Scientific and Practical Cyber Security Journal (SPCSJ) 3(3): 16 - 17 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

Beyond The Vault: Evaluating authentication controls within secure storage mobile applications.

Gionathan Armando Reale
Honorary Security Team Member of Stratus5, USA.

ABSTRACT

With the dramatic increase in smartphone usage within the last decade and an increase in privacy demands in modern post-Snowden world, many users strive for a safe and convenient way to store personal data and media. In order to fill these demands, software developers have filled the market with mobile applications designed to safely store sensitive content. Within this article I evaluate the efficiency of authentication controls from a sample of secure storage mobile applications.

KEYWORDS: Infosec, Mobile Security, Vulnerabilty, Pentesting, Authentication, Bruteforce

Introduction

It is reported that 49% of smartphone users have sent or received intimate content [1], It is no wonder that many people opt to install mobile applications in the hopes of controlling and securing personal content which, if left insecure, could cause them and others significant harm or embarrassment. The potential problem arises when the mobile applications which are trusted to secure data and media are not regularly tested and are poorly built.

Method

The most popular approach to preventing unauthorised access within secure storage mobile applications is to use a form of password/pattern/fingerprint or PIN based authentication. I set out to test, with a small sample of secure storage mobile applications, how well these controls were implemented.

My sample consisted of ten secure storage mobile applications. All applications were tested on an Android 8.0.0 smartphone device and sourced from the Google Play Store[2]. The testing consisted of reviewing the options available to users to protect against unauthorised access, attempting to trigger and detect anti-bruteforce mechanisms, as well as evaluating risk, based on the outcome of the two previous factors.

When intending to trigger and detect anti-bruteforce mechanisms I manually submitted failed login attempts over a period of ten to twenty minutes. I used the documentation and settings within the applications to review their authentication options, and when evaluating risk I took into account the protective mechanisms (or lack thereof) I had detected and the potential ease a motivated attacker would have to bypass authentication given the settings and controls in place.

Results

Upon testing, I discovered that only two out of the ten mobile applications in my sample had anti-bruteforce protection and adequate controls for strong authentication. The remaining mobile applications (8/10) in my sample did not have anti-bruteforce protection. Three mobile applications offered users the option to set adequate authentication controls, such as the ability to set a long complicated passphrase or ability to enable multi-factor authentication. The majority (7/10) of mobile applications tested did not offer secure authentication options to users. Instead they opted for a less secure four digit PIN, which would, given the correct circumstances, allow a motivated attacker to gain unauthorised access.

Limitations

The project as a whole has significant limitations, the first being that the sample size I used for testing was rather small. There are numerous mobile applications offering secure storage solutions. It would be wrong to assume any firm conclusions could be made based on this research alone.

The next limitation was that risk suggested by my data may not reflect the actual risk users face by using a particular application mentioned in this article. The actual risk would depend on other factors and the threat model of the user, for example: if a user leaves their phone unattended in public and unlocked, they would be at more risk than a user who kept their phone encrypted and within sight at all times.

Another limitation is that all the mobile applications were tested within an Android environment. It may be possible that other versions of the application for other platforms may have been more secure.

The final limitation was that I only tested the product within the «FREE» version, it is possible that upon payment some of the mobile applications tested may have been a lot more secure, allowing users to pay more if their threat model required it. Other limitations may exist.

Discussion

Privacy is an important value within today's society, given the percentage of smartphone users worldwide[1] and the use of smartphones to store, send and receive sensitive content. It is important that solutions offered as secure are reviewed and evaluated on a consistent basis. My findings suggest that some of the secure storage mobile applications simply may not have sufficient security that could stop a motivated and persistent attacker. The limited size of the sample group limits the overall significance of the results, but this data implies that poor authentication controls within this type of mobile application could be a widespread issue.

REFERENCES

[1] Mcafee. Feb 2014. [Online]
https://securingtomorrow.mcafee.com/consumer/identity-protection/love-and-tech/?culture=en-us&affid=0&cid=140623
[2] Google Play Store [Online]
play.google.com