1300 - Bypassing Android Password Manager Apps Without Root

Sunday at 13:00 in Track 2
45 minutes | Demo, Exploit
Stephan Huber*Fraunhofer SIT*

Siegfried Rasthofer*Fraunhofer SIT*

Security experts recommend using different, complex passwords for individual services, but everybody knows the issue arising from this approach: It is impossible to keep all the complex passwords in mind. One solution to this issue are password managers, which aim to provide a secure, centralized storage for credentials. The rise of mobile password managers even allows the user to carry their credentials in their pocket, providing instant access to these credentials if required. This advantage can immediately turn into a disadvantage as all credentials are stored in one central location. What happens if your device gets lost, stolen or a hacker gets access to your device? Are your personal secrets and credentials secure?

We say no! In our recent analysis of well-known Android password manager apps, amongst them are vendors such as LastPass, Dashlane, 1Password, Avast, and several others, we aimed to bypass their security by either stealing the master password or by directly accessing the stored credentials. Implementation flaws resulted in severe security vulnerabilities. In all of those cases, no root permissions were required for a successful attack. We will explain our attacks in detail. We will also propose possible security fixes and recommendations on how to avoid the vulnerabilities.

Stephan Huber

Stephan Huber is a security researcher at the Testlab mobile security group at the Fraunhofer Institute for Secure Information Technology (SIT). His main focus is Android application security testing and developing new static and dynamic analysis techniques for app security evaluation. He found different vulnerabilities in well-known Android applications and the AOSP. In his spare time he enjoys teaching students in Android hacking.

Siegfried Rasthofer

Siegfried Rasthofer is a vulnerability- and malware-researcher at Fraunhofer SIT (Germany) and his main research focus is on applied software security on Android applications. He developed different tools that combine static and dynamic code analysis for security purposes and he is the founder of the CodeInspect reverse engineering tool. He likes to break Android applications and found various AOSP exploits. Most of his research is published at top tier academic conferences and industry conferences like DEF CON,

BlackHat, HiTB, AVAR or VirusBulletin.

#defcon25/by_track/track2/Sunday #defcon25/By_Day/_Sunday