Unauthorized access to the communication base station

Powered by GreenVolt Home Energy

Overview

These attacks involve malicious actors setting up unauthorized base stations to intercept, manipulate, or degrade communication between legitimate users and network operators. In this blog, we will explore how to identify and mitigate these threats effectively. These devices are not theoretical. While some government use may be authorised, many fake base station deployments operate in a. This paper has been accepted to appear at USENIX Security '25. Though efforts have been made to defeat this threat, up to this day, the presence of FBSes and the multi-step attacks (MSAs). A fake base station exploits vulnerabilities in the broadcast message announcing a base station's presence, which is called SIB1 in 4G LTE and 5G NR, to get user equipment to connect to the fake base station.

Unauthorized access to the communication base station

Is Your Phone Safe? The Hidden Dangers of Base ...

Base station spoofing has emerged as a significant threat in the digital age, exploiting vulnerabilities in cellular networks to steal data and compromise privacy.

Fake Base Stations - Telecom's Open Front Door for Hackers

Fake base stations, or IMSI catchers, are increasingly used by state and criminal actors to spy, disrupt, or impersonate mobile users. This blog explores how they work, who deploys them, ...

Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack ...

An FBS is an unauthorized device an attacker uses to im-personate a legitimate BS within a cellular network. FBSes typically consist of a radio transceiver capable of broadcast-ing signals at legitimate ...

Communication Base Station Access Control , HuiJue Group E-Site

During a recent infrastructure audit in Germany, we discovered 68% of access points lacked proper zero-trust architecture implementation. The fundamental mismatch lies between physical security ...

Fake Base Station Detection and Link Routing Defense

We designed and built a defense scheme which detects and blacklists a fake base station and then, informed by the detection, avoids it through link routing for connectivity availability.

Exposing and Addressing Fake Base Station Vulnerabilities in 5G ...

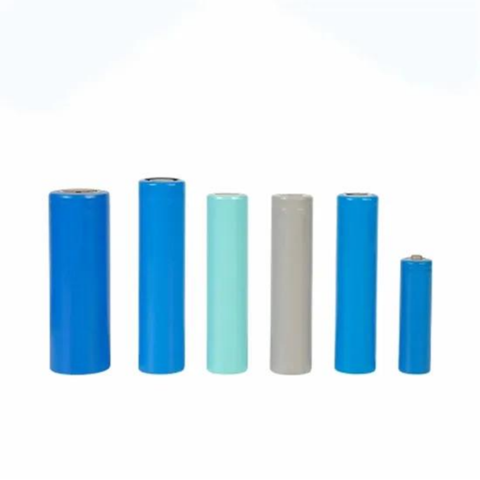
Through simulated experiments, we demonstrate how attackers can capture and replay 5G authentication vectors, bypassing security protocols and gaining unauthorized access.

How Hackers Can Hijack Your Device Without You Knowing - ...

The flaw can be exploited by an attacker setting up a rogue base station, which masquerades as a legitimate cellular network. A victim's device (referred to as User Equipment or ...

How to Identify and Mitigate Rogue Base Station Attacks

These attacks involve malicious actors setting up unauthorized base stations to intercept, manipulate, or degrade communication between legitimate users and network operators. In this blog, ...



Bolstering Data Privacy and Mobile Security: An Assessment of IMSI

Rogue base stations can perform a passive attack known as IMSI catching. This attack sniffs cellular communication without the user's knowledge to collect mobile device identities that are ...

Preventing theft and vandalism on the mobile base station

As the expertised manufacturers of enclosures, it's important for us to improve safety of the base station and to protect critical equipment like batteries, copper cables, and diesel. Here are five suggestions ...

Contact Us

For catalog requests, pricing, or partnerships, please visit: https://kidsandparents.pl