WHAT IS MTLS?

Mutual Transport Layer Security encrypts, protects, and authenticates data as it travels across 5G network functions—ensuring data is continuously authenticated at each point as it travels through the network and enabling Zero Trust.

WHAT IS ZERO TRUST?

An approach to network security that relies upon continuous monitoring authentication of all data, users, applications, and devices accessing or traveling through a network.

HTTP/2 SECURITY

mTLS serves as an enabler of Zero Trust on 5G networks, enhancing security as information travels across 5G network functions.

5G Security Test Bed Validates Security of HTTP/2 Protocol for 5G Networks

At the request of the FCC, the Communications Security, Reliability, and Interoperability Council (CSRIC) VIII advisory group examined and made recommendations to enhance security for the newly adopted 5G signaling protocol, HTTP/2. The wireless industry's 5G Security Test Bed recently conducted an analysis to assess CSRIC's findings and recommendations, determining that the use of mutual transport layer security (mTLS) encryption enhances network security by serving as an enabler of Zero Trust.

HTTP/2 in 5G Networks

HTTP/2 is the first major revision of Hypertext Transfer Protocol (HTTP), the original protocol used to transfer information on the World Wide Web. HTTP/2 has been implemented into most web browsers since 2015 and includes improved features over the previous HTTP/1.1, such as increased speed.

HTTP/2 is now being used in 5G network to handle most of the 5G signaling that takes place to validate, control, and direct traffic that flows through the network. When used in this way, known HTTP/2 vulnerabilities can be mitigated through the advanced security features available in 5G network architectures. CSRIC considered HTTP/2's vulnerabilities in a 5G context and recommended specific safeguards that protect 5G networks when implemented, summarizing the concerns and recommendations as documented in a 2023 report.

mTLS Enables Zero Trust and Secures HTTP/2 Signaling on 5G Networks

To assess CSRIC's recommendations, the 5G STB analyzed results from prior tests it conducted on 5G standalone (SA) networks and mTLS security. It confirmed that:

- ✓ The use of mTLS, by constantly encrypting and authenticating information as it travels through the network, prevents a bad actor with access to the core, but without valid credentials, from deciphering or inserting malicious messages into the network.

- ✓ mTLS prevents a malicious network function (NF), without approved credentials, from connecting with other network functions, the malicious NF is consequently unable to send such requests.

What Does This Mean?

HTTP/2 is used in the 5G core because it has better performance and is more secure. The way it is being used in the 5G core in conjunction with mTLS, along with other recommendations made in the CSRIC WG3 report that help enable Zero Trust, make it dramatically more secure. Although the use of mTLS is a recommended but not required standard, the wireless industry already implements this technology in 5G SA network architecture, enhancing the security of information exchanged through its SA networks.

To learn more about the Test Bed, membership, or read the full report, visit www.5Gsecuritytestbed.com.

5G SECURITY™ TEST BED