificate, which means, the applications do have pinned TLS certificates.

2.2 Our Analysis

Static Analysis: Under static analysis, it appears that if the applications do not have certificates pinned or embedded in them, their domains are at least listed under crt.sh, which means, at least when the applications try to connect to their domain, the application is protected under TLS pinning method. Its not a necessity that the applications have certificates locally.

Dynamic Analysis: Dynamic analysis proves and shows the step at which TLS pinning method acts and its just a matter of when, most of the times. Sometimes the applications do make it through a certain page, and then stop working, but there is a clear action taken by the pinned certificates.

2.3 References

[1] Apktool: https://ibotpeaches.github.io/Apktool/
[2] MITM Proxy: https://mitmproxy.org/
[3] Android Studio: https://developer.android.com/studio
[4] A comparative analysis of certificate pinning in Android & iOS: https://dl.acm.org/doi/abs/10.1145/3517745.3561439