Insecurity of the 2G/GSM Mobile Network Connection in Android and iOS
Jan Riedler
M. Sc. Cybersecurity

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Insecurity of the 2G/GSM Mobile Network Connection in Android and iOS

The attack vector 2G/GSM in modern smartphones – Can we protect it?

The Problem

The insecurity of the higher network protocols

Despite the advancements in mobile network technology, modern smartphones continue to support 2G/GSM for backward compatibility and coverage in areas where newer generations (3G, 4G, 5G) might not be available. This legacy support creates a significant security vulnerability:

- Karakoc et al. [1] have shown that a 5G connection can be downgraded to 4G by setting up a fake 5G base station that sends a "NAS Registration Reject" message. This causes the device to disable its 5G capabilities and search for a 4G network instead (until a device restart happend/SIM is replaced).
- Shaik et al. [2] have shown that 4G connection can easily be downgraded to a 2G connection. For this, an attacker sets up a fake 4G base station that just sends a "TAU Reject message" to the device, which then drops its 4G connection and seeks for a 2G network instead (until a device restart happend/SIM is replaced).
- 2G is insecure because it uses outdated encryption algorithms (A5/1 and A5/2) that can easily be broken in real time, and it lacks base station authentication, **allowing attackers to set up fake base stations and intercept communications**. These vulnerabilities make it susceptible to "Man-in-the-Middle" attacks and decryption of data [3].
- 2G is activated by default in Android and iOS. With Android 12+, 2G can be deactivated in the settings, with iOS only in lockdown mode since iOS 17. 2G is still enabled for emergency calls after deactivation.

Goal

Make the world more private

The aim of the project is to improve security and thus our privacy in modern smartphones due to the problem described above. This is to be realised through the following points:

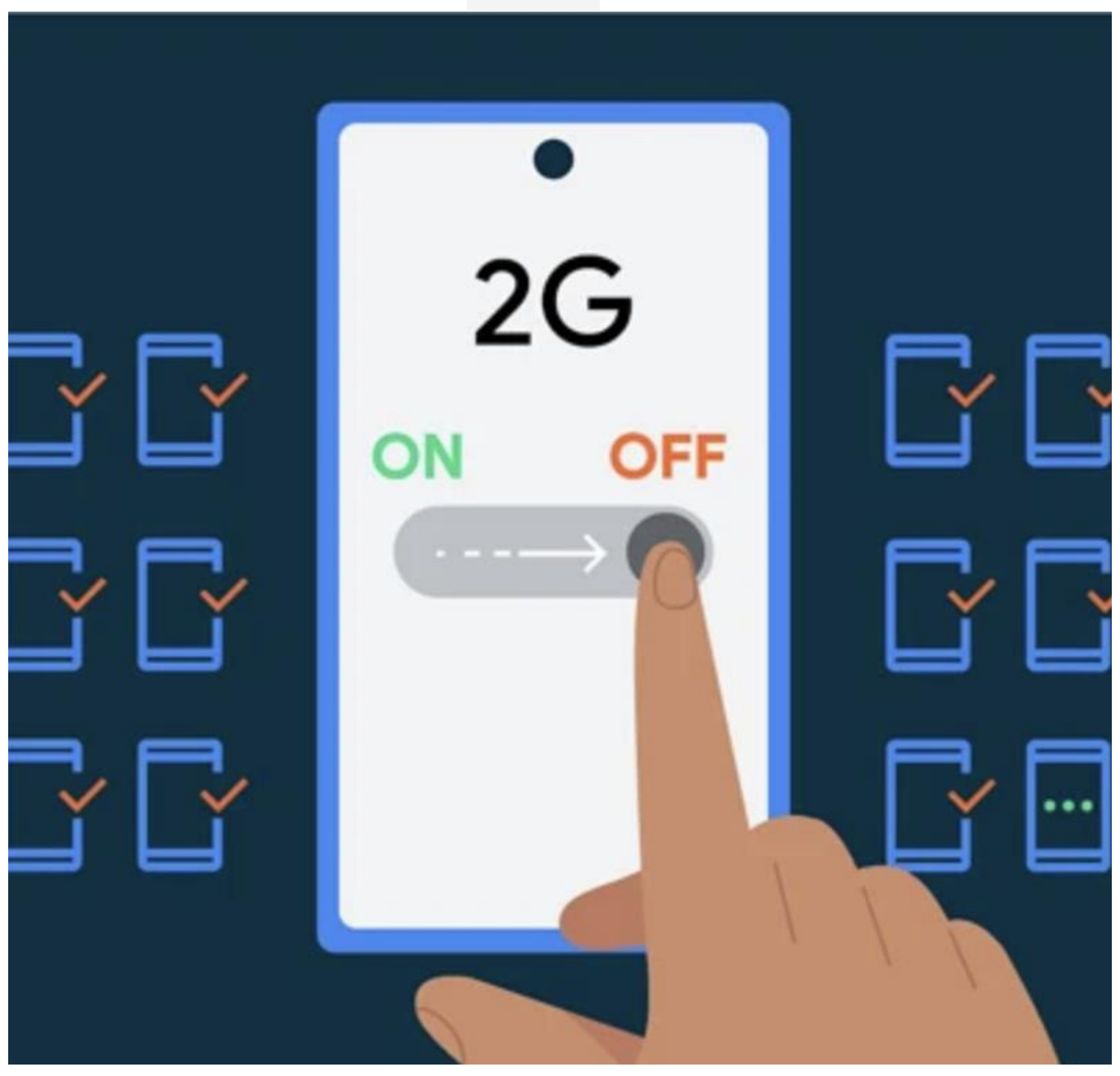
- Investigate whether current versions of smartphone operating systems have implemented countermeasures against these downgrading attacks.
- If such countermeasures are lacking, the goal is to propose or identify useful solutions which **can be implemented directly, without having to make adjustments to the base station** (allows faster realisation).
- **This project should also examine whether 2G can still be utilized for non emergency calls despite being disabled in the settings (finding a vulnerability that allows this to happen).**

Solution

a.k.a. the Procedure

In order to realise the above-mentioned goals, various procedures can be applied. The following is intended merely as a suggestion:

- Perform the downgrading attacks described by Shaik et al. [2] and Karakoc et al. [1] in the current versions of Android and iOS. If these are still possible: Find possible countermeasures that do not require any modifications to the base station by analysing the protocols of the respective generations.
- If countermeasures have already been implemented (unlikely), check them. In Android the code is open source. For iOS you can attempt to understand iOS's behavior by reverse engineering—observing system behavior, analyzing interfaces, and deducing patterns or logic.
- Since 2G can be deactivated via software in the current versions, try to find security vulnerabilities through code analysis and reversing techniques



https://thehackernews.com/2023/08/new-android-14-security-feature-it.html

Connection to the Lecture

Within the lecture series, the professors presented their research area. This proposal is connected to the lecture of Jiska Classen. According to her HPI website [4], Jiska Classen has three main research areas: Next Generation Wireless Security, Reverse Engineering and Mobile Device Security and Privacy. All of these areas are addressed within this proposal. Reverse engineering techniques need to be applied to analyse iOS behaviour for 2G deactivation. Clearly this also plays into the area of Mobile Device Security and Privacy. Since this also involves attacks on the current generation of mobile phones, the area of next generation wireless security is also addressed, which she also dealt with in the lecture.

Reverse Engineering Techniques

- Dynamic Analysis: Analyzing the behavior of a program while it executes. Example Tool: Frida
- Static Analysis: Examining the code and structure of a program without executing it. Example Tool: IDA Pro
- Fuzzing: Inputting random or unexpected data to find vulnerabilities or trigger crashes. Example Tool: AFL++

Realisation of Breaking GSM in Real Time
Educational Purposes

Quellen: [1] Bedran Karakoc, Nils Fürste, David Rupprecht, and Katharina Kohls. 2023. Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G. In Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. 97–108; [2] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2015. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. arXiv preprint arXiv:1510.07563 (2015).; [3] S. Gindraux. 2002. From 2G to 3G: a guide to mobile security. In Third International Conference on 3G Mobile Communication Technologies. 308–311. https://doi.org/ 10.1049/cp:20020410; [4] HPI, https://hpi.de/classen/home.html, Access: 09.07.2024