







Systematization of partial lockscreen bypasses on Android

Advisor: **Florian Draschbacher**

Motivation

The lockscreen is one of the most powerful security mechanisms on mobile platforms. It is intended to ensure only authorized users can meaningfully interact with the device and its contents. Consequently, lockscreen bypasses are some of the most-sought-after security vulnerabilities on mobile platforms. While full lockscreen bypasses [1] are pretty rare finds, partial bypasses are discovered relatively frequently [2]. Despite not fully unlocking the phone, these partial bypasses still allow a physical attacker to extract sensitive information from it. The objective of this project is to systematize all partial lockscreen bypasses on Android from the last 3 years.

Steps

-  Identify and study related scientific literature on (partial) lockscreen bypasses on Android
-  Scan through the last 3 years of Google's Android Security Bulletins and the security changelogs of Samsung
-  Note down all vulnerabilities that relate to (partial) lockscreen bypasses
-  Come up with a systematization, i.e. cluster your finds in a meaningful way

Literature

- > **D. Schütz**
Accidental \$70k Google Pixel Lock Screen Bypass
<https://bugs.xdavidhu.me/google/2022/11/10/accidental-70k-google-pixel-lock-screen-bypass/2022>
- > **V. Constantinescu**
New Android Lock Screen Bypass Vulnerability Exposed
<https://www.bitdefender.com/en-us/blog/hotforsecurity/new-android-lock-screen-bypass-vulnerability-exposed-2023>

Courses & Deliverables

- Introduction to Scientific Working**
Short report on background
Short presentation

Note: You can select these topics *only* for the ISW course. If you are considering to combine ISW with a bachelor's thesis at ISEC (highly recommended), check the full list of topics: <https://www.isec.tugraz.at/bachelor-thesis>

Recommended if you're studying

- CS
- ICE
- SEM

Prerequisites

- > Interest in **mobile security**

Advisor Contact

florian.draschbacher@tugraz.at