White paper

Anritsu envision : ensure

A Bottom-Up Approach to 5G Network Slicing Security in User Equipment

Introduction

5G networks have become an integral part of the global digital economy and the communication infrastructure that corporations, government, and military organizations will rely on for the foreseeable future. These networks' success will depend in good part on their ability to resist, survive, and recover from a growing number of traditional and emerging cyberthreats. This mandates that all elements of their infrastructure, along with the user equipment (UE) that accesses them, be rigorously tested in order to ensure their compliance with 5G security protocols standards and identify potential vulnerabilities to the growing number of attack strategies.

Smart phones, mobile computing devices, and other types of UEs present one of the largest, most complex attack surfaces in the 5G ecosystem. Some of this is due to the sheer number of devices operating in an open, uncontrolled environment and the large number of manufacturers who produce them. UE devices also present an attractive attack surface because they communicate via radio signals. Drilling down a bit further, we find that many of their potential vulnerabilities lie in the complex set of protocols they must use to negotiate, establish, and secure network slices (i.e., the virtual point-to-point pipelines that deliver pre-negotiated levels of speed, latency, quality of service [QoS], and security within a 5G network).

Securing 5G UE products against these threats requires a "bottom-up" approach where:

a) Security is an integral part of the design that begins in the early stages of their development.

b) Every stage of functional verification includes testing for potential vulnerabilities and ensuring strict compliance with 5G's protocols and security standards.

This bottom-up methodology should be applied to evaluating new designs for both UE and infrastructure equipment, as well as for verifying system updates and upgrades – especially ones that add new 3GPP features.

This white paper will help you understand how to use testing and verification of network slicing functionality as part of a bottom-up strategy for hardening your products against cyberthreats. Many of the same practices discussed here can also be applied to the ASICs, processors, software, and other major components that are used in 5G end products. This white paper begins with a brief overview of the 5G network slicing architecture and the security mechanisms that protects it, and then takes a deeper dive into strategies for verification and testing of UEs during the development process.

Network Slicing 101

5G is a significant departure from 4G LTE. 4G LTE provided an IP data pipe primarily designed for the delivery of voice, video, and other multimedia services, and included secondary provisions for supporting machine-to-machine (M2M) and Internet-of-Things (IoT) applications. In contrast, the 5G standard was specifically architected so that it could be optimized for a range of use cases.

The 5G network architecture implements a feature called network slicing. This enables network providers to create virtual end-to-end network connections with clearly defined channel capacities, QoS parameters, priority levels, and security requirements that are tailored to application requirements and UE capabilities. These applications can range from sub-kbit/s, high-latency data streams used to read utility meters and manage streetlights in Smart Cities, to Ultra-Reliable Low Latency Communication (URLLC) services that will provide connectivity for critical applications such as autonomous vehicles, factory automation systems, and telesurgery robots. The same mechanism will be used to provide highly reliable, secure communication services for government, law enforcement, and military organizations (Figure 1).

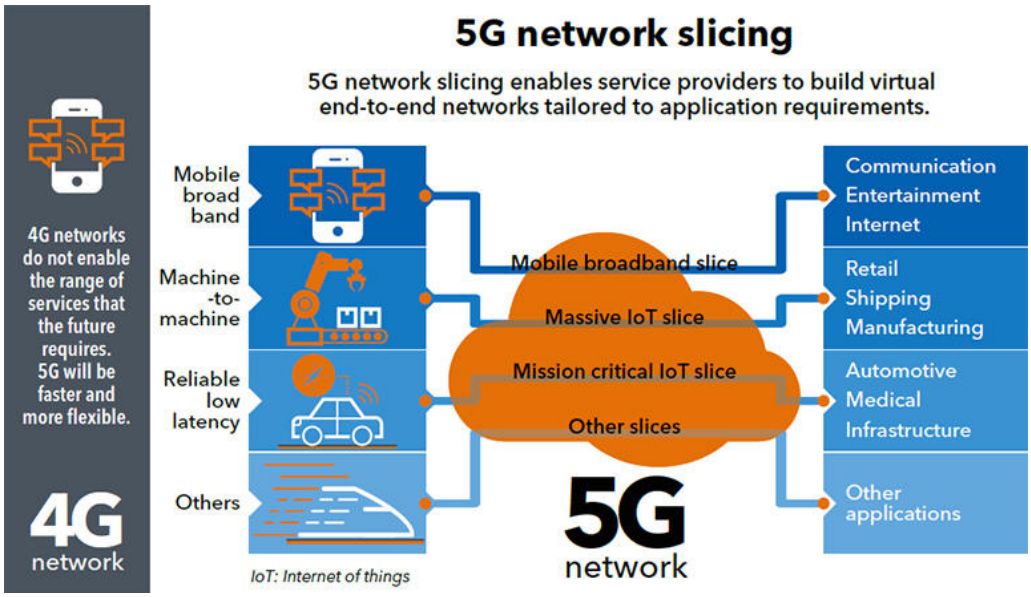
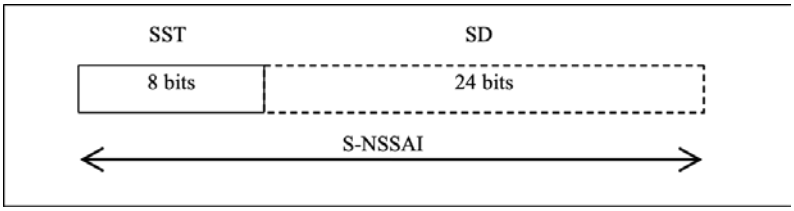


Figure 1: *A top-level view of how 5G network slicing provides end-to-end virtual connections with guaranteed levels of speed, QoS, security, and reliability. (Michael Geller and Pramod Nair (June 2018). 5G Security Innovation with Cisco. Cisco Blogs. https://blogs.cisco.com/sp/5g-security-innovation-with-cisco.)*

How a 5G Network Creates a Network Slice

To get a better sense of how network slicing works, let's look at the process of how a smartphone (or any other 5G UE) establishes a connection (also known as an application/PDU session) with a 5G network. First, the UE contacts the local radio access network (RAN) and initiates a sequence of transactions known as the network slicing provisioning procedure. The Authentication Server Function (AUSF) inspects the UE's credentials to ensure it possesses a valid identity and that it is authorized to access the RAN. This is followed by an exchange of capability information and the submission of one or more data frames, known as Single Network Slice Selection Assistance Information (S-NSSAI). This contains the slice/service type (SST) that defines the level of service it requires and a slice differentiator (SD) field, which contains optional information that helps the network understand more about the resources the network slice requires and to differentiate it from the other application sessions currently in progress (Figure 2).



Slice/Service Type	SST Value	Characteristics
MBB	1	Slice suitable for the handling of 5G enhanced mobile broadband
URLLC	2	Slice suitable for the handling of Ultra-Reliable Low Latency Communication
MIoT	3	Slice suitable for the handling of massive IoT
V2X	4	Slice suitable for the handling of vehicle to everything services

Figure 2: *The S-NSSAI frame structure and standardized SST values. Notes: The support of all standardized SST values is not required in a public land mobile network (PLMN). Services indicated in this table for each SST value can also be supported by means of other SSTs. (From 3GPP 23.003 28.4.2 and 23.501 5.15.2.2.)*

The number of single NSSAIs required to define an application session's requirements vary and are referred to collectively as the NSSAI. At present the following NSSAI types have been defined:

- **Configured NSSAI:** NSSAI provisioned in the UE applicable to one or more PLMNs (may include a default).
- **Subscribed S-NSSAI:** UE specific based on subscriber information and the serving PLMN.
- **Requested NSSAI:** NSSAI provided by the UE to the Serving PLMN during registration.
- **Allowed NSSAI:** NSSAI provided by the serving PLMN during a registration procedure, for example, indicating the S-NSSAIs values the UE could use in the Serving PLMN for the current registration area.
- **Rejected NSSAI:** NSSAI rejected by the PLMN (e.g., due to subscriber profile or availability).

As illustrated in Figure 3, the network presents the information contained in the NSSAI to its Policy Control Function (PCF), which maintains the UE Route Selection Policy (URSP) data to determine the best routing for the network slice and the services it can provide the UE. During this process, the PCF uses the Non-Access Stratum (NAS) messaging protocol to acknowledge the UE and inform it of the resources available to it. The UE uses NAS messaging to request a protocol data unit (PDU) session for specific applications based on the URSP-NSSAI mapping information it has been given.

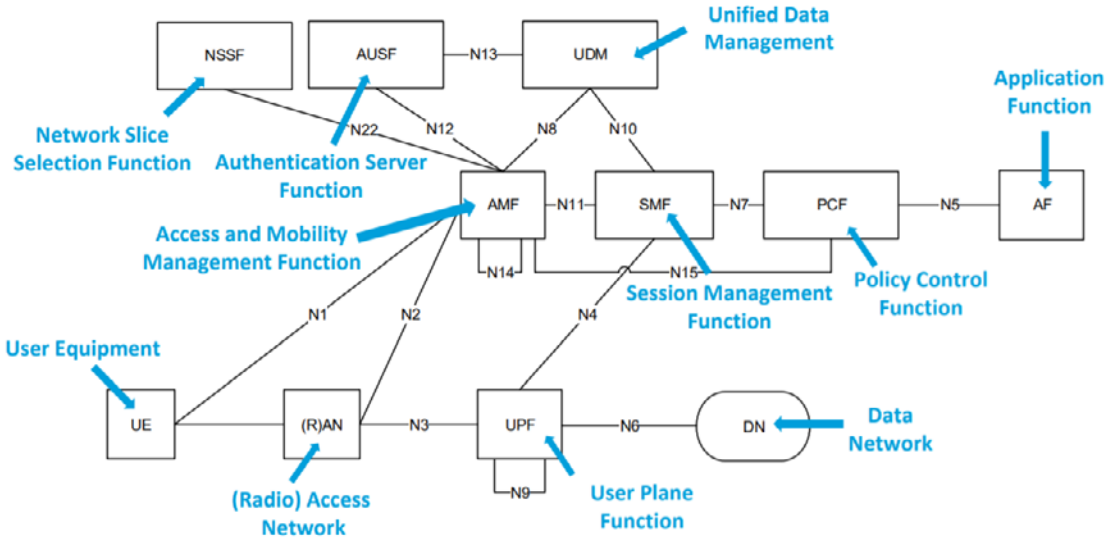


Figure 3: *Top-level block diagram of a 5G base station. Image courtesy of AT&T.*

The network then uses the PDU request to establish and provision a network slice across the RAN and core network (CN) that then connects the UE to a target network server or other edge computing resource. It should be noted that a single UE may use multiple network slices, each one dedicated to a specific application with its own priority, capacity, and QoS requirements. Figure 4 illustrates how the URSP and its associated protocols can be used to individually route and provision the network slice according to the capacity, priority, and QoS parameters agreed to between the UE and the PCF. In this case, the UE is running two different applications (PDU sessions) – one that works with a cloud-based application server (Route 1) and another that is supported by an edge data network (Route 2). Segmented routing also ensures that each network slice's latency is optimized for each application.

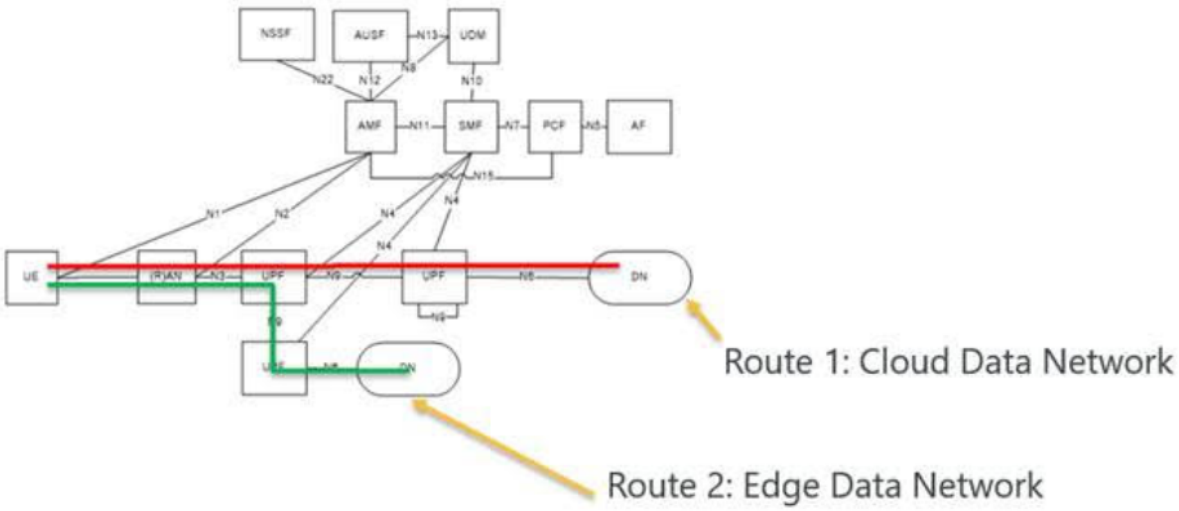


Figure 4: *The URSP mechanism allows each application within a UE device to have its own network slice that is optimally provisioned and routed to its requirements. Image courtesy of 3GPP.*

Potential Vulnerabilities and Attacks

Although 5G networks are potentially vulnerable to some type of attack at nearly every point within their system, many of the most significant threats involve the UE or RAN that connects the UE to the core network. As illustrated in Figure 5, vulnerabilities in these system elements may permit malicious interruptions such as signal jamming, distributed denial-of-service (DDoS) attacks, and spoofing. If attackers can use the UE to gain access to the protocol layer, malicious control signals can misdirect traffic, force disconnections, misprovision required functions, or shut down capabilities.

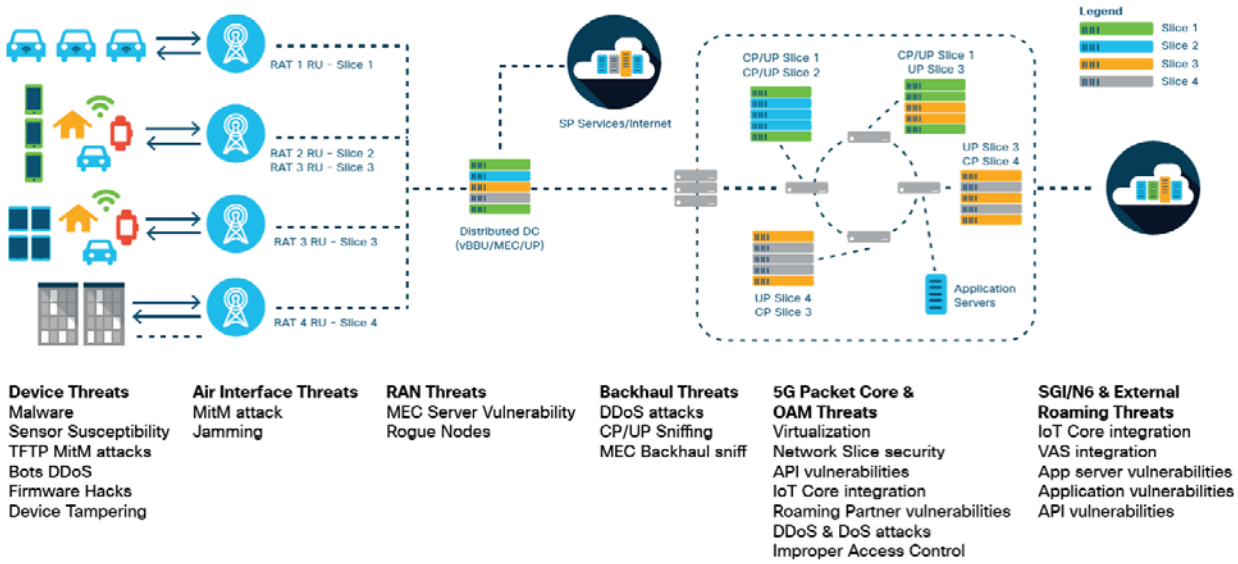


Figure 5: *5G vulnerabilities*

According to William Malik, VP of Infrastructure Strategies at Trend Micro, attacks that target UEs in 5G networks can be classified under four primary categories (Lee Goldberg (2019), "#InfosecNA: Security Risks of 5G, and How to Fix Them," Infosecurity Magazine, 26 Nov 2019, https://www.infosecurity-magazine.com/news/security-risks-5g-how-fix/):

1. **Mobile-to-Infrastructure:** One such scenario would involve a mobile botnet (i.e., a large number of infected UE devices controlled by an attacker's command and control (C&C) servers) that launch DDoS attacks on a 5G infrastructure with the goal of making that 5G network's functions and services unavailable

2. **Mobile-to-Internet:** A large mobile botnet can also be used to access a 5G network to launch a similar DDoS attacks on public websites.

3. **Mobile-to-Mobile:** A smaller number of infected devices can be used to launch attacks on other mobile customers with the aim of spreading malware (for example, viruses, worms, rootkits) or causing a localized DoS.

4. **Internet-to-Mobile:** In this attack, a malicious server on the Internet targets each UE with malware embedded inside applications, games, or video players from untrusted app stores. Once downloaded and installed, the malware enables the attacker to steal stored personal data on the device, further spread the malware to other devices, or control the device and use it to launch attacks on other devices and networks.

UEs can also play a role in attacks on a mobile network infrastructure. One of the common attacks used today, which may also potentially be used against 5G, is the rogue base station (RBS) threat. In this scenario, the RBS masquerades as a legitimate base station to facilitate a man-in-the-middle (MITM) attack between the mobile UE and the mobile network. An attacker can use the RBS to launch different attacks on mobile users and networks. These attacks include stealing user information, tampering with transmitted information, tracking users, compromising user privacy, or causing DoS for 5G services.

Although 5G networks will have security enhancements intended to protect them against RBS-based threats, attacks may still be possible using, for example, the following threat vectors:

- An attacker can exploit 5G/LTE interworking requirements to launch a downgrade attack.
- A compromised 5G small cell can create an RBS threat to 5G networks and customers.
- An attacker could exploit a lack of gNB authentication in an idle mode to force users to camp on an RBS that, as the number of “campers” grows, could create a DoS (i.e., public safety warnings, incoming emergency calls, real-time application server push services, etc.).

Security Testing Begins with Functional Verification

Security testing of a smartphone or other UE device is part of the overall functional verification process it undergoes during development. It can be broken down into two general classes of tasks:

1. Rigorous verification of the unit's ability to support the 5G standard's security mechanisms and protocols.

2. Testing the unit's ability to detect and properly respond to a wide range of incorrect inputs and other error conditions generated by the RAN, CN, and whatever computer or device it is communicating with. These tests are important because some types of attacks exploit software flaws that can cause a device to react incorrectly to unexpected inputs or other types of unforeseen conditions.

Both of these tasks require that the unit under test (UUT) undergoes an exhaustive series of exercises where each network condition and error parameter is run through its full range of possible values. Since running these tests on an actual 5G network would be extremely impractical, network simulators (such as the one shown in Figure 6) are used instead. In most of these tests, the simulator uses its wireless interface to communicate with the UUT as if it were an actual 5G RAN base station. When necessary, the simulator also provides an IP interface that emulates the characteristics of a CN user plane function (UPF) that can be connected to whatever application the test requires.

Testing Network Slicing Security

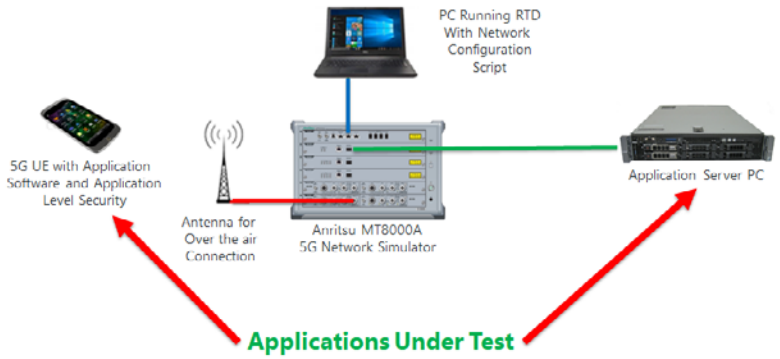


Figure 6: *A top-level view of simulator-based security testing*

Once configured, the network simulator can respond to the UE's requests to establish and use one or more network slices to support end-to-end tests that include the UE application layer. This configuration is usually done using scripting software that simplifies the creation and editing of test sequences. For example, an advanced scripting tool, such as Anritsu's Rapid Test Designer (RTD), allows developers to quickly create a configuration script that defines the available resources (bandwidth, priority, security, etc.), network conditions (impairments, latency/variation, error rates, etc.), and other network properties for each network slice used in the test.

A scripting tool can be used to configure the simulator and generate the data traffic needed to verify the functionality of the UE's implementations of various parts of the 5G protocol – such as URSP mapping, URSP selection, and NSSAI selection – under the widest possible range of operating conditions. In the example shown in Figure 7, the message editor of Anritsu's RTD scripting tool is being shown from a test sequence for verifying the functionality of the UE's ability to support the creation of a valid NSSAI and acknowledge an allowed/rejected message that occurs during the creation of a network slice.

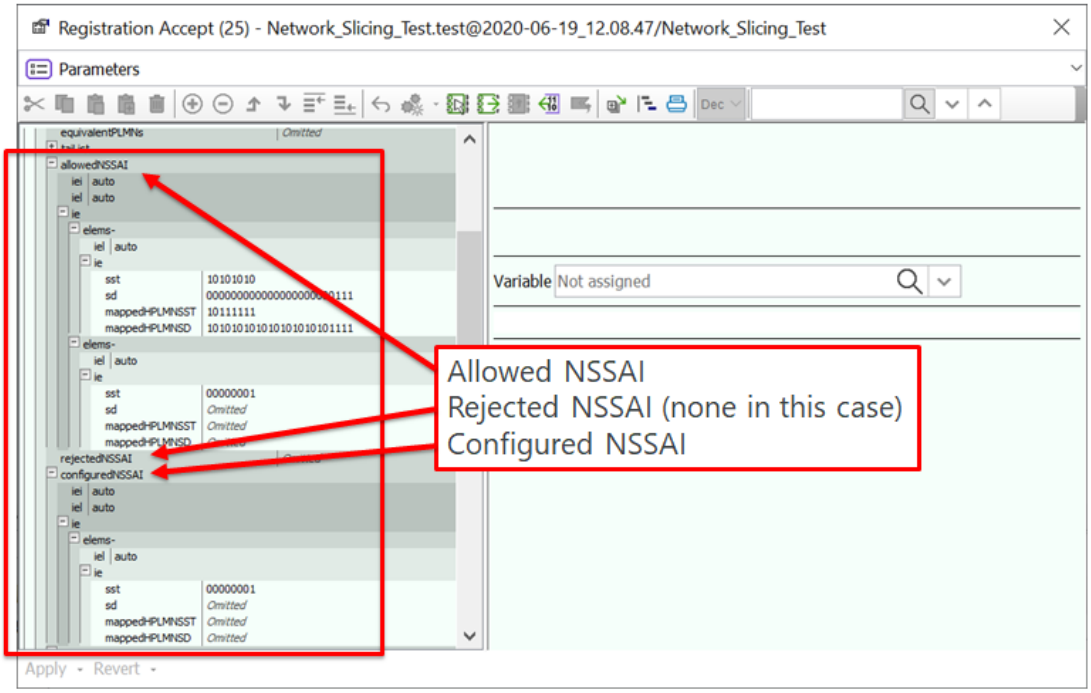


Figure 7: *This part of a network slicing test script exercises the NSSAI exchange through the full range of allowable and non-allowable parameter and timing values.*

Scripts are also invaluable for verifying the functionality and security of applications that reside locally on the UE or remote applications that reside in the cloud or on servers. Figure 8 illustrates how these scripts are used to configure the simulator for end-to-end application testing. In this case, the simulated control plane, user plane, and each RAN link negotiated between the UE and the simulator are programmed to present a specific set of network resources to the UE then exhibit the desired behavior needed to simulate a series of normal and abnormal network conditions. In addition, each network slice created during the test is mapped to a specific configuration defined within the RTD script. In order to facilitate efficient, thorough testing, the simulator can record a full set of signaling traces and log files that occur during each test and provide a detailed analysis of NAS messages for URSP checking.

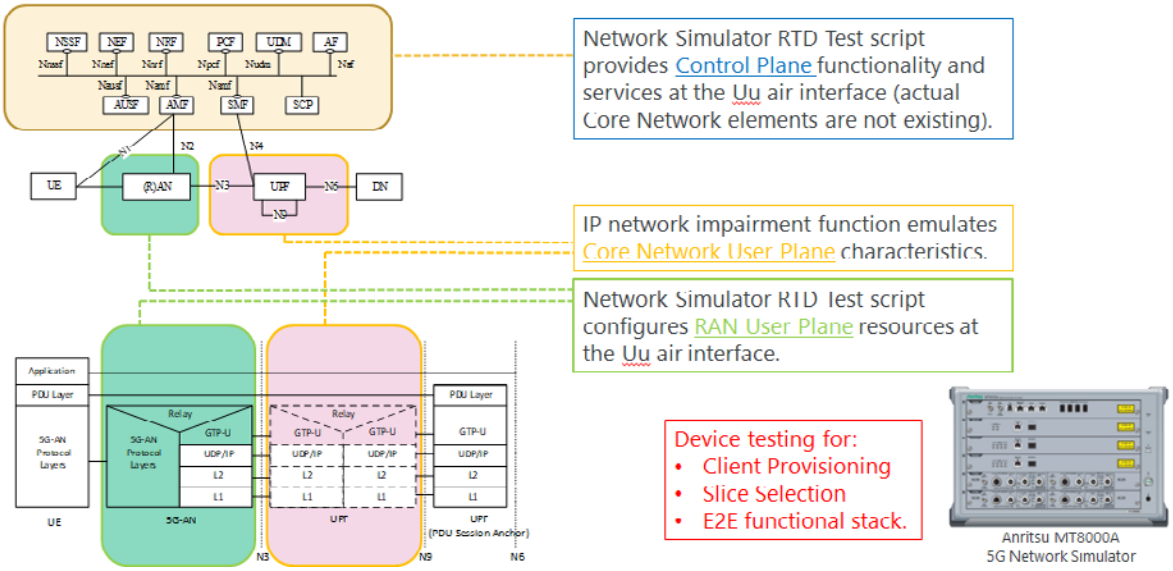


Figure 8: *A network simulator can be configured as an end-to-end functional stack for application testing (in this case, an Anritsu Radio Communication Test Station MT8000A 5G network simulator).*

If properly implemented, the functional tests described here can also make up a significant portion of the security tests needed to identify any potential vulnerabilities in the UE design and the applications they support. This is because a surprising number of frequently used attack strategies exploit flaws in a device's response to corner cases, data errors, signaling errors, and other fault conditions. If a device has been rigorously exercised under most, if not all, of these conditions during functional verification, your security tests can focus on the other classes of attacks, such as gaining access to the UE either through a malware-laden application or spoofing (e.g., MITM attack).

Network simulators can also be used to perform end-to-end network slicing security tests that focus on the application-level security of the UE and the application server. This involves exercising all the relevant NAS protocols and security mechanisms, such as those used to authenticate the user for the application. Once configured, a simulator suite, such as the Anritsu MT8000A/RTD solution, provides the pipe with flexible configuration of network slices and routing according to the URSP.

Conclusion

Since 5G networks have become an integral part of the global digital economy, their infrastructure equipment and the mobile devices that use them must be robust, reliable, and highly resistant to cyberattack. Producing secure products begins with rigorous functional testing and verification for compliance with 5G network standards, as well as ensuring an emphasis on the complex protocols and security mechanisms used to negotiate, establish, and maintain network slices between a UE device and the CN.

These tasks can be efficiently executed using network simulators coupled with scripting tools that can configure them to produce the desired network and associated resources (as well as any impairments, out-of-range parameters, and error conditions a device is expected to encounter). Ensuring the device reacts in a predictable manner to both normal and abnormal network procedures can close the door on a large number of potential cybersecurity exploits used to gain access to the UE and network itself. The simulator can also serve as a highly effective test bed for simulating other, more aggressive types of cyberattacks.

Anritsu's Radio Communication Test Station MT8000A provides all-in-one support for the development of 5G communication terminals, chipsets, and devices. With a 5G base station emulation function, a single MT8000A test platform supports both FR1 (to 7.125 GHz) and FR2 (millimeter-wave) bands as well as existing LTE for simulating 5G non-standalone (NSA) with LTE – maximizing your test environment to ensure the security of network slices as well as other RF, protocol, and use-case tests. With its modular architecture and robust software offering, the MT8000A provides the flexibility and expandability needed to future-proof your test environment. For more information, please visit anritsu.com.

List of Acronyms

AUSF	Authentication Server Function
CN	Core Network
DDoS	Distributed Denial-of-Service
eMBB	Enhanced Mobile Broadband
IoT	Internet-of-Things
M2M	Machine-to-Machine
MIoT	Massive Internet-of-Things
MITM	Man-in-the-Middle
NAS	Non-Access Stratum
NSSAI	Network Slice Selection Assistance Information
PCF	Policy Control Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
QoS	Quality of Service
RAN	Radio Access Network
RBS	Rogue Base Station
S-NSSAI	Single Network Slice Selection Assistance Information
SD	Slice Differentiator
SST	Slice/Service Type
UE	User Equipment
UPF	User Plan Function
URLLC	Ultra-Reliable Low Latency Communication
URSP	User Equipment Route Selection Policy
UUT	Unit Under Test
V2X	Vehicle-to-Everything

Anritsu envision : ensure

Specifications are subject to change without notice.

• United States
Anritsu Company
450 Century Pkwy, Suite 109,
Allen, TX, 75013 U.S.A.
Toll Free: 1-800-267-4878
Phone: +1-972-644-1777
Fax: +1-972-671-1877

• Canada
Anritsu Electronics Ltd.
700 Silver Seven Road, Suite 120,
Kanata, Ontario K2V 1C3, Canada
Phone: +1-613-591-2003
Fax: +1-613-591-1006

• Brazil
Anritsu Electrônica Ltda.
Praça Amadeu Amaral, 27 - 1 Andar
01327-010 - Bela Vista - Sao Paulo - SP - Brazil
Phone: +55-11-3283-2511
Fax: +55-11-3288-6940

• Mexico
Anritsu Company, S.A. de C.V.
Av. Ejército Nacional No. 579 Piso 9, Col. Granada
11520 México, D.F., México
Phone: +52-55-1101-2370
Fax: +52-55-5254-3147

• United Kingdom
Anritsu EMEA Ltd.
200 Capability Green, Luton, Bedfordshire LU1 3LU, U.K.
Phone: +44-1582-433280
Fax: +44-1582-731303

• France
Anritsu S.A.
12 avenue du Québec, Batiment Iris 1-Silic 612,
91140 Villebon-sur-Yvette, France
Phone: +33-1-60-92-15-50
Fax: +33-1-64-46-10-65

• Germany
Anritsu GmbH
Nemetschek Haus, Konrad-Zuse-Platz 1
81829 München, Germany
Phone: +49-89-442308-0
Fax: +49-89-442308-55

• Italy
Anritsu S.r.l.
Via Elio Vittorini 129, 00144 Roma Italy
Phone: +39-06-509-9711
Fax: +39-06-502-2425

• Sweden
Anritsu AB
Kistagången 20B, 164 40 KISTA, Sweden
Phone: +46-8-534-707-00
Fax: +46-8-534-707-30

• Finland
Anritsu AB
Teknobulevardi 3-5, FI-01530 VANTAA, Finland
Phone: +358-20-741-8100
Fax: +358-20-741-8111

• Denmark
Anritsu A/S
Kay Fiskers Plads 9, 2300 Copenhagen S, Denmark
Phone: +45-7211-2200
Fax: +45-7211-2210

• Russia
Anritsu EMEA Ltd.
Representation Office in Russia
Tverskaya str. 16/2, bld. 1, 7th floor.
Moscow, 125009, Russia
Phone: +7-495-363-1694
Fax: +7-495-935-8962

• Spain
Anritsu EMEA Ltd.
Representation Office in Spain
Edificio Cuzco IV, Po. de la Castellana, 141, Pta. 5
28046, Madrid, Spain
Phone: +34-915-726-761
Fax: +34-915-726-621

• United Arab Emirates
Anritsu EMEA Ltd.
Dubai Liaison Office
P O Box 500413 - Dubai Internet City
Al Thuraya Building, Tower 1, Suite 701, 7th floor
Dubai, United Arab Emirates
Phone: +971-4-3670352
Fax: +971-4-3688460

• India
Anritsu India Pvt Ltd.
2nd & 3rd Floor, #837/1, Binnamangla 1st Stage,
Indiranagar, 100ft Road, Bangalore - 560038, India
Phone: +91-80-4058-1300
Fax: +91-80-4058-1301

• Singapore
Anritsu Pte. Ltd.
11 Chang Charn Road, #04-01, Shriro House
Singapore 159640
Phone: +65-6282-2400
Fax: +65-6282-2533

• P. R. China (Shanghai)
Anritsu (China) Co., Ltd.
27th Floor, Tower A,
New Caohejing International Business Center
No. 391 Gui Ping Road Shanghai, Xu Hui Di District,
Shanghai 200233, P.R. China
Phone: +86-21-6237-0898
Fax: +86-21-6237-0899

• P. R. China (Hong Kong)
Anritsu Company Ltd.
Unit 1006-7, 10/F., Greenfield Tower, Concordia Plaza,
No. 1 Science Museum Road, Tsim Sha Tsui East,
Kowloon, Hong Kong, P. R. China
Phone: +852-2301-4980
Fax: +852-2301-3545

• Japan
Anritsu Corporation
8-5, Tamura-cho, Atsugi-shi,
Kanagawa, 243-0016 Japan
Phone: +81-46-296-6509
Fax: +81-46-225-8359

• Korea
Anritsu Corporation, Ltd.
5FL, 235 Pangyoyeok-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, 13494 Korea
Phone: +82-31-696-7750
Fax: +82-31-696-7751

• Australia
Anritsu Pty Ltd.
Unit 20, 21-35 Ricketts Road,
Mount Waverley, Victoria 3149, Australia
Phone: +61-3-9558-8177
Fax: +61-3-9558-8255

• Taiwan
Anritsu Company Inc.
7F, No. 316, Sec. 1, Neihu Rd., Taipei 114, Taiwan
Phone: +886-2-8751-1816
Fax: +886-2-8751-1817

2021-02 A Bottom-Up Approach to 5G Network Slicing Security in User Equipment