5G SECURITY™ TEST BED

Securing 5G:

Test Bed Confirms Key 5G Standalone Network Features Enhance User Data Security

Fall 2023 5G Security Test Bed Report Highlights

The 5G Security Test Bed and Its Findings

The 5G Security Test Bed Is the Latest Industry Initiative to Advance 5G Security.

The wireless industry prioritizes stronger security and reliability with every generation of its mobile networks. Stakeholders from across the entire wireless ecosystem work together to develop and improve security features for wireless networks and consumers. The wireless industry's 5G Security Test Bed is the next piece of this commitment. The 5G Security Test Bed is the only initiative that uses commercial-grade network equipment to demonstrate and validate how 5G security standards recommendations will work in real-world conditions.

Validating FCC CSRIC VII Recommendations for 5G Network Security

For this round of tests, the 5G Security Test Bed set out to test recommendations from the FCC's Communications Security, Reliability, and Interoperability Council VII (CSRIC VII) advisory committee. CSRIC VII Working Group 3 worked to identify and evaluate optional features in 5G standards, developed by the international standards body 3GPP, that would potentially cause security gaps in 5G architectures if not implemented. Based on its assessment, CSRIC made several recommendations, which the 5G Security Test Bed verified through this round of tests.

Why 5G Networks Are Secure: Segmented Network Functions, Encryption, and Mutual Authentication

One of the innovations of 5G is the introduction of a Service-Based Architecture (SBA) in which core network functionalities are delivered through a set of interconnected network functions (NFs).

The nature of 5G network architectures enables greater flexibility, targeted customization, and enhanced security when it comes to protecting the network. This includes the implementation of different types of encryption methods—such as mutual transport layer security (mTLS), IP security (IPsec) tunneling, and New Radio Encryption (NEA2) algorithms—that secure and authenticate different network functions as they direct and control traffic throughout the network.

Key Findings:

The 5G Security Test Bed executed several tests to confirm that the implementation of optional 3GPP protections, as recommended by the FCC's CSRIC advisory committee, would improve 5G network security. The tests validated that:

- ✓ **NEA2 algorithms protect user identity data traveling over the air.** Tests 1 and 2 implemented a 3GPP-defined algorithm on the 5G network interface to encrypt user identity information during transmission, ensuring it was indecipherable, and confirmed user identity information is not transmitted before encryption security is established.
- ✓ **Packet Data Conversion Protocol (PDCP) layer protection can be implemented at the full data rate.** Tests 3 and 4 implemented confidentiality protection on the 5G network layer that controls the way user and data traffic is handled. They also confirmed protection can be implemented at the full data rate.

- ✓ **Subscription Concealed Identifier encryption can protect subscriber identity information.** Test 5 implemented a subscription concealed identifier (SUCI) to encrypt the user-identifying information traveling through the network, then confirmed the user device can register to the network with SUCI encryption obscuring identity information.
- ✓ **IPsec tunnels protect data transmission across transport links.** Test 6 implemented an IPsec tunnel to encrypt the data packets traveling through the network, then confirmed that user and control plane traffic transmitted through the tunnel cannot be captured, modified, or injected by an unauthorized entity.
- ✓ **Transport layer security protects data traveling across the Service-Based Architecture interface:** Test 7 implemented transport layer security (TLS) to protect the network elements of the 5G core, then confirmed that with TLS encryption, data packets cannot be captured, modified, or injected on the SBA interface.

5G Security Test Bed Results

Test Cases 1 and 2: NAS and RRC Signaling Confidentiality.

These test cases were designed to demonstrate that only non-user identity related information is transmitted over the air—from the 5G device to the 5G radio to the 5G core—prior to the implementation of signaling encryption.

When the payload data travels from the user's device to the wireless radio tower, it is controlled through a process called Radio Resource Control (RRC) signaling. When the data travels to the 5G core, it is controlled through a process called Non-Access Stratum (NAS) signaling.

The tests confirm that, after implementing a 3GPP-defined cipher algorithm called NEA2 on the network's RRC and NAS interfaces, any data related to the user's identity is encrypted. Prior to encryption, only non-user identity related information can be exchanged, ensuring user confidentiality is preserved.

Test Cases 3 and 4: Access Stratum User Plane Confidentiality and Integrity

These test cases involve the protection of user data traveling over the air from the UE to the wireless radio tower. To test this, NEA encryption was implemented on a layer of the network called the PDCP, or packet data convergence protocol, which controls the way user and data traffic is handled.

The tests confirm that with encryption disabled, all user data is observable, while the data is not observable after the encrypted channel is established.

Test Case 5: Protecting User-Identifying Information as It Travels through Networks

This test was designed to demonstrate robust protections around user privacy and data protection on 5G standalone networks.

Mobile devices have unique global identifiers called Subscription Permanent Identifiers (SUPI) or International Mobile Identifiers (IMSI), which tie individual users to their devices such as through SIM cards. To protect against revealing identifying data about a device's owner, 5G uses the subscription concealed identifier (SUCI) to encrypt the SUPI as it securely transfers this data across the network.

The test confirms that with the use of a SUCI to encrypt the user-identifying information found in the SUPI, identity information is protected as it travels through the network.

WHAT ARE IMSI, SUPI, AND SUCI?

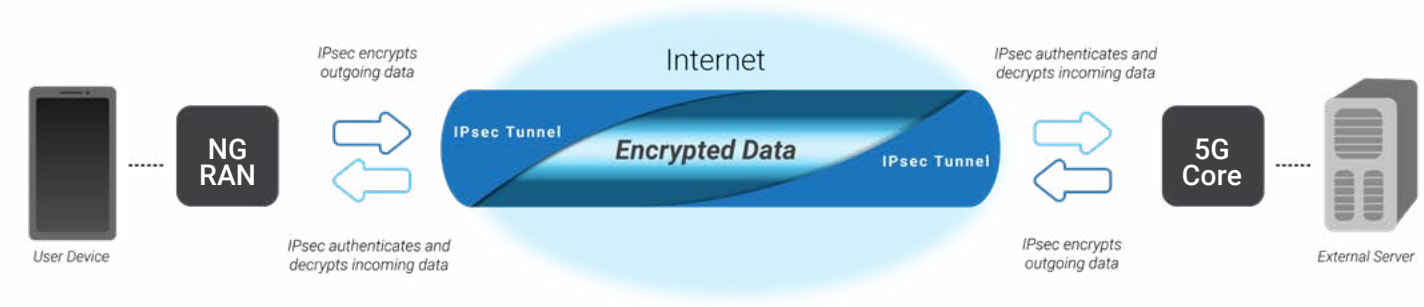
An International Mobile Subscriber Identity (IMSI) is a unique global identifier that ties an individual user to their device, such as through a SIM card. With 5G, the IMSI was updated to the Subscription Permanent Identifier (SUPI), which provides higher security.

5G networks protect these private identifiers—and their users—by encrypting them. Once they are encrypted, they are referred to as a SUCI, or Subscription Concealed Identifier.

Test Case 6: IP Security and Tunneling Protect Network Traffic from Hijacking

This test was designed to demonstrate that an encryption method called an IPsec (IP security) tunnel can be used to protect the data packets traveling through a network.

The two-part test confirms that when the traffic is transmitted through the IPsec tunnel, unauthorized entities are unable to capture, modify, or inject new packets of data into the network —ensuring the data is safe from theft or corruption.



When traveling through an IPsec tunnel, user plane traffic (that is, traffic from the user's device) or control plane traffic (that is, information from the network's control interface) cannot be captured, modified, or injected by an unauthorized entity.

Test Case 7: Transport Layer Security Provides Extra Layers of Protection for Individual Network Elements

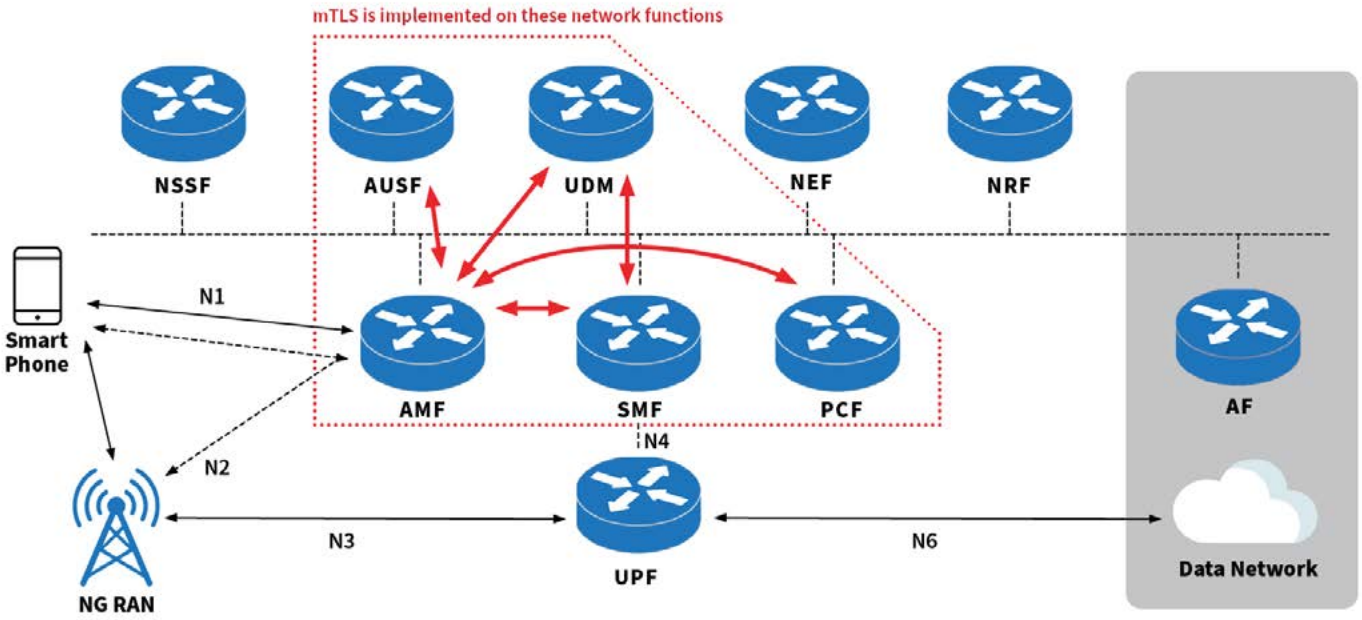
This test was designed to demonstrate that when transport layer security is used to protect the network elements of the 5G core, data cannot be captured, modified, or injected by unauthorized users, applications, or programs.

The test confirms that with no encryption, unauthorized entities can eavesdrop, modify, and insert traffic into the network. When mutual transport layer security (mTLS) is implemented, network traffic is encrypted and undecipherable, and any attempt by an unauthorized user to modify the traffic or inject new data into it results in the connection being terminated.

WHAT IS TRANSPORT LAYER SECURITY?

Transport layer security, or TLS, is a standard for securing data that uses cryptography to encrypt and decrypt data exchanged between sender and recipient networks. The sending and receiving networks decrypt the data they exchange by using public and private digital keys ranging from 128 to 2048 bits long.

In 5G networks, this happens between network functions (NFs), the components that process and control traffic on the network. mTLS takes things a step further, with the sending and receiving network functions each authenticating the other before exchanging information, providing an additional layer of security, as shown below.



Key:

Network Function (NF): Each component of a 5G network plays a different role in transferring data across the network.

mTLS (Mutual Transport Layer Security) Connection: Both network functions authenticate each other to confirm they are valid, then exchange information over the encrypted TLS connection.

Key Takeaways

- The 5G Security Test Bed tests focused on protecting user data, including the confidentiality and integrity of user and device identifiers, and ensuring privacy and confidentiality at multiple locations in the 5G system, including over the air between the user device and physical tower, between the network functions, across untrusted backhaul connections, and on the network's SBA interface.

- The security measures tested include IPsec tunneling (secure gateways between user equipment, physical network towers, and 5G network functions), mutual transport layer security (the mutual authentication of network functions that takes place before data is sent and received over the encrypted TLS connection), and NEA encryption (a type of encryption that is implemented on specific layers of the 5G network).
- The 5G STB found that all of the protection and encryption measures protect user identity and other data from being intercepted, modified, or injected back into the network by unauthorized users. The tests also found that when these optional security protection measures were not configured, 5G traffic could be intercepted and manipulated by unauthorized users.

The test results successfully verified that implementation of 3GPP's optional standards for 5G standalone networks, as recommended by the FCC's CSRIC advisory committee, significantly strengthens 5G network security.

This is great news for consumers—the U.S. wireless industry already voluntarily adopts 3GPP's optional standards to its 5G standalone networks. Implementation will continue to grow as the wireless industry upgrades its 5G networks from non-standalone (5G networks built on a 4G infrastructure) to standalone (networks designed and built specifically for 5G) nationwide. More than 250 million people are already covered by 5G standalone networks across the U.S., and this number will grow steadily, connecting more people to advanced network security features, as carriers continue rolling out network upgrades in the coming months.

Next Steps

For future tests, the 5G Security Test Bed is exploring additional aspects of network function security, false base stations, roaming security, and 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 will also conduct additional phases of network slicing tests.

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