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

The wireless industry's 5G Security Test Bed completed its latest round of tests, investigating and verifying a network slicing security scenario outlined in an AdaptiveMobile Security (AMS) report. This Test Bed effort resulted in the development of enhanced wireless network security and user data protections, strengthening the international 5G network slicing standard.

Network Slicing and Slice Identifiers

Network slicing is a technology that enables wireless network operators to split a single 5G network into multiple virtual networks—or "slices"—within the shared physical network. Network slicing can be used to provide fine-grained and customizable service offerings to meet the diverse needs of a variety of customers and applications, such as in public safety, transportation, security, and many other contexts.

The 5G Security Test Bed—a wireless industry-led endeavor that leverages collaboration between wireless providers, equipment manufacturers, cybersecurity experts, academia, and government agencies—focused on network slicing in its latest round of testing to validate 5G security recommendations and use cases. The Test Bed's Technical Advisory Committee designed and executed this set of tests based on "provisioning" scenarios described in AdaptiveMobile's 2021 report, *A Slice in Time: Slicing Security in 5G Core Networks*.

To correctly allocate, or provision, 5G network traffic to its authorized slice, each network slice or bundle of slices is given its own identifier called the Single-Network Slice Selection Assistance Information (S-NSSAI). In its report, AMS suggested that a device could improperly access a network slice if user devices are provisioned with the wrong slice ID.

Network Slicing Tests and Results

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

- ✓ **Test Case 1: Access to Unauthorized Network Slice by Modifying Slice ID.** In this hypothetical test case defined by AMS, a compromised user device could leverage existing permission to access a specific 5G network function (NF) that is accessible on an authorized slice, create a connection to another network function shared by a different slice, then use that to gain access to the 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 a Mis-Provisioned User Slice.** In this test 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.**

Both scenarios are niche cases that are extremely difficult to execute in practice, and only one was confirmed to be executable, while the other was automatically corrected by the network's existing controls.

Network Slicing Tests Strengthened 5G Network Security

After AdaptiveMobile filed its report as a Common Vulnerability Disclosure (CVD) with international standards body 3GPP, the standards organization began addressing the hypothetical scenario in new releases, but it could not create definitive standards until the issue was confirmed in the real world.

Thanks to the 5G Security Test Bed's validation of the scenario on a live 5G network, 3GPP was able to conclusively verify and address the potential issue. Specifically, 3GPP updated the international technical standards for 5G to require the NF Service Producer to confirm that the NF Service Consumer has authorization to access at least one of the slices the user device is registered to, by cross-checking and verifying that the device's slice identifiers match the NF Service Producer's slice identifiers listed 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. As new participants and the diversity of test cases grow, the 5G Security Test Bed will continue testing and contributing to the evolving future of 5G network security.