5G Security Test Bed Confirms Implementation of 5G Standalone Network Features Improves User Data Security

The wireless industry's 5G Security Test Bed successfully tested and confirmed that the implementation of optional network security features, including IPsec tunneling, mTLS security, and NEA encryption, protects user data as it is transmitted through various parts of 5G standalone networks.

Robust User Privacy Protections: IPsec Tunneling, mTLS, and NEA Encryption

The 5G Security Test Bed, a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies, has completed its third set of tests to verify the efficacy of 5G security recommendations. The 5G Security Test Bed executed seven tests to confirm that the implementation of optional 3GPP protections, as recommended by the FCC's CSRIC advisory group, would improve 5G network security. The tests validated that:

- ✓ **New Radio Encryption (NEA2) algorithms protect user identity data traveling over the air.** After implementing a 3GPP-defined algorithm on the 5G network interface to encrypt user identity information during transmission, the Test Bed confirmed it was indecipherable. It also 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.** After implementing confidentiality protection on the 5G network layer that controls user and data traffic, the Test Bed confirmed that protection can be implemented at the full data rate. Due to testing equipment limitations, the 5G STB was unable to verify to the degree desired.

- ✓ **Subscription Concealed Identifier (SUCI) encryption can protect subscriber identity information.** After implementing a Subscription Concealed Identifier (SUCI) to encrypt the user-identifying information traveling through the network, the Test Bed confirmed that the user device can register to the network with SUCI encryption obscuring identity information.

- ✓ **IPsec tunnels protect data transmission across transport links.** After implementing an IPsec tunnel to encrypt the data packets traveling through the network, the Test Bed 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.** After implementing transport layer security (TLS) to protect the network elements of the 5G core, the Test Bed confirmed that with TLS encryption, data packets cannot be captured, modified, or injected on the network interface.

5G SECURITY™ TEST BED

What Does This Mean?

A core strength of 5G networks is that they are virtualized, with network functions interconnected on the Service-Based Architecture (SBA) interface, enabling significant flexibility when it comes to securing 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 (NEA) Algorithms, which secure and authenticate different network functions as they interact with each other, control, and route traffic throughout the network.

The successful results of these tests verify that implementation of 3GPP's optional standards for 5G standalone networks, as recommended by the FCC's CSRIC advisory group, 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.

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

Formally launched in 2022, the 5G Security Test Bed is a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, and academia. Its sole purpose is to test and validate 5G security recommendations and use cases from government agencies, standards bodies, wireless operators, and others. The Test Bed is the only initiative that uses commercial-grade network equipment to demonstrate and validate how 5G security recommendations will work in real-world conditions.

The 5G Security Test Bed's members span industry, government, and academia, including AT&T, T-Mobile, UScellular, Ericsson, MITRE, Intel, SecureG, the University of Maryland, and Virgina Tech Advanced Research Corporation (VT-ARC).

The 5G Security Test Bed Enhances the Future of 5G Security

As new participants and the diversity of test cases grow in tandem, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security, including additional phases of network slicing tests. For future tests, the 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 is also exploring opportunities to test configurations of Open Radio Access Network (RAN) to verify security recommendations.

The 5G Security Test Bed members and administrator welcome engagement from stakeholders with an interest in Test Bed's mission, and we expect to develop more and diverse test cases along with new participants. To learn more about the Test Bed, membership, or read the full report, visit www.5Gsecuritytestbed.com.

5G SECURITY™ TEST BED