Electronic fraud base station communication

False base stations execute attacks in the Radio Access Network (RAN) of cellular systems, adversely affecting the network or its users. To address this challenge, we propose a behavior rule specification ...

This week has seen credible reports from authorities in both Switzerland and South Korea that believe fake base stations are being used to facilitate fraud for the first time in either ...

Fake base stations (FBSes) pose a significant security threat by impersonating legitimate base stations (BSes). Though efforts have been made to defeat this threat, up to this day, the presence of FBSes ...

Fake base stations exploit vulnerabilities in mobile networks by mimicking legitimate cell towers. These rogue stations deceive nearby mobile devices into connecting to them instead of the ...

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, ...

This study investigates the vulnerabilities of 5G networks exploited by FBSs, which hijack communications by mimicking legitimate base stations and compromising user equipment (UE).

For the first time, we systematically study fake base station attacks and their main influencing factors. We use a specification-conform simulation model that lets us analyze fake base ...

To address RBS attacks, it is essential to create a RBS/FBS detection system. In this paper, we proposed three different approaches to detect RBS/FBS, including the user equipment ...

The wireless transceiver broadcasts radio signals to impersonate legitimate base stations. The laptop connects to the transceiver (e.g., via an USB interface) and controls what to ...

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.

Web: https://www.upstreamjhb.co.za