5G Security Test Bed Verifies Mutual Transport Layer Security as Enabler of Zero Trust

The 5G Security Test Bed recently completed a fourth round of tests focused on mutual transport layer security (mTLS), successfully demonstrating mTLS's efficacy in the encryption and mutual authentication of communications between 5G network functions.

Encryption Across 5G Network Functions: Transport Layer Security and Zero Trust

The 5G Security Test Bed, a unique collaborative endeavor between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies, has completed its fourth set of tests to verify the efficacy of 5G security recommendations. The Test Bed's Technical Advisory Committee designed and conducted five tests to verify recommendations made by the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) around the use of transport layer security on the Service-Based Interface (SBI) between the 5G network functions.

All five tests were successful, confirming that mTLS is a valid means for encrypting and authenticating data traveling between 5G network functions that exchange data across the SBI, enabling Zero Trust in a 5G environment. The tests validated that:

✓ **Additional encryption within the 5G network strengthens security.**
If a 5G network is breached, information within the network can be vulnerable to exposure. mTLS encryption adds an additional layer of security within the 5G core network itself to protect data from attackers.

✓ **Mutual Transport Layer Security protects 5G networks by:**

- **Encrypting and protecting critical data at both ends of the network.** mTLS can encrypt critical user, device, and network information via HTTPS, as well as authenticate and authorize both sides of the HTTPS connection.

- **Rejecting expired and invalid credentials.** After implementation of mTLS, expired or invalid credentials on one end will lead to a failed SBI connection, keeping out-of-date functions that may have vulnerabilities from attaching to the network.

- **Cross-authenticating credentials issued by different certificate authorities.** A 5G core solution can be implemented securely using different CAs, ensuring that mTLS sessions can be established across different certificate authorities.

Because mTLS can be used at numerous points within a 5G network to constantly authenticate the validity of users and functions attempting to connect, it can serve as a foundational component of the Zero Trust approach to network security.

What Does This Mean?

Zero Trust has long been recognized by the wireless industry, and recently by the federal government, as a multifaceted and flexible defense against network attacks. A 2021 Executive Order instructed the federal government to "advance toward Zero Trust Architecture" on its networks, and the Office of Management and Budget released additional guidance for federal agencies that included requirements to encrypt network traffic. The National Institute of Standards and Technology's (NIST) foundational guidance on Zero Trust also recommends "authenticating all connections and encrypting all traffic" on a network.

Together, this round of 5G Security Test Bed tests verifies the important role mTLS can play as a Zero Trust enabler. Zero Trust principles dictate continuous validation of users and data traveling on a network, and the tests successfully demonstrated that mTLS can reliably encrypt and authenticate communications between the network functions that operate on the 5G core's interface.

The mTLS ability to authenticate the validity of network functions that attempt to connect to an SBI, while restricting access to the network from invalid network functions, demonstrates its value as a foundational component of Zero Trust.

This is great news for consumers—mTLS is already being deployed, and implementation will continue to grow as the U.S. 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—like mTLS and Zero Trust—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 and facilities to demonstrate and validate how 5G security recommendations will work in practical, real-world conditions.

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

The 5G Security Test Bed Improves 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.