5G SECURITY™ TEST BED

Securing 5G:

5G Security Test Bed Proves Encryption Technology Improves Network Security

First Report Highlights

The 5G Security Test Bed (5G STB) and Its Findings

The 5G Security Test Bed (5G STB) 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 new 5G Security Test Bed (5G STB) is the next piece of this commitment.

Testing Industry Recommendations to the FCC's CSRIC

For its inaugural tests, the 5G STB set out to assess and validate recommendations the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) made in a 2020 report on security features for 5G non-standalone (NSA) networks, or those built on top of 4G networks and technology, which are often the first iteration of 5G networks.

CSRIC recommendations have not typically involved actual testing, so industry and academia saw value in validating the effectiveness and achievability of CSRIC VII's recommendations.

Real-World Testing: A First of Its Kind

One of the 5G STB's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the 5G STB's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G STB 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.

Key Findings

The 5G STB successfully tested encryption methods for securing data sent from a user device through a 5G NSA network over an untrusted connection, validating that:

- ✓ **IPsec encryption protects networks**
  By implementing an encryption method called an IPsec tunnel—which is a secure pathway where data is encrypted as it travels through a public network—eavesdroppers could not decipher, modify, or inject user or control traffic transferred through the network.

- ✓ **Adding Transport Layer Security (TLS) enhances IPsec encryption further**
  IPsec encryption was performed in a TLS and non-TLS context. Implementing TLS encryption—which uses cryptography that can only be deciphered at the traffic's origin and destination networks with digital keys—further enhanced these protections.

The successful tests confirm that when CSRIC's NSA recommendations are implemented, data from consumers, governments, and enterprises is more secure and not subject to tampering.

The 5G STB's Next Steps

The 5G Security Test Bed's verification of the CSRIC NSA recommendations in a real-world environment is the first of its kind—and it's just the beginning. Future test cases will assess 5G standalone (SA) architecture, where a 5G network is built with only 5G components. Anticipated test case topics include CSRIC's SA recommendations, network slicing and roaming security concerns, IMSI privacy, and new trust anchor solutions.

What is the 5G Security Test Bed?

Formally launched in 2022, 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.

The 5G STB's founding members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, and SecureG; and academic partner the University of Maryland, which also serves as the Test Bed Administrator.

The 5G STB is guided by a Technical Advisory Committee (TAC) made up of the 5G STB's founding members and the Test Bed Administrator. The TAC advises the Test Bed Administrator on the day-to-day technical and operational activities and decisions related to the Test Bed, including but not limited to: development of use cases to be tested, test plan development and review, raw test data analysis, test result and report generation, and development of recommendations to standards bodies based on results.

FOUNDING MEMBERS

WIRELESS PROVIDERS

AT&T

uscellular

T-Mobile

INDUSTRY

ERICSSON

MITRE

SECURE

ACADEMIA

UNIVERSITY OF MARYLAND

How the 5G STB Advances 5G Security: A First-of-Its-Kind Approach

One of the 5G Security Test Bed's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the 5G STB's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G STB reflects the industry's collaborative approach to 5G security—it was created by the directive of CTIA and members of its Cybersecurity Working Group (CSWG), an industry initiative that convenes the country's leading telecom and tech companies to assess and address the present and future of cybersecurity. The 5G STB further builds on the work of a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include the 3rd Generation Partnership Project (3GPP), the Alliance for Telcommunications Industry Solutions (ATIS), the International Telecommunication Union (ITU), the Department of Homeland Security (DHS),
the National Institute of Standards and Technology (NIST), and the FCC, among others.

More specifically, the 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

Why Test CSRIC VII Recommendations?

The FCC tasked CSRIC VII to evaluate the transition from the fourth generation of mobile networks (4G) to the fifth generation (5G) to ensure continued reliability, interoperability, and security. The evolution to 5G is a process that takes time, and this means new technology will coexist with legacy technology. As a result, many initial operations of 5G service use both 4G LTE and 5G equipment. The radio portions of the system are 5G, but the core network can be shared with LTE.

Networks that provide 5G service using a combination of 4G and 5G components are referred to as "non-standalone" (NSA) architecture, while independent 5G networks using components built specifically for only 5G are termed "standalone" (SA) architecture.

CSRIC VII's work resulted in several key reports and recommendations focusing on non-standalone deployment, calling out key 5G features that operators can deploy to ensure the security of their service.

As both NSA and SA networks will be around for years to come, the 5G STB saw value in validating the security features available in these networks in an existence-proof setting. Following the FCC's leadership, the 5G STB utilized the CSRIC VII recommendations to create three test cases to validate encryption security features that can be used in 5G NSA deployments.

5G STB Test Results: Successful Validation of 5G Network Security Recommendations

For its inaugural tests, the 5G STB assessed and validated recommendations from CSRIC's VII 2020 report on optional security features for 5G NSA networks. The 5G STB successfully tested encryption methods for securing data sent from a user device through a 5G NSA network over an untrusted connection.

WHAT IS AN UNTRUSTED CONNECTION?

In a typical wireless network, the connection or link between the radio network and the core network is owned or leased and controlled by one entity (the operator). Depending on how the network is configured, the operator can trust that the link is secure.

In the case of the 5G STB, the radio access network is located at UMD and the core network is at MITRE, and they are connected through the internet. Since the endpoints are controlled by two separate entities, the connection is considered an untrusted link that requires protection so it does not expose the data it carries.

Test Cases 1 and 2: User Plane and Control Plane Confidentiality and Integrity

Test Case 1 focused on securing the user plane—the part of the network that carries the personal content of our everyday communications from device to device. Test Case 2 focused on securing the control plane—the part of the network that controls *how* our data is sent from one place to another. Carriers can also protect this data using a secure tunnel.

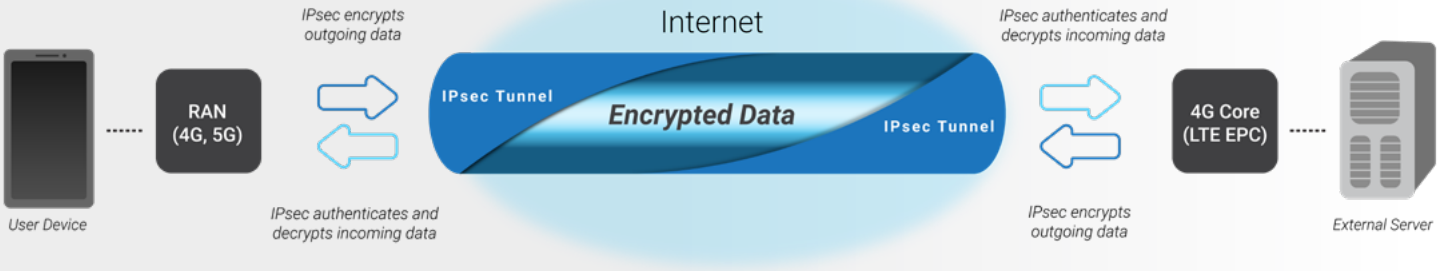
To protect both user and control traffic from eavesdropping or manipulation, carriers can put it in a secure tunnel (called an IPsec tunnel) while it traverses an untrusted link between a user device and the 5G core network. These test cases demonstrated three key findings:

- When networks use an IPsec tunnel over an untrusted connection, all data sent through that connection appears encrypted with no ability to read the contents.
- When networks use the tunnel over an untrusted connection, bad actors are prevented from any eavesdropping on the data.
- When networks use the tunnel over an untrusted connection, bad actors are unable to tamper with or inject false data into it. In fact, false or modified data gets stopped in the tunnel and is unable to even reach the user's device.

Without the tunnel, bad actors can eavesdrop, read, modify, and inject modified data into the connection, which can move freely into the user's device and through the internet. Both test cases found that an IPsec tunnel protects against these actions. For Test Case 2, the false data was also flagged with ABORT messages from the system.

WHAT IS AN IPSEC TUNNEL?

The security method the 5G STB used in tests 1 and 2 consists of an IPsec (IP Security) tunnel. IPsec is a suite of internet protocols that creates a secure "tunnel" through which data can be securely transferred between devices. IPsec tunnels 1) encrypt the data transmitted between two parts of a network through an untrusted connection and 2) authenticate the validity of each packet of data that is exchanged.



Test Case 3: TLS Security on the User Plane

For an even higher layer of security, networks can implement Transport Layer Security (TLS) with the IPsec tunnel. Test Case 3 focuses on performing IPsec encryption in a TLS and non-TLS context. This test case demonstrated four key findings:

- ✓ In a TLS context, all user traffic is encrypted between the user device and its endpoint.
- ✓ In a TLS context, eavesdropping is prevented.
- ✓ In a TLS context, the flow of false or modified data is stopped regardless of whether a secure tunnel is also employed over the untrusted connection.
- ✓ When both TLS and a secure tunnel are implemented, even the source and destination of the data is encrypted.

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.

Key Takeaways

All tests of CSRIC's NSA recommendations were successful, and the suggested security features have been validated. Specifically, the tests confirm that when CSRIC's NSA recommendations are implemented, data from consumers, governments, and enterprises is secure and unable to be tampered with. They confirm that when carriers apply IPsec and TLS encryption technology on 5G NSA networks, additional security protections are extended to these 4G-based networks.

Next Steps

The 5G Security Test Bed's verification of CSRIC's NSA recommendations in a real-world environment is the first of its kind—and it's just the beginning. As new participants and the diversity of test cases grow in tandem, the 5G STB will continue contributing to the evolving future of 5G network security.

The 5G STB has already begun work on its next set of test cases, which will assess 5G standalone (SA) architecture, where a 5G network is built with only 5G components. Anticipated future test case topics include CSRIC's SA recommendations, network slicing and roaming security concerns, IMSI privacy, and new trust anchor solutions.

The 5G STB members and administrator welcome engagement from stakeholders with an interest in the mission of the 5G Security Test Bed. To learn more about the 5G STB or membership, read the full report, or view and download the report one-pager, visit www.5Gsecuritytestbed.com.


5G
SECURITY™
TEST BED