5G SECURITY TEST BED™

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

March 2024

Table of Contents

Introduction

At the request of the Federal Communications Commission (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 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. The findings are summarized in this report.

What Is HTTP/2 Protocol?

HTTP/2 is the first major revision of Hypertext Transfer Protocol (HTTP), the original protocol used to transfer information on the World Wide Web. The new HTTP/2 protocol 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 networks to handle most of the 5G signaling that takes place to validate, control, and direct traffic that flows through the network.

When used on 5G network interfaces, known HTTP/2 vulnerabilities can be mitigated through the advanced security features available in 5G network architectures. CSRIC's Working Group 1 (WG1) considered these vulnerabilities in a 5G context and recommended specific safeguards that protect 5G networks when properly implemented. In June 2023, the group summarized the recommendations in its "Report on Best Practices to Mitigate Security Vulnerabilities in HTTP/2."[1]

CSRIC's HTTP/2 Assessment and Recommendations

The CSRIC VIII report considered four classes of vulnerabilities:

1) Client Initiated Attacks on Servers
2) Heist Attacks
3) Custom HTTP/2 Headers
4) Implementation Vulnerabilities

Further, the report identified best practices and made specific recommendations for each class. Client Initiated Attacks on Servers comprise attacks in which a malicious actor sends valid HTTP requests to a server, and the recommendation is to employ insider threat mitigation practices and controls. The Heist Attack extracts encrypted information based on how an operating system handles other protocols, and the recommendation is to scan the 5G core constantly for vulnerabilities. The Custom HTTP/2 Header attack assumes a compromised network function that modifies some of the custom header fields to attack the producer, and the recommendation is to monitor network function activity. Implementation Vulnerabilities are specific to a vendor's implementation of HTTP/2, and the recommendation is to keep the systems patched and up to date.

In the 5G Security Test Bed's analysis to assess CSRIC's HTTP/2 concerns and recommendations, no new tests specific to those recommendations were necessary. The Test Bed leveraged results from prior tests, which provide relevant evidence supporting mitigations to the potential vulnerabilities associated with HTTP/2 use on the 5G Service-Based Architecture (SBA) interface (SBI).

[1] CSRIC VIII Working Group 1 (WG1) "Report on Best Practices to Mitigate Security Vulnerabilities in HTTP/2," June 2023.

This document discusses the applicability of those tests, which were based on previous recommendations from CSRIC VII Working Group 3 (WG3) Report 2 for securing Standalone (SA) architecture, "Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security."[2] Specifically, 5G Security Test Bed test cases TC-SA-07 from the CSRIC SA-motivated tests[3] and TC-SBI-04 from the mTLS tests[4] contain relevant findings.

The 5G Security Test Bed Proves mTLS Enhances HTTP/2 Security on 5G Networks

While the 5G Security Test Bed's tests did not explicitly duplicate any of the vulnerabilities outlined by CSRIC VIII WG1, our general recommendation is to use encrypted HTTP (HTTPS) on the SBI, which would apply Zero Trust principles to each network function connection. Zero Trust principles dictate continuous validation of users and data traveling on a network, and mutual transport layer security (mTLS) plays an important role as a Zero Trust enabler.

Specifically, the test case TC-SA-07 demonstrated how the use of mTLS prevents unauthorized actors from inserting valid requests into the SBI. This is because mTLS ensures the sending and receiving network functions authenticate each other to confirm they are valid, then exchange information over the encrypted TLS connection. mTLS also ensures encryption of signaling information exchanged between the various 5G network functions (NFs).

Furthermore, TC-SBI-04 demonstrated that mTLS prevents a malicious network function, without approved credentials, from connecting with other network functions and is consequently unable to send such requests.

For the first three classes of vulnerabilities outlined by CSRIC, mTLS provides significant protection, requiring successful attacks of this sort to first compromise an authorized network function. With regard to the fourth class, exploration of implementation vulnerabilities is outside the scope the 5G Security Test Bed. More details on the results of the prior testing are provided below.

TC-SA-07: CSRIC 7 WG 3 – mTLS for SBA Interfaces

This test case demonstrated the benefits of mutual authentication and encryption on the 5G core SBI. Initially, the core was configured to use HTTP/2 to connect network functions. With that configuration, tests showed how an actor with access to the SBI could eavesdrop on traffic, as well as modify and inject false traffic. The second part of the test involved instantiating mTLS, where each network function mutually authenticates with each other and the traffic between them is encrypted. With encrypted traffic, an actor with access to the SBI but without valid credentials can neither eavesdrop nor inject traffic destined to network functions. The results of the tests are summarized in the table below.

[2] CSRIC VII Working Group 3 (WG3) "Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security," March 10, 2021.
[3] 5G Security Test Bed CSRIC-Inspired SA Test Report, "Securing 5G: CSRIC VII 5G Standalone Network Test Report," Q4 2023, available at https://5gsecuritytestbed.com/wp-content/uploads/2023/12/5G-STB-SA-Technical-Report-Q42023.pdf.
[4] 5G Security Test Bed mTLS on SBI Test Report: "Securing 5G: mTLS Security on 5G Network SBI Test Report," Q4 2023, available at https://5gsecuritytestbed.com/wp-content/uploads/2023/12/5G-STB-mTLS-Technical-Report-Q42023.pdf.

Condition	Status
Able to eavesdrop on SBA interfaces when mTLS not implemented	Able to identify IP addresses for AMF, AUSF, NRF, SMF, UDM; as well as IMSI/SUPI
Able to modify traffic on SBA interfaces when mTLS not implemented	Able to intercept message between NRF and AMF and modify SMF IP address without producing error
Able to insert traffic on SBA interfaces when mTLS not implemented	Able to insert duplicate packets on SBA interface, which is received successfully by the AMF, causing it to issue a GOAWAY command
Unable to eavesdrop on SBA interfaces when mTLS implemented	After successful mTLS handshake, all subsequent data encrypted and undecipherable
Unable to modify traffic on SBA interfaces when mTLS implemented	After successful mTLS handshake, any attempt to modify encrypted traffic results in an error and reset, tearing down the connection
Unable to insert traffic on SBA interfaces when mTLS implemented	Inserting duplicate encrypted packet into SBA interfaces causes error and disconnection of session between network functions
Overall Test	Success

TC-SBI-04 – Unknown VNF Attach Prevention

This test case installs a certificate on the AMF network function using a different root certificate authority ("AMF-root-CA") than that used for the other network functions in the 5G core. As a result, when the AMF tries to authenticate to the NRF, the handshake fails because the NRF does not recognize the CA used for the AMF certificate. This test case is intended to demonstrate mutually authenticated TLS, and how untrusted credentials on one end will lead to a failed SBI connection. This will prevent any unwanted network functions from attaching to the network.

Condition	Status
Certificate signed by AMF-root-CA installed successfully on AMF	Certificate using "AMF-root-CA" successfully installed on AMF
Handshake between AMF and NRF fails	AMF responds to NRF with "Unknown CA" Fatal Alert
Overall Test	Success

Conclusions

HTTP/2 is used in the 5G core because it is has better performance, and its vulnerabilities are well-understood. In spite of its vulnerabilities, the way HTTP/2 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 significantly more secure. As a result, the 5GSTB recommendation to employ mTLS among the 5GC network functions form part of the solution to the vulnerabilities raised in the CSRIC VIII WG1 report on HTTP/2 vulnerabilities.

While the 5G Security Test Bed did not execute tests specific to the CSRIC VIII WG1 recommendations, prior tests related to SBA security using mTLS demonstrate two key benefits: (1) when mTLS is implemented among the network functions, an actor with access to the core, but without valid credentials, can neither decipher nor insert malicious messages; and (2) a network function with a

credential not signed by the correct certificate authority cannot establish an encrypted connection to the other network functions in the core. Consequently, the vector for attacks such as Client Initiated Attacks on Servers, Heist Attacks, and Custom HTTP/2 Headers is significantly reduced.

mTLS in conjunction with HTTP/2 significantly enhances 5G network security, and the 5G Security Test Bed echoes CSRIC's recommendation that it be implemented in 5G networks. Although the use of mTLS is a recommended but not required standard, the wireless industry already implements this technology in the 5G SA network architecture, enhancing the security of information exchanged through its networks.

About 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 Security Test Bed reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. The Test Bed's members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, SecureG, Syniverse, and Intel; and academic partner the Virgina Tech Advanced Research Corporation (VT-ARC).

The 5G Security Test Bed further works with 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 International Telecommunication Union (ITU), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Federal Communications Commission (FCC), among others.

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/.