5G SECURITY TEST BED™

Securing 5G:

5G Security Test Bed's Network Slicing Tests Strengthen 5G Security

Spring 2024 Network Slicing Phase 2 Report Highlights

OVERVIEW:

The 5G Security Test Bed and Its Findings

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

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. The 5G Security Test Bed 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.

Network Slicing Tests Lead to Improvements in 5G Security

The 5G Security Test Bed completed its latest round of tests, investigating and verifying network slicing security features outlined in a 2021 AdaptiveMobile Security (AMS) report, *A Slice in Time: Slicing Security in 5G Core Networks*. These tests resulted in the development of enhanced wireless network security and user data protections, strengthening the international 5G network slicing standard.

Key Findings:

Based on guidance from its Technical Advisory Committee (TAC) and the AMS report, the 5G Security Test Bed created and executed two tests to demonstrate whether a theoretical network slicing mis-provisioning scenario outlined by AMS could be exploited in a real-world environment.

✓ **Test Case 1: Access to Unauthorized Network Slice by Modifying Slice ID.** In this hypothetical case defined by AMS, a compromised user device could leverage existing permission to access a specific 5G network function that is accessible on an authorized slice, create a connection to another network function shared by another slice, and use that to gain access to data on the other slice. **The Test Bed confirmed the scenario and reported its findings to 3GPP, leading to updated technical standards that resolved the potential issue and strengthened 5G network security.**

✓ **Test Case 2: 5G Network Override to Reroute Mis-Provisioned User Slice.** In this case defined by the Test Bed, a mis-provisioned, mis-configured, or otherwise manipulated user device attempts to provision itself for a slice different from the one defined and authorized by the network operator. **The Test Bed demonstrated the scenario and successfully verified that 5G's existing security features mitigated the issue—the network recognized that the network slice was incorrectly provisioned, overrode the invalid request, and directed the traffic to the correct slice.**

Thanks to these tests—the first to validate and assess these theoretical cases on a live 5G network—the 3rd Generation Partnership Project (3GPP) updated the 5G technical specifications found in TS 33.501, Release 18, resolving the vulnerability. The Test Bed's work directly enabled stronger international standards for network slicing, enhancing 5G security.

Network Slicing, Slice Identifiers, and Test Cases:

Network Slicing

Network slicing is a technology that enables mobile network operators to provide fine-grained, customizable network offerings to meet the diverse needs of a variety of customers and applications, such as in public safety, transportation, security, and many other contexts.

Often, network slices are discussed in the context of leading commercial applications, such as the four wireless network service types defined by 3GPP: eMBB (Enhanced Mobile Broadband), URLLC (Ultra-Reliable Low-Latency Communication), mMTC (Massive Machine-Type Communication), and Vehicle to X (V2X). In addition, network slices for specific uses, such as vehicle-to-infrastructure, or a specific company's industrial control system, are also considered for application of the network slicing concept.

Network slices can be viewed as logical networks sharing a common physical infrastructure. The security for network slicing will be critical to certain segments of commercial customers. Regarding network slice security, because network slices leverage network function (NF) virtualization and a service-oriented architecture, the main focus for slice security has been to ensure isolation among different slices. Specifically, there are two aspects of isolation: resource provision/isolation and security isolation. Security isolation not only requires slice-specific access control and security measures, but also ensures that potential problems in one slice will not spill over to other slices.

Network Slice Identifiers and Potential Exploits

In the 5G network core, each slice is given a unique identity called the Single-Network Slice Selection Assistance Information (S-NSSAI). The S-NSSAI is used to identify, differentiate, authorize, and route each slice and the data traveling on it. The S-NSSAI identifies each slice in two parts: a mandatory Slice Service Type (SST), which is a predefined value for one of the wireless network service types defined by 3GPP listed above, and an optional Slice Differentiator (SD), which is used to differentiate between slices of the same type.

In some cases, user equipment (UE) may be authorized to access more than one slice, and the network further differentiates these with a group or list of up to eight slices identified by Network Slice Selection Assistance Information (NSSAI). NSSAIs can fall into several categories, including Allowed, Rejected, Configured, or Requested NSSAIs.

At the time of its report release, AdaptiveMobile noted that 3GPP standards did not require mobile network operators (MNOs) to assign each slice a unique identifier, or that Slice Differentiators be random, adding that, "With all the new network functions and services in 5G, roaming and legacy interaction will become quite complex."

With no guidance for interoperability between vendors in 3GPP's technical standards at that point, *A Slice in Time* highlighted a hypothetical scenario where slices could potentially be manipulated to do more than they should be able to do, including by brute forcing or guessing slice identifiers to access unauthorized information or resources within the network.

Definition of Test Cases

Based on guidance from its Technical Advisory Committee (TAC) and the AdaptiveMobile report, the 5G Security Test Bed created and executed two tests to demonstrate whether the theoretical scenario could be exploited in a real-world environment.

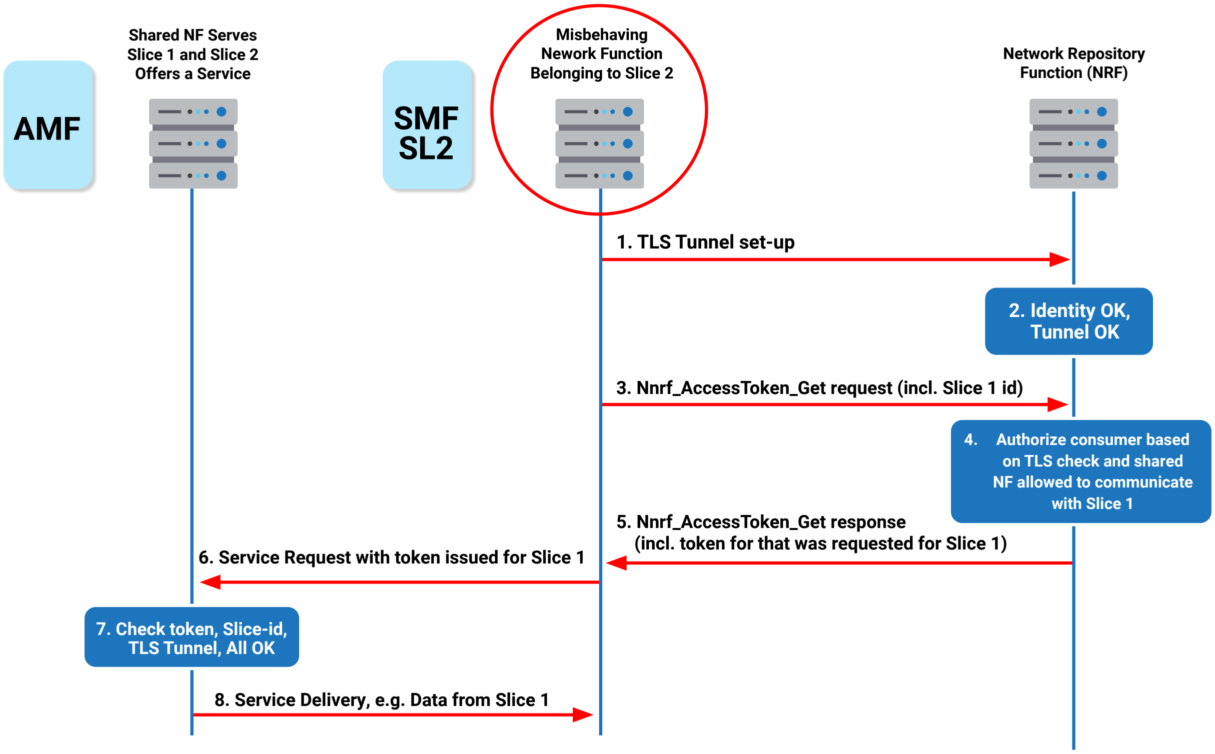
In the first potential exploit outlined in the AdaptiveMobile report, “Malicious Access to a Different Slice by Modifying Slice Differentiator,” a rogue network function or a rogue slice from a compromised partner (Slice 2 in this example) could establish a transport layer security (TLS) connection that appears valid because it is using the correct slice identity. This rogue slice would then be allowed to access the network function shared with the valid Slice 1 and granted a valid identification token. With this access token, the network’s transport/IP layer security would determine the rogue slice is a valid connection, granting it access to personal data or resources within the network.

The report discusses how this would work:

> *The underlying problem is that no layer matching is mandated by the specifications. As there is no matching between layers, the NRF would only see, on the lower transport/IP layer, an “authenticated partner” and, on the upper signalling layer, a valid slice identity and service request. There is no cross-check that the slice identity in the request matches the slice identity used for the TLS tunnel. As a result, the NRF would issue an authorization ticket to the rogue Slice 2 to use services on Slice 1.*

The 5G Security Test Bed performed the first live 5G network tests to confirm that this hypothetical vulnerability exists, listed in this report as Test Case 1.

Diagram of Test Case 1 Vulnerability

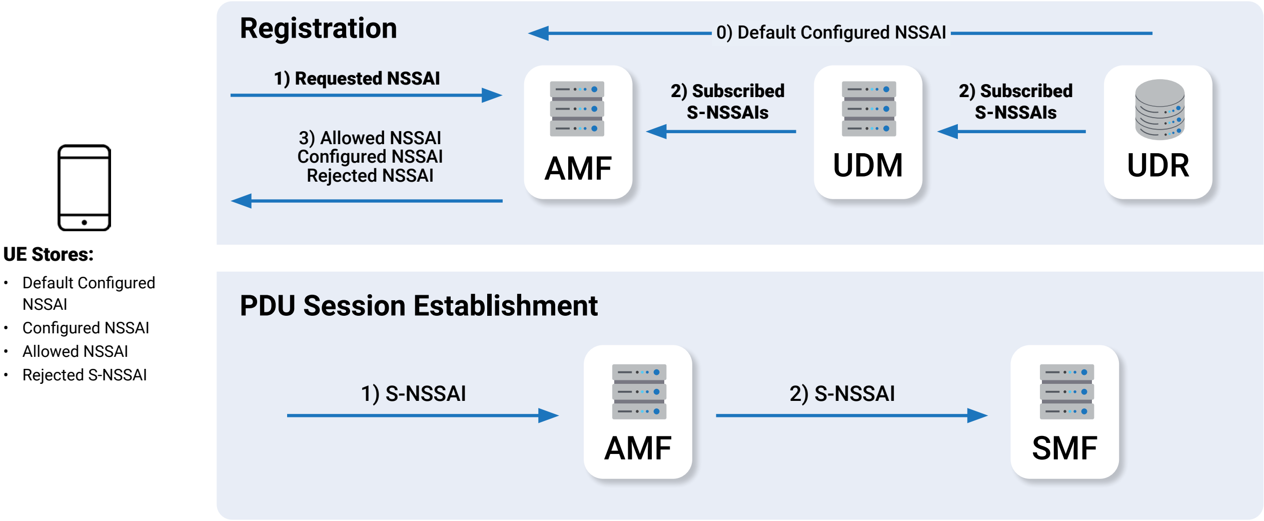

AMF
Shared NF Serves Slice 1 and Slice 2 Offers a Service
SMF SL2
Misbehaving Nework Function Belonging to Slice 2
Network Repository Function (NRF)
1. TLS Tunnel set-up
2. Identity OK, Tunnel OK
3. Nnrf_AccessToken_Get request (incl. Slice 1 id)
4. Authorize consumer based on TLS check and shared NF allowed to communicate with Slice 1
5. Nnrf_AccessToken_Get response (incl. token for that was requested for Slice 1)
6. Service Request with token issued for Slice 1
7. Check token, Slice-id, TLS Tunnel, All OK
8. Service Delivery, e.g. Data from Slice 1

Test Case 1: Message Flow of Hypothesized Vulnerability

In addition, the Test Bed developed a second test case based on the hypothetical scenario, "Static Subscriber S-NSSAI Override of UE-Requested NSSAI by Dynamic Core Signaling Assignment," or more simply called "5G Network Override to Reroute a Mis-Provisioned User Slice."

In Test Case 2, the Test Bed assumed that a user device had been mis-provisioned to a network slice that was inconsistent with how it was recorded by the network operator. In this example, the UE should be provisioned for Slice 2, but it incorrectly presents Slice 1 as the Requested NSSAI to the network. Test Case 2 was conducted to determine whether the network would override the incorrect request and direct the UE to the correct slice.

Diagram of Slice Selection and Use for Test Case 2



Test Case 2: Slice Selection and Use

The scenario outlined by AdaptiveMobile and demonstrated in Test Case 1 is a niche edge case that requires a very specific set of circumstances to occur and would be difficult to execute in the real world. However, by confirming with real-world tests and disclosing the findings to 3GPP, the 5G Security Test Bed enabled stronger 5G network standards that eliminated the scenario and enhanced 5G security.

5G Security Test Bed Results

Test Case 1: Access to Unauthorized Network Slice by Modifying Slice ID

Test Case 1 verified that a modified request could be sent from a rogue network function and slice, then shared with other network functions to gain access to information on other slices. To do so, the NRF generated a valid token for the shared AMF network function and provided it to the rogue network function.

✓ **Confirmed:** The shared AMF network function responded to the maliciously crafted token and granted the rogue network function access to the network, thus confirming that the hypothetical scenario could be exploited. The Test Bed reported its findings to 3GPP, leading to updated standards resolving the issue.

Test Case 2: 5G Network Override to Reroute a Mis-Provisioned User Slice

Test Case 2 was designed to test a second potential exploit and confirm that the network would override incorrectly provisioned UE by comparing its network slice request to the network slice provisions recorded by the network operator. To do so, the UE was incorrectly provisioned with a Requested NSSAI for Slice 1, but the network overrode it using the default subscribed S-NSSAI in the subscriber UDM slice profile (Slice 2). This forced the UE to connect to the correct Slice 2.

- ✓ **Confirmed:** The test confirmed that the 5G network's existing controls detected the mis-provisioned network slice request, overrode the request, and redirected the UE to its correct slice.

Key Takeaways

The 5G Security Test Bed conducted the first ever real-world tests to verify that the hypothetical scenario identified in an AdaptiveMobile Security report could be executed on a live 5G network—leading to strengthened international standards for network slicing and enhancing 5G security.

The 5G Security Test Bed's Findings Drove Stronger Network Slicing Security

AdaptiveMobile's network slicing report was submitted to GSMA as a Common Vulnerability Disclosure (CVD) in 2021. As a result, 3GPP began assessing and addressing the hypothetical vulnerability in new releases, but the standards body could not create definitive standards until the scenario was validated.

Thanks to the 5G Security Test Bed's validation of the scenario on a live 5G network, 3GPP was able to add a solution in updated technical standards. 3GPP's Service and System Aspects Working Group 3 (SA3) wrote a Change Request (CR) that was accepted and implemented recently in TS 33.501, Security architecture and procedures for 5G system, Release 18, in section 13.4.1.1.2.

Specifically, 3GPP now requires the NF Service Producer to confirm that the NF Service Consumer has authorization to access at least one of the slices the UE is registered to, by cross-checking and verifying that the UE's slice identifiers match the NF Service Producer's slice identifiers listed in the access token.

TS 33.501 added the following language to ensure that with shared NFs, the NF slice identifier is now checked:

> *If applicable (e.g., when the request is for information related to a specific UE), the NF Service Producer may check that the NF Service Consumer is allowed to access (as indicated by the NF Service Producer's NSSAIs in the access token presented by the NF Service Consumer) at least one of the slice(s) that the UE is currently registered to, e.g., by verifying that the UE's allowed NSSAI(s) intersect with the NF Service Producer's NSSAIs in the access token.*

The successful execution of these tests reflects the 5G Security Test Bed's value as a platform for testing and validating theoretical scenarios in real-world conditions, providing validation of use cases that had previously been discussed only in theory.

Next Steps

As new participants and the diversity of test cases grow, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security. The 5G Security Test Bed is exploring future tests of network function security, false base stations, roaming security, and aspects of 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 and enhance Open Radio Access Network (Open RAN) security.

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/.

5G
SECURITY™
TEST BED