DEMO: Recent Advancements in Detecting Cellular Attacks with CellGuard

Swantje Lange
swantje.lange@hpi.de
Hasso Plattner Institute
University of Potsdam
Potsdam, Germany

Lukas Arnold
larnold@seemoo.tu-darmstadt.de
Secure Mobile Networking Lab
TU Darmstadt
Darmstadt, Germany

Maximilian Paß
maximilian.pass@student.hpi.de
Hasso Plattner Institute
University of Potsdam
Potsdam, Germany

Matthias Hollick
mhollick@seemoo.tu-darmstadt.de
TU Darmstadt, Secure Mobile Networking Lab, Darmstadt, Germany
IMDEA Networks Institute, Madrid, Spain

Jiska Classen
jiska.classen@hpi.de
Hasso Plattner Institute, University of Potsdam
Potsdam, Germany

Abstract

A viable remote attack surface of smartphones is the baseband chip, which handles the communication with cellular networks. One attack that is often conducted, e.g., to track users, is the deployment of Rogue Base Stations (RBSs). We built and actively maintain CellGuard, an iOS app that analyzes the interaction of an iPhone with its baseband chip to detect whether the phone connects to an RBS.

In this demo, we showcase CellGuard's base functionality of dissecting baseband communication packets and assessing nearby cells for trustworthiness, as well as recent developments. We present the latest changes to the app, including support for Apple's new C1 and C1X baseband chips, architectural improvements, user interface enhancements, and additional notifications for suspicious baseband activity.

CCS Concepts

• **Security and privacy → Mobile and wireless security**.

Keywords

Fake Base Station, App-based Detection, Apple C1 Baseband

ACM Reference Format:
Swantje Lange, Lukas Arnold, Maximilian Paß, Matthias Hollick, and Jiska Classen. 2026. DEMO: Recent Advancements in Detecting Cellular Attacks with CellGuard. In *Proceedings of the 19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '26), June 30-July 03, 2026, Saarbrücken, Germany.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3765613.3814569

1 Introduction

Smartphones are our prevalent means of communication. Attacks on cellular connections can leak private information, ranging from metadata of encrypted traffic to sophisticated attacks that intercept decrypted traffic or gain code execution on a smartphone. These attacks are commonly carried out by RBSs, where an attacker tricks a smartphone into connecting to a malicious base station not under control by the Mobile Network Operator (MNO). As attacks are carried out wirelessly, without traversing the Internet, they only leave few traces. This makes it difficult to prove active exploitation of cellular vulnerabilities. Nonetheless, governments invest into baseband exploitation even on the latest cellular technologies, such as 5G SUbscription Permanent Identifier (SUPI) catchers [6].

To combat those attacks, we developed and maintain the iOS app CellGuard [2], which detects when a phone connects to RBSs. The app runs on all iPhones with iOS versions from 14 to 26, and is available for non-jailbroken iPhones via Apple's TestFlight and for jailbroken iPhones via TrollStore and AltStore. Installation guides for both setups are available on the CellGuard website [5]. Since the initial release in 2024, the app has been under active development as we work to improve its technical functionality and usability.

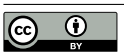
CellGuard examines the communication between an iPhone's application processor and the baseband by parsing the communication logs. To derive meaningful information from this communication, users need to increase the verbosity of the logs by installing a debug profile for the cellular baseband [1]. Analyzing the baseband's communication reveals parts of the packets it receives and enables the detection of anomalies and cellular attacks. CellGuard warns users if connections to suspicious network cells are detected.

We reverse-engineer the protocols used by the basebands shipped with iPhones to enable log interpretation. The older iPhone models 7 to 11 use Intel basebands that employ the Apple Remote Invocation (ARI) [3] protocol. The more recent iPhones, from 12 to 17, use Qualcomm basebands that communicate via the Qualcomm MSM Interface (QMI) protocol. The iPhone 16e, 17e, and Air use the new Apple baseband chips.

We develop a tool that can be deployed easily, is usable by laypersons, and gives information about cellular attacks run in the wild. Thereby, we aim to facilitate research projects examining the security and privacy of cellular networks. We solicit the community to contribute further metrics to detect RBSs or cellular attacks.

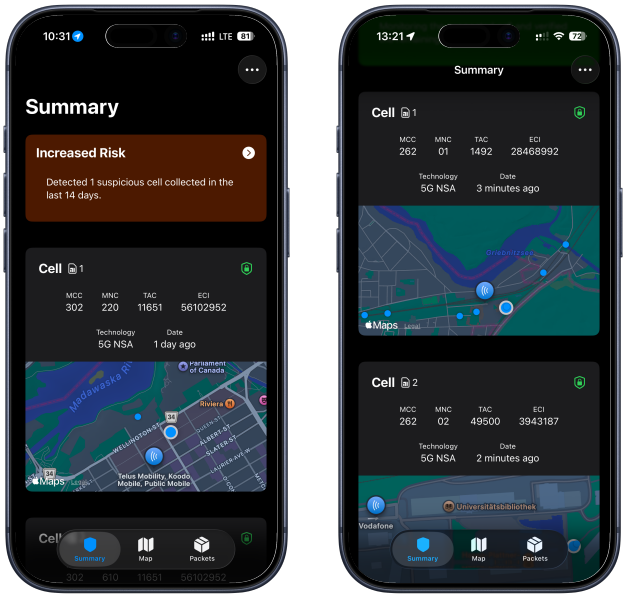
2 Recent Advancements

Since the initial development and publication of CellGuard [2], we integrated numerous changes that we will practically demonstrate.



WiSec '26, Saarbrücken, Germany

ACM ISBN 979-8-4007-2201-1/2026/06
https://doi.org/10.1145/3765613.3814569



(a) Home screen of the CellGuard app summarizing the analysis.

(b) On dual-SIM phones, the cells of both SIM cards are assessed.

Figure 1: User Interface of the CellGuard app.

The source code is publicly available [4]. We continuously ensure compatibility with new iOS versions, including iOS 26.

Apple C1/C1X Baseband Support. CellGuard now supports the new Apple C1 and C1X basebands shipped with the iPhone 16e (C1), the iPhone 17e, and the iPhone Air (C1X). The Apple basebands use the ARI protocol, but with extended functionality compared to the Intel basebands in iPhone models 7 to 11. In particular, they support 5G and satellite communication.

Cell Information from Packets. Cell information is now extracted directly from the communication packets rather than retrieved from the system logs. This improves the temporal correlation between cell information and observed packets, since the information originates from the same source. On jailbroken iPhones, this technique requires only one tweak instead of two.

Dual-SIM Support. CellGuard now supports dual-SIM devices. We extended the QMI and ARI parsers, the verification pipeline, and the user interface to handle two active SIM cards simultaneously.

Connectivity Events. To advance the observability of the phone's status, we added the tracking of connectivity status events. Users can inspect when their phone disconnected from the network or when a SIM card was inserted or ejected. Knowing what happened to the phone is especially interesting for time periods when the phone was not under a user's control, e.g., during custody.

Sysdiagnose Management. On non-jailbroken devices, CellGuard relies on sysdiagnose archives to access baseband logs. We added a full import, export, and delete workflow with metadata storage and progress detection. An iOS Shortcut integration lets users directly navigate to the system settings to import a sysdiagnose. Notifications inform them when a sysdiagnose is ready for import.

Usability Improvements. To make the complex topic of cellular network traffic and attacks approachable to everyday smartphone users, we provide a reworked onboarding UI to explain how the app works and how users can interact with it. On non-jailbroken devices, CellGuard sends a notification when the baseband debug profile is about to expire, so that users can reinstall it on time. Cell details now display up-to-date information about the cell's MNO. The verification scores use color coding and weekly grouping, and the cell list shows the lowest score for quick assessment. CellGuard also displays a 5G NSA technology indicator in the cell information.

User Study. To further improve the RBS detection algorithm, we conduct a user study. Users can opt in to participate. If a participant's CellGuard app detects a suspicious cell, it reports the cell's data to the study server. Users can also proactively report cells they believe are suspicious, even if the cells are not flagged.

3 Demonstration

We show how the CellGuard app guides users through the cell assessment process. The app explains how to create a sysdiagnose and detects when its creation is started and when it is ready for import. With the iOS Shortcut, users can jump to the settings to perform the import. The app then analyzes the phone's communication logs.

We will provide a sysdiagnose for import that includes logs from a suspicious cell. In this way, participants can see how CellGuard analyzes and classifies cells. In the app, users can inspect the cells that the phone connected to. Next to general cell information, they can see the trustworthiness score, the eight metrics it depends on, and which packets were sent between the baseband and iOS.

Optionally, we will set up a small Faraday cage with an RBS. Participants can place a test iPhone into the cage, so that the iPhone attempts a connection with the RBS. Subsequently, the participants can create a sysdiagnose and import it into the CellGuard app. The app will extract the cell information and communication traces, and run the rating algorithm. The RBS will be flagged as suspicious in the app. Participants can voluntarily use their own iPhone, install CellGuard via TestFlight, and conduct a measurement within the Faraday cage.

References

[1] Apple. 2026. Profiles and Logs. https://developer.apple.com/feedback-assistant/profiles-and-logs/. Accessed: 2026-04-02.
[2] Lukas Arnold, Matthias Hollick, and Jiska Classen. 2024. Catch You Cause I Can: Busting Rogue Base Stations using CellGuard and the Apple Cell Location Database. In *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*. ACM, 613–629. doi:10.1145/3678890.3678898
[3] Tobias Kröll. 2021. ARIstoteles: iOS Baseband Interface Protocol Analysis. doi:10.26083/tuprints-00019397
[4] Secure Mobile Networking Lab. 2026. CellGuard Source Code. https://github.com/seemoo-lab/cellguard. Accessed: 2026-04-06.
[5] Secure Mobile Networking Lab. 2026. CellGuard Website. https://cellguard.seemoo.de/. Accessed: 2026-04-06.
[6] Stadt Berlin. 2025. Haushaltsplan von Berlin für die Haushaltsjahre 2026/2027, Polizei Berlin, Landeskriminalamt. https://www.parlament-berlin.de/ados/19/IIIPlen/vorgang/d19-2627%20Band%2005%20-%20Epl%2005.pdf#page=162. Accessed: 2026-04-07.