5G SECURITY TEST BED™

Securing 5G:

5G Security Test Bed Assesses 5G Network Resiliency Against False Base Station Attacks

Q3 2025 False Base Station Report Highlights

The 5G Security Test Bed and Its Findings

An Industry Initiative to Advance 5G Security by Testing in Real-World Conditions

The 5G Security Test Bed is a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies, created with a sole focus on testing and validating 5G security recommendations and use cases from government groups, wireless operators, and others. It is the only initiative that uses commercial-grade network equipment and facilities to demonstrate and validate how 5G security standards recommendations will work in practical, real-world conditions.

Tests Validate 5G Device Protections Against Multiple False Base Station Attack Scenarios

The 5G Security Test Bed completed its latest round of tests, assessing mobile device behavior in response to attacks from false base stations (FBS) impersonating legitimate 5G networks. The Test Bed's Technical Advisory Committee (TAC) established 10 test cases (TC) covering several false base station attack scenarios.

Key Findings

Each test was conducted twice to assess resilience against false base station attacks on devices with and without 5G authentication protocols. First, the tests were performed on a 5G test device ("user equipment," or UE) with a 5G Authentication and Key Agreement (5G AKA) SIM, where the SIM is provisioned with encryption protocols for securely authenticating users on a 5G network. Each test was then repeated with a different, unencrypted SIM (Null encryption SIM).

The tests confirmed that devices provisioned with encrypted identities are resilient against these attacks.

- ✓ **Encrypted 5G Devices Reject Invalid Authentication and Connection Attempts from False Base Stations.**
- ✓ **Encrypted 5G Devices Do Not Share Data During False Base Station Attacks.**
- ✓ **5G Device Protections Work As Intended, Securing Data on Encrypted SIMs.**

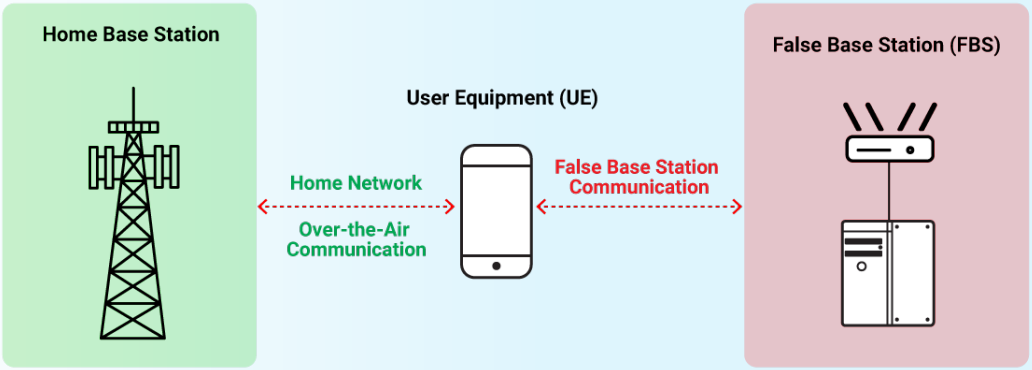
In all testing, the 5G device with encrypted identifiers recovered from the attacks or avoided them completely, and it did not reveal any private identifying information in any of the attack scenarios. The test results confirm 5G networks are significantly more resilient against false base station attacks compared to earlier systems, due to their encryption and authentication protocols.

False Base Stations, 5G Network Protections, and Test Cases

What Is a False Base Station?

A false base station (FBS), also known as a rogue base station or IMSI catcher, is an unauthorized or malicious device that mimics a legitimate wireless network to intercept communications, track users, or disrupt services.

A false base station exploits vulnerabilities in how mobile devices connect to networks, tricking them into connecting to the false base station instead of their legitimate "home" network. While 4G and older networks were susceptible to having private information intercepted in these attacks, 5G networks are fortified against them through 5G privacy and encryption protocols that are provisioned to the SIM cards on 5G devices.



5G Device Protections Against False Base Station Attacks

With very few exceptions, the SIM cards on 5G-enabled devices are provisioned with encryption and authentication protocols when running on 5G networks. These 5G AKA SIMs conceal and protect private device identity information traveling to and from the device.

5G networks identify devices by their SUPI (Subscriber Permanent Identifier), which is encrypted as a SUCI (Subscription Concealed Identifier) to enhance privacy. This replaces the IMSI (International Mobile Subscriber Identity) previously used in 4G networks, which was not encrypted. 5G networks have built-in, enhanced security due to implementation of the SUCI, which prevents attackers from accessing private information.

5G devices are provisioned with 5G AKA SIMs the majority of the time, per standards set by 3GPP, the international mobile standards body. In fact, 5G devices are only provisioned with a Null encryption SIM when the device is in emergency mode, which is meant to connect with unknown networks by design. After an FBS attack, a 5G AKA SIM-provisioned device can reconnect to its home network after toggling airplane mode or power cycling the device, or it will reset itself and reconnect after a timeout in alignment with 3GPP standards.

Definition of Test Cases

The Test Bed's TAC executed 10 test cases to assess 5G device behaviors in response to false base station attacks. The test cases covered four high-level categories, assessing mitigations against each type of attack:

User Equipment Radio Resource Control (RRC) Connection Scenarios. Test Cases 1 and 2 assessed whether the test device would successfully connect to the false base station via the RRC, and if so, whether subsequent registration and authentication procedures would protect it from fully connecting to the false base station. TC 1 began with the device not connected to any network, while TC 2 used a high-powered false base station to lure the device from an existing connection with its home network.

Authentication Handshake Scenarios. Test Cases 3 through 5 assessed whether the false base station could lure the device to connect in three scenarios: when the FBS omitted the authentication handshake, when it attempted to "fake" the handshake using fabricated credentials, and when it "replayed" old authentication credentials captured from an earlier connection between the device and the home network.

Denial-of-Service (DoS) Attacks. Test Cases 6 through 8 assessed whether the false base station could successfully execute DoS attacks against the test device, forcing it to disconnect from its home network after receiving "5GS Services Not Allowed," "Cell Barred," and "PLMN Not Allowed" messages, tricking the device into a state where it is unable to reconnect to its home network.

False Public Warning System (PWS) Messages. Test Cases 9 and 10 assessed whether the false base station could successfully execute DoS attacks against the test device using fake Public Warning System (PWS) messages alone, and PWS messages combined with "PLMN Not Allowed" messages, respectively.

False Base Station Test Results

As noted above, each of the 10 test cases was conducted twice to assess resilience to false base station attacks on devices with and without 5G authentication protocols. The first two tests assessed RRC connection scenarios, three assessed invalid authentication handshake scenarios, three assessed various DoS attack scenarios, and two assessed DoS attack scenarios through false public warning system messages.

Test Cases 1 and 2: False Base Station Attacks Fail in Encrypted Devices Due to Mutual Authentication Procedures

Test Cases 1 and 2 are designed to observe a successful Radio Resource Control connection between the test device and false base station when the device is either not attached or attached to its home network, respectively, then confirm that the device does not fully connect and register to the false base station Core.

What Is a Radio Resource Control Protocol?

The RRC serves as the 5G network's control center, a protocol that manages all radio resources and connections on the network—that is, it is the initial gateway before authenticating and fully connecting with the 5G Core network.

In both the encrypted and unencrypted scenarios for these test cases, the 5G test device successfully connected with the false base station's RRC. Through the RRC, both the encrypted and unencrypted SIM profiles requested registration with the false base station Core. For the encrypted SIM, the test device avoided fully connecting to the false base station because the false base station could not decipher the device's identity, and mutual authentication is required to connect with any 5G base station. For the unencrypted SIM, the false base station did not have the SIM's identifiers in its database, and it was also unable to fully connect.

When provisioned with an encrypted SIM, the test device was able to successfully reconnect to its home network after the false base station connection attempt failed in each of these test cases. When provisioned with an unencrypted SIM, the device remained in a repetitive loop until the false base station was turned off.

Test Cases 3 – 5: Rejecting False Base Station Authentication Attempts Using Invalid Credentials

Test Cases 3 through 5 assessed responses to several invalid false base station authentication attempts. In TC 3, the false base station used a "Security Mode Failure" message to attempt to connect to the test device without providing any authentication at all; in TC 4, the false base station attempted to connect to the device using fabricated authentication credentials; and in TC 5, the false base station replayed old authentication credentials that were previously recorded between the test device and the home network.

In all three test cases, both the encrypted and unencrypted 5G devices successfully rejected the false base station's illegitimate authentication requests, and the connections with the false base station were terminated.

Test Cases 6 – 8: Resilience Against DoS Attacks Using Registration Rejection Messages

Test Cases 6 through 8 assessed responses to denial-of-service attacks caused by three different registration rejection messages, respectively: "5GS Services Not Allowed," "Cell Barred," and "PLMN Not Allowed." In each of these test cases, the false base station lured the device away from its home network by operating at higher power, then responded to the device's connection attempts with the respective rejection messages.

When the false base station rejected the device's connection in Test Cases 6 and 8 with the "5GS Services Not Allowed" and "PLMN Not Allowed" messages, the device was barred from connecting to both the false base station and the home networks until the false base station was powered off and the test device was powered off and back on. This occurred for both the encrypted and unencrypted SIMs. Although the false base station was able to prevent the device from connecting to any network, it was unable to capture any private information.

For Test Case 7, the false base station impersonated the test device's home network by cloning its technical specifications, then used a "Cell Barred" message to reject the device's attempts to connect to the false base station Core, rendering it unable to connect to either network. After the false base station was turned off, the device considered its home network "Not Barred" and immediately reconnected with its home radio base station in both the encrypted and unencrypted scenarios. As in TCs 6 and 8, the false base station was unable to capture any private information.

Test Cases 9 and 10: False Base Station DoS Attacks Using Spoofed PWS and "PLMN Not Allowed" Messages

Test Cases 9 and 10 assessed device responses to spoofed Public Warning System messages containing a "Commercial Mobile Alert System" (CMAS) test, sent by the false base station. In both test cases, the test device ignored the PWS message as expected, then connected to the RRC. Afterward, the device attempted to connect to the false base station's Core network under both the encrypted and unencrypted SIM scenarios.

In TC 9, the false base station rejected the encrypted device's registration request with the message "UE identity cannot be derived by the network," due to the 5G SIM being encrypted. After this rejection, the test device immediately reestablished its connection with its home network. The false base station similarly rejected the connection in TC 10, but with the message "PLMN Not Allowed." In this test, the encrypted device successfully reconnected with its home network after disconnecting from the false base station.

In the unencrypted scenarios for both test cases, the UE also ignored the spoofed PWS messages, then successfully connected to the RRC. In TC 9, the false base station rejected the UE's connection request with the registration rejection message "MAC Failure" due to the SIM not being encrypted. The false base station also rejected the device's connection request in TC 10, but with the registration rejection message "PLMN Not Allowed." In these test cases, the unencrypted device was able to reconnect to its home network after the false base station was turned off and the device was reset by toggling airplane mode on and off.

Summary and Key Takeaways

5G Networks Are a Massive Improvement Over 4G, Protecting Private Data Against False Base Station Attacks

The results for scenarios executed on the 5G AKA SIM-encrypted device in the majority of the test cases demonstrate that: (1) The device will not fully connect to the false base station after connecting to its RRC (TCs 1 and 2); (2) the device will not fully connect to the false base station when the false base station attempts to omit or use invalid credentials (TCs 3 – 5); (3) the device will automatically recover from a "Cell Barred" DoS attack after the false base station is turned off (TC 7); and (4) the device will not fully connect to the false base station when it attempts to connect using a spoofed Public Warning System message (TC 9). In each of these scenarios, the test device did not fully connect to the false base station's Core network, was able to reconnect to its own home network, and did not reveal any private information.

For the remaining test cases (TCs 6, 8, and 10) conducted on the encrypted test device, the device did not immediately reconnect to its home network after the FBS attack. However, the device was able to reconnect with its home network after resetting it by toggling airplane mode on and back off, and it did not share any private device identifiers.

When the tests were executed on the device with unencrypted identifiers, which were the norm for 4G networks, results were mixed, but the test device was also able to reconnect with its network in each case, sometimes after reset.

In every test scenario, the device with the encrypted SIM successfully recovered from the false base station attacks or avoided them completely, and no identifying information was revealed—demonstrating resilience in overcoming false base station attacks thanks to 5G encryption and mutual authentication protocols.

Encrypted 5G Devices Behave as Intended, Protecting Private Device Identifiers

Per recommendations from the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC)[1] and 3GPP, 5G device identifiers are always encrypted as the default setting in 5G networks, except in rare scenarios when the device is in emergency mode, which is meant to connect with unknown networks by design.

For devices provisioned with 5G AKA SIMs, encryption and mutual authentication protocols protect against losing private information during false base station attacks:

- Use of the SUCI, the encrypted identifier on 5G networks, prevents false base stations from accessing private device identifiers.
- 5G devices are provisioned with 5G AKA SIMs the majority of the time, per CSRIC recommendations
- 5G AKA SIM-provisioned devices that have been disconnected from their networks due to false base station DoS attacks can reconnect to their home networks after disconnecting from the false base station, toggling airplane mode, power cycling the device, or waiting for the device to reset on its own after a built-in timeout.

[1]See CSRIC VII WG3, Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (Mar. 2021), https://www.fcc.gov/file/20606/download.

- The 5G device reset timeline is set by the equipment manufacturer, per 3GPP standards, balancing risks associated with false base stations and network management needs for device roaming.

Recommendations and Next Steps

Recommendations for 3GPP

While 5G encryption protected the test device from losing private information to the false base station in these tests, the device was sometimes prevented from connecting to a network until it was manually reset. In the event a manual reset does not occur, 5G devices are configured to eventually reset on their own, based on standards specified by 3GPP, built into the device by the manufacturer, and set by the network operator within those parameters.

Resilience and recovery from false base station attacks can be improved at the device level by shortening the wait timers in the 3GPP standards, which "[give] an opportunity to UEs to recover and avoid lock-outs," as 3GPP notes in its technical specifications. 3GPP sets 5G standards with many network use cases in mind. When devices are roaming, for example, infrequent network resets are better. If a device is unable to connect to a network after a false base station attack, however, a reset as soon as possible is preferable. The 5G Security Test Bed recommends that 3GPP reassess these standards and consider making the reset timelines shorter as it considers the needs of all use cases across 5G networks.

Next Steps for the 5G Security Test Bed

Additional testing in a future phase using different commercial devices is warranted to understand their behavior with respect to the 3GPP standards' expected behavior for the DoS attack and false Public Warning System message test cases.

As new participants and the diversity of test cases grow, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security. The Test Bed continues to explore testing of network function security, roaming security, and aspects of 5G cloud security that arise with use of the Network Exposure Function (NEF), the Application Function (AF), and Multi-access Edge Computing (MEC). The Test Bed is also exploring opportunities to test configurations and enhance Open Radio Access Network (Open RAN) security.

For more information, or to participate in the 5G Security Test Bed, please contact Harish Punjabi (hpunjabi@ctia.org; (202) 845-5701), or visit https://5gsecuritytestbed.com/.


5G
SECURITY™
TEST BED