

Securing 5G: CSRIC VII 5G Standalone Network Test Report *Q4 2023*

Table of Contents

Introduction	
Scope of Report	5
Background	5
Why CSRIC VII	5
CSRIC VII Working Group 3's Report and Recommendations for 5G Standalone Architecture	6
Definition of CSRIC Test Cases	7
Test Results	9
Introduction	9
IPsec Configuration	11
SIM Card Profiles	12
Test Case 1: CSRIC 7 WG 3 – NAS Signaling Confidentiality	12
Part 2: Using NEA2 Encryption	21
Test Case 2: CSRIC 7 WG 3 – RRC Signaling Confidentiality	24
Test Case 3: CSRIC 7 WG 3 – Access Stratum User Plane Confidentiality	31
Test Case 4: CSRIC 7 WG 3 – Access Stratum User Plane Integrity	33
Test Case 5: CSRIC 7 WG 3 – SUPI/SUCI Privacy Enabled	36
Test Case 6: CSRIC 7 WG 3 – IPsec on Transport Links	39
Test Case 7: CSRIC 7 WG 3 – Transport Layer Security for SBA Interfaces	47
Conclusions and Next Steps	60
Appendix: Acronyms	63

Introduction

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

The wireless industry prioritizes stronger security and reliability with every generation of its mobile networks. With 5G in particular, secure connectivity is the foundation that supports and enhances the many benefits these networks provide. The wireless industry devotes significant resources to 5G security and has expanded its efforts through 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. Its members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, SecureG, and Intel; and academic partners the University of Maryland and Virgina Tech Advanced Research Corporation (VT-ARC).

The 5G Security Test Bed has a Technical Advisory Committee (TAC) made up of its members and the Test Bed Administrator. The TAC advises the Test Bed Administrator on the day-to-day technical and operational activities and decisions related to the Test Bed, including but not limited to: development of use cases to be tested, test plan development and review, raw test data analysis, test result and report generation, and development of recommendations to standards bodies based on results.

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.

The 5G Security Test Bed Uses Real-World Equipment, Validating Real-World Applications

One of the 5G Security Test Bed's core values lies in its ability to validate 5G security use cases in a real-world environment, using an actual 5G network architecture. Leveraging a significant investment and in-kind contributions, the Test Bed's founding members built this state-of-the-art, private 5G network from scratch for the singular purpose of evaluating 5G network security.

The 5G Security Test Bed's previous testing activities have worked to validate the recommendations of the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) advisory group, for both non-standalone and standalone network configurations. In addition, the Test Bed draws on recommendations from its own Technical Advisory Committee to address emerging vulnerability research. The first report in this series focused on the validation of the CSRIC non-standalone configurations, while this report addresses the CSRIC standalone configuration recommendations and network slicing. The 5G Security Test Bed will continue evaluating additional recommendations and use cases from CSRIC and other entities in future tests. It is not set up to be a platform for identifying vulnerabilities or conducting penetration testing of networks or equipment.

Real-World Testing

The 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

Real-World Applications

The 5G Security Test Bed's tests and outcomes support several applications that can drive new technology and transform cities, government, and industries. Use cases include government and enterprise applications, general network security protections, and smart city applications such as:

- Primary Use Cases: Network Security
 - o Protecting Information in Transit
 - o Roaming Security
 - o Subscriber Privacy
 - o Zero Trust Network Security
 - o False Base Station Detection and Protection
 - o 5G Cloud Network Security

• Secondary Use Cases: Devices and Applications

- o High-Resolution Video Surveillance (e.g. Smart Cities, Large Venues)
- o LTE/5G Drones with High-Resolution Video Feedback (e.g. Smart Cities)
- o Dynamic Supply Chain Verification (Real-Time Monitoring and Logistics)
- o Automated, Reconfigurable Factories
- o Autonomous Vehicles
- o Immersive AR/VR

The 5G standalone network architecture tested for this report makes up key components of these applications because they enable service to be customized to diverse needs and requirements. The test cases outlined here show how these new and evolving uses can successfully adopt enhanced security capabilities while improving performance and capability.

Scope of Report

This report addresses recommendations derived from the FCC's Communications Security, Reliability, and Interoperability Council VII March 2021 report, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security.*¹ The report focused on the implementation of security protections in 5G "standalone" (SA) networks (that is, networks designed and built specifically for 5G) by assessing security features from 3GPP TS 33.501, the primary technical standard for 5G SA. (By contrast, non-standalone networks offer 5G service together with 4G LTE over shared infrastructure.) The first report from the 5G Security Test Bed focused on NSA networks supporting both 5G and 4G traffic.

This 5G STB report's scope is to evaluate and verify CSRIC VII's recommendations for SA architecture by investigating the security features associated with 5G network infrastructure and the devices that can access a 5G SA network.

Background

Why CSRIC VII

The Communications Security, Reliability, and Interoperability Council is a federal advisory committee that provides the Federal Communications Commission with recommendations to enhance the security, reliability, and interoperability of communications systems. CSRIC provides a forum for industry and government technical experts to assess developing technology and analyze complex issues. It is a leading venue for stakeholders in and outside of government to share ideas and best practices, and to help the FCC stay abreast of cutting-edge technology

¹ CSRIC VII WG3, Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (Mar. 2021), <u>https://www.fcc.gov/file/20606/download</u>.

and security issues affecting the communications sector. CSRIC's work continues to influence government and industry agendas and activities.

The FCC charters CSRIC every two years. CSRIC VII's charter was from March 2019 to March 2021, and it focused on a range of public safety and homeland security-related communications matters, including issues related to 5G network evolution. 5G offers significant and novel capabilities compared with previous generations of wireless networks, but new capabilities, infrastructure, and equipment can also introduce security risks. The FCC tasked CSRIC VII with examining these security risks and making recommendations associated with the evolving standards' optional security features. Because 5G standards and specifications continue to develop, CSRIC VII's work offered an opportunity to update future standards.

Likewise, the 5G Security Test Bed's work in testing CSRIC's recommendations can be used both to inform network architecture and operation, and to enhance future 5G standards.

CSRIC VII Working Group 3's Report and Recommendations for 5G Standalone Architecture

CSRIC VII's Recommendations

CSRIC VII worked to identify and evaluate optional features in the 3GPP standards that would potentially cause security gaps in 5G if not implemented. In March 2021, CSRIC's Working Group 3 (WG3, "Managing Security Risk in Emerging 5G Implementations") released a report, *Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security.*² The report focused on identifying optional features in proposed 3GPP standards that might diminish the effectiveness of 5G security, and made recommendations to address these gaps.

Several security features outlined in 3GPP TS 33.501 releases 15 and 16 were mandatory for equipment vendors to implement, but optional for 5G network operators to deploy. CSRIC VII WG3 looked at the optional security features and conducted a risk assessment and analysis on those measures, including: confidentiality for Non-Access Stratum (NAS) signaling,³ user plane confidentiality and integrity, radio resource control signaling confidentiality, Subscription Permanent Identifier (SUPI)/International Mobile Subscriber Identity (IMSI) privacy, and network security, including IP security (IPsec) and transport layer security (TLS).

² Id.

³ "NAS signaling" carries the user data from the user equipment to the MME through the S1 pathway.

Based on its assessment, CSRIC VII WG3 made eight recommendations:

- **Previous CSRIC Recommendations:** Communications sector members and stakeholders should adopt CSRIC-recommended 5G SA threat mitigations from previous CSRIC VI, V, and IV reports.⁴
- NAS Signaling Confidentiality: Operators should convey only non-user identity related information until security context is established. (CSRIC noted that 3GPP TS 33.501 encrypts all NAS messages after security context is established.)
- User Plane Confidentiality: Operators should apply user plane (UP) confidentiality protections at the Packet Data Convergence Protocol (PDCP) layer.
- User Plane Integrity: OEM and network infrastructure vendors should support, and operators should implement, the 3GPP TS 33.501 Release 16 and 128-NIA3 capabilities of supporting integrity protection and user data replay protection at the full data rate available to the user equipment. (Release 15 required only 64kbps.)
- **RRC Signaling Confidentiality:** Operators should protect RRC-signaling (Radio Resource Control) confidentiality and convey only non-identity related information prior to establishing security context.
- **SUPI/IMSI Privacy:** Devices and networks in the U.S. should use IMSI privacy, and permit the null encryption only for making emergency services calls (i.e. 9-1-1).
- Network Security—IPsec: Operators should apply IPsec or a tunneling technology such as VPN tunnels for transport.
- Core Network Security—Transport Layer Security (TLS): Operators should apply TLS for Service-Based Architecture (SBA) interfaces.

Definition of CSRIC Test Cases

Based on the CSRIC VII WG3 recommendations, the 5G STB established and executed seven test cases described in this report, as follows:

1. NAS Signaling Confidentiality:

a. <u>CSRIC VII WG3 Recommendation</u>: Operators should convey only non-user identity related information until security context is established.

⁴ See CSRIC VI WG3, Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks (Sept. 2018), <u>https://www.fcc.gov/file/14500/download;</u> CSRIC V WG6, Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network (making recommendations for security-by-design principles in the core communications network) (March 2016), <u>https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_FINAL_%20wAppendix_0316.pdf</u>; and CSRIC IV WG4, Wireless Segment Cybersecurity Risk Management and Best Practices (March 2015), <u>https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf</u>.

b. <u>5G STB Test Case 1:</u> Demonstrate how user identity related information can be transmitted confidentially by testing the implementation of NAS Signaling encryption. Once an encrypted channel is established, only non-user identity related information should be observable.

2. RRC Signaling Confidentiality:

- a. <u>CSRIC VII WG3 Recommendation:</u> Operators should protect RRC-signaling confidentiality and convey only non-identity related information prior to establishing security context.
- b. <u>5G STB Test Case 2:</u> Demonstrate that the PDCP provides RRC signaling confidentiality between the user equipment and NG-RAN (Next Generation Radio Access Network) using 128-bit NEA algorithms.

3. Access Stratum User Plane (Payload Data) Confidentiality:

- a. <u>CSRIC VII WG3 Recommendation:</u> Operators should apply user plane confidentiality protections at the PDCP layer.
- b. <u>5G STB Test Case 3:</u> To demonstrate that the PDCP provides user plane data confidentiality between the user equipment and NG-RAN using 128-bit NEA algorithms.

4. Access Stratum User Plane (Payload Data) Integrity:

- a. <u>CSRIC VII WG3 Recommendation</u>: Operators should apply user plane confidentiality protections at the PDCP layer.
- b. <u>5G STB Test Case 4-1</u>: Demonstrate that the PDCP provides user plane data integrity protection at the full rate.

5. SUPI/IMSI User Privacy:

- a. <u>CSRIC VII WG3 Recommendation</u>: Devices and networks in the U.S. should use IMSI privacy.
- b. <u>5G STB Test Case 5-1</u>: Register a device on the test network by exchanging identity information using the subscription concealed identifier (SUCI) to encrypt the SUPI.

6. Network Security:

- a. <u>CSRIC VII WG3 Recommendation:</u> Apply IPsec or tunneling technology to protect network security during transport.
- b. <u>5G STB Test Case 6:</u> Use IPsec to transmit user plane and control plane (CP) messaging while protecting confidentiality, integrity, and replay.

- 7. Core Network Security (Transport Link Encryption):
 - a. <u>CSRIC VII WG3 Recommendation</u>: Use TLS for SBA interfaces and tunneling technology for transport when not using the SBA.
 - b. <u>5G STB Test Case 7:</u> Demonstrate TLS encryption to protect SBA interfaces in the 5G core.

Test Results

Introduction

This document presents test results based on use cases derived from the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) VII Working Group 3 (WG3) Report 2 recommendations for securing 5G standalone networks based upon its analysis of optional security requirements in 3GPP TS 33.501.

The configuration used for these tests comprises radio access network (RAN) equipment hosted at the University of Maryland (UMD) and a dual-mode core (DMC), that provides both 4G LTE and 5G functionality hosted at the MITRE Corporation. The core is the Ericsson DMC, PCC version 1.19. The connection between the RAN at UMD and the DMC at MITRE goes over the internet and, for the scenarios considered here, is treated as an untrusted link.⁵ **Error! Reference source not found.** shows the relevant components of the Test Bed, including available test points. Not all of the test points shown in the diagram were used for these tests.

The routers shown at each location are Ericsson 6672 routers (referred to as R6672, or R6K). The switches shown are each Pluribus Freedom 9372-X switches. For the tests implemented here, the two switches are considered part of the "untrusted" backhaul link. The core is configured to support two network slices. The first slice, referred to as Slice 1 in this report, is considered the default enhanced mobile broadband (eMBB) network slice. The second slice, Slice 2, emulates a private network and includes the ability to form an IPsec tunnel to create a highly secure slice. The IPsec tunnel is configured with one endpoint at the baseband unit (BBU) and the other at the core-side R6672 router. On the server on the core side, there are two virtual web servers instantiated, one for each slice, and isolated from each other. All tests for the test cases discussed in this report were executed on Slice 2.

⁵ In the actual implementation, there are additional security measures implemented, including an IPsec tunnel between the UMD and MITRE campus/corporate networks. For the purposes of these tests, this tunnel is considered part of the untrusted link and therefore, any encryption implemented for the tests is in addition to these measures.

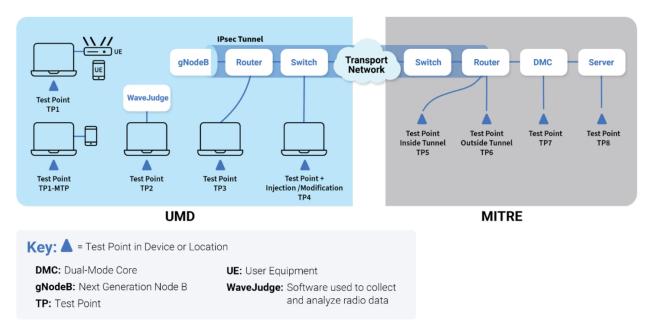


Figure 1: 5G STB Lab Component Block Diagram and Test Points

Tests were run with band N41 for the new radio (NR) using a Sierra Wireless EM9190 card connected to a laptop by USB as a cellular modem, as well as a Qualcomm Mobile Test Platform (MTP) device. For the purposes here, we will refer to the combination of that laptop and the cellular modem as the UE.

Packets are captured on each of the identified test points in Figure 1: at the UE(s) (TP1), on the RAN-side Pluribus switch (TP4), on the Core-side R6K router (TP6), and at the DMC (TP7). These test points are identified with numbers as shown in the figure and described in more detail in Table 1.

Table 1: Test Point Descriptions

Test Point	Description and Use					
TP1-S	Laptop connected to Sierra Wireless card and/or software-defined radio (SDR); Wireshark captures packets originating at and destined to UE laptop; other tools access SDR controls and data					
TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data					
TP2	WaveJudge interface					
TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)					
TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"					
TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"					
TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC					
TP7	CNOM tool accessing DMC messages and command line interface on core					
TP8	Applications running on application server in MITRE facility					

IPsec Configuration

3GPP TS 33.401 requires IPsec, when used, to support ESP and IKEv2 with certificates-based authentication. The security gateway (SEG) is optional to use. The following requirements are from 33.401, section 12, Backhaul link user plane protection:

In order to protect the S1 and X2 user plane as required by clause 5.3.4, it is required to implement **IPsec ESP** according to RFC 4303 [7] as profiled by TS 33.210 [5], with confidentiality, integrity and replay protection.

Tunnel mode IPsec is mandatory to implement on the eNB for X2-U and S1-U. On the X2-U and S1-U, transport mode IPsec is optional for implementation. NOTE 1: Transport mode can be used for reducing the protocol overhead added by IPsec. On the core network side a **SEG may be used** to terminate the IPsec tunnel.

For both S1 and X2 user plane, **IKEv2 with certificates based authentication shall be implemented**. The certificates shall be implemented according to the profile described by TS 33.310 [6]. IKEv2 shall be implemented conforming to the IKEv2 profile described in TS 33.310 [6].

3GPP TS 33.501 retains these IPsec requirements for 5G SA and NSA, when IPsec is used.

CSRIC 7 WG 2 Report 2 recommends IPsec on untrusted links to provide confidentiality and integrity protection over the S1-MME, S1-U, and management interfaces.

IPsec is implemented on Slice 2, with tunnel endpoints at the RAN and at the core-side R6K.

SIM Card Profiles

Some tests require different SIM card profiles to tests the desired functionality. Table 2 lists the different profiles that were used during each test.

Table 2: SIM Card Profiles

ID	IMSI	Profile
Ν	310 014 791 791 001	N (NULL)
А	310 014 791 791 011	А
В	310 014 791 791 021	В

Test Case 1: CSRIC 7 WG 3 – NAS Signaling Confidentiality

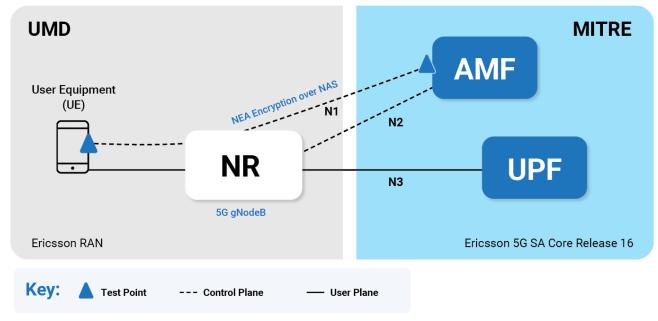


Figure 2: Test Case SA-01 Configuration

Test Case ID: TC-SA-01

Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the NAS signaling confidentiality, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends only non-user identity related information shall be conveyed prior to security context being established. Note, after security context is established, all NAS messages are encrypted according to 3GPP TS 33.501.

This test involves implementation of NAS signaling encryption on the N1 interface. Once encrypted channels are established, user identity info may be securely exchanged.

Used	Test Point	Description and Use					
Х	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop					
TP1-MTP		Laptop connected to Qualcomm MTP; QXDM allows access to low-level data					
	TP2	WaveJudge interface					
TP3 (Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)					
TP4 TP5		tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"					
		tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"					
х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC					
	TP7	CNOM tool accessing DMC messages					
	TP8	Applications running on application server in MITRE facility					

Test points used:

		SIM			
Slice	IP pool	LABEL	SIM LABEL IMSI	DNN	DN SERVERS
				dnn-embb-	
Slice 2	172.24.1.0/24	N21	3100147917910021	stb2.mitre.net	192.168.59.146/28

Network Slice 2 and a UE with Profile B SIM were used throughout the tests. The UE used for Slice 2 was a Sierra Wireless Modem, which is connected and controlled by a laptop outside the Faraday Cage. IPsec for for Slice 2 and control traffic was turned on/off as and when required.

To ensure that the core did not retain the UE state, we deleted the UE context from the core (Figure 3), and ensured that the IPsec tunnel for the transport channel between the RAN and core was up (Figure 4).

```
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh delete_subscriber -imsi 310014791791021
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh delete_subscriber -imsi 310014791791001
Subscriber identity: "310014791791001" is not registered.
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
```

Figure 3: Deleting UE Context from Core

MUMD02	MUMD02AVW> st ipsec								
221118	8-16:31:13 169	9.254.2.2 22.0h	MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317						
====== Ргоху	Adm State	Op. State	MO						
====== 14282		1 (ENABLED)	Transport=1,Router=NRCUCP,IpsecTunnel=1						
====== Total:	1 MOs								

Figure 4: IPsec enabled between BBU and Core-side R6K router

This test has two parts; 1) with NEA0 (no encryption) and 2) with NEA2 activated to encrypt NAS signaling. For Part 1, on the core side, we used a command line interface command to set priority for the NAS encryption algorithm making NEA0 (null algorithm) the highest priority (specifically, priority 1). See Figure 5 for the initial NEA settings, Figure 6 for the commands changing the priority settings, and

```
=== mtramcamiar erv@errc-bc-mm-controtter-a andr ~ # dsu der_uea_ardorrtum -uame ueaa
                   Active Data Planned Data
Parameter
                         20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 1
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea algorithm -name nea1
                   Active Data Planned Data
Parameter
        . . . . . . . . . .
                         20221109120424
timestamp
planState
prio (N1SecurityAlgorithmPriority) 2
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea2
                    Active Data Planned Data
Parameter
20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 3
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea3
Parameter
                   Active Data Planned Data
timestamp
                         20220727201309
planState
orio (N1SecuritvAlgorithmPrioritv) 0
```

Figure 7 displaying the encryption setting to NULL (NEA0). For the second part, we set encryption back to NEA2 with the highest priority.

Test Results for 5G STB – CSRIC-Inspired SA Use Cases

=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea0 Parameter Active Data Planned Data 20221118100928 timestamp planState prio (N1SecurityAlgorithmPriority) 1 === mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea1 Active Data Planned Data Parameter -----20221109120424 __ timestamp planState prio (N1SecurityAlgorithmPriority) 2 === mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea2 Active Data Planned Data Parameter timestamp 20221118100928 planState prio (N1SecurityAlgorithmPriority) 3 === mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea3 Active Data Planned Data Parameter -----20220727201309 timestamp planState prio (N1SecurityAlgorithmPriority) 0

Figure 5: Confidentially Core Setting - NEA2 (128-NEA2 cipher algorithm) before configuration change

```
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh modify nea_algorithm -name nea2 -prio 1
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh modify_nea_algorithm -name nea0 -prio 3
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea0
                         Active Data Planned Data
arameter
_____
imestamp
                 20221118100928 20221118161841
                               Modified
lanState
rio (N1SecurityAlgorithmPriority) 1
                                       3
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea1
arameter
                          Active Data Planned Data
.....
                           20221109120424
imestamp
lanState
rio (N1SecurityAlgorithmPriority) 2
== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea2
                        Active Data Planned Data
arameter
imestamn
                   20221118100928 20221118161826
```

Figure 6: Confidentially cipher algorithm setting changes

```
== mildmcamial elaGelic-bc-ww-contlorel-a ANCR ~ # deu dei ardolitum -uame usaa
Parameter
                  Active Data Planned Data
20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 1
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea1
Parameter
                     Active Data Planned Data
timestamp
                         20221109120424
planState
prio (N1SecurityAlgorithmPriority) 2
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea2
                    Active Data Planned Data
Parameter
20221118164429
timestamp
planState
prio (N1SecurityAlgorithmPriority) 3
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name nea3
Parameter
                   Active Data Planned Data
20220727201309
timestamp
planState
orio (N1SecuritvAlgorithmPrioritv) 0
```

Figure 7: Confidentially Core Setting changes – NEA0 (no encryption) now has the highest priority (priority 1)

```
- Incrumedantor cryecite permit concruter o Aned - # Ash Acruea ardorrenin - Hame Head
                       Active Data Planned Data
Parameter
20221118171329
timestamp
planState
prio (NlSecurityAlgorithmPriority) 3
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea_algorithm -name neal
                  Active Data Planned Data
Parameter
timestamp
                20221109120424
planState
prio (N1SecurityAlgorithmPriority) 2
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get nea algorithm -name nea2
Parameter
                 Active Data Planned Data
timestamp
                       20221118171329
planState
prio (N1SecurityAlgorithmPriority) 1
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ # gsh get_nea algorithm -name nea3
Parameter
                  Active Data Planned Data
timestamp
                20220727201309
planState
prio (NlSecurityAlgorithmPriority) 0
=== mtrdmcamf01 erv@eric-pc-mm-controller-0 ANCB ~ #
```

Figure 8: Confidentially Core Setting changes – NEA2 (no encryption) now has the highest priority (priority 1)

Part 1: Using NEA0 Encryption

Upon starting the UE, it sends an initial message with a registration request. Figure 9 shows the Wireshark interpretation of the captured message from the UE indicating that for the 5G mobile identity, the type of identity is SUCI, the concealed identifier. Subsequently, the AMF requests

authentication (Figure 10) and the UE responds (Figure 11). After authentication, the core indicates the ciphering algorithm to be used, in this case NEA0, as shown in Figure 12. Subsequent transmissions are processed with the NEA0 (NULL) algorithm, resulting in decipherable messages, as shown in Figure 13 and Figure 14, in which details of the messages are visible such as the UE's IMEISV.

Tme 101 2022-11-18 16:48:49.834484 103 2022-11-18 16:48:49.88807 105 2022-11-18 16:48:50.651307 106 2022-11-18 16:48:50.674457 107 2022-11-18 16:48:50.691301 108 2022-11-18 16:48:50.091301	10.220.67.1910.10.205.67.20410.	220.67.19		Langth Info 182 InitialUEMessage, Registration request							
101 2022-11-18 16:48:49.834484 103 2022-11-18 16:48:49.888077 105 2022-11-18 16:48:50.051307 106 2022-11-18 16:48:50.074457 107 2022-11-18 16:48:50.085769	10.220.67.19 10. 10.205.67.204 10. 10.220.67.19 10. 10.205.67.204 10.	205.67.204	NGAP/NAS-5GS								
103 2022-11-18 16:48:49.888077 105 2022-11-18 16:48:50.051307 106 2022-11-18 16:48:50.074457 107 2022-11-18 16:48:50.085769	10.205.67.204 10. 10.220.67.19 10. 10.205.67.204 10.	220.67.19		182 InitialUEMessage, Registration request							
105 2022-11-18 16:48:50.051307 106 2022-11-18 16:48:50.074457 107 2022-11-18 16:48:50.085769	10.220.67.1910.10.205.67.20410.		MGAD /MAS-SGS								
106 2022-11-18 16:48:50.074457 107 2022-11-18 16:48:50.085769	10.205.67.204 10.	205.67.204									
107 2022-11-18 16:48:50.085769				142 UplinkNASTransport, Authentication response							
	10.220.67.19 10.		NGAP/NAS-5GS	134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command							
108 2022-11-18 16:48:50.091301				258 SACK (Ack=1, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration reque							
	10.205.67.204 10.	220.67.19	NGAP/NAS-5GS	142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command							
criticali	ty: reject (0)										
⊻ value											
RAN-U	E-NGAP-ID: 16790000										
✓ Item 1: id-NAS-P	UU										
ProtocolIE-F.	ield										
id: id-NA	S-PDU (38)										
	ty: reject (0)										
⊻ value											
			:037819cded0d7f5a43a7f2	2722fd7a3508aad12e3aa50							
	on-Access-Stratum 5G										
	Plain NAS 5GS Mess										
				agement messages (126)							
	0000 = Sp										
				age, not security protected (0)							
	✓ 5GS registration		request (0x41)								
			Paquest bit (EOP), No	follow-on request pending							
			ration type: initial r								
	✓ NAS key set id		action office superior in								
			curity context flag (T	SC): Native security context (for KSIAMF)							
			t identifier: 7								
	✓ 5GS mobile iden										
	Length: 54										
	0 =	= Spare: 0									
	.000 =	SUPI format	t: IMSI (0)								
	0 =	= Spare: 0									
	001 =	Type of ide	entity: SUCI (1)								
	Mobile Cour	ntry Code (M	CC): United States (31	0)							
	Mobile Netw	work Code (M	NC): TEST IMSI HNI (014	4)							
	Routing ind	dicator: 0									
			scheme Id: ECIES scheme	me profile B (2)							
			y identifier: 12								
				3508aad12e3aa500508cea89cb781cc7e365b22f8a0							
				a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b							
	Ciphert	ext: 22f8a06	14b								

Figure 9: Test Case SA-01 Initial UE Message

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help No. The Defination Definition Defi								
Imput Source Destination Protocol Length Info 101 2022-11-18 16:48:49.434444 10:208.67.19 10:208.67.19 NGAP/NAS-565 142 DomilinkNASTransport, Authentication request 105 2022-11-18 16:48:49.434844 10:228.67.19 10:228.67.29 NGAP/NAS-565 142 DomilinkNASTransport, Authentication request 105 2022-11-18 16:48:59.043147 10:228.67.29 10:228.67.19 NGAP/NAS-565 142 DomilinkNASTransport, Authentication request 106 2022-11-18 16:48:59.043147 10:228.67.19 NGAP/NAS-565 134 SACK (Ack-1, Arund-32768), DomilinkNASTransport, Security mode command 107 2022-11-18 16:48:59.04314 10:228.67.19 NGAP/NAS-565 134 SACK (Ack-1, Arund-16:384), UplinkNASTransport, Security mode command 107 2022-11-18 16:48:59.04314 10:228.67.244 10:228.67.19 NGAP/NAS-565 134 SACK (Ack-1, Arund-16:384), UplinkNASTransport, Security mode command 108 2022-11-18 16:48:59.04316 10:228.67.19 NGAP/NAS-565 142 SACK (Ack-1, Arund-16:384), UplinkN								
No. Time Source Destination Protocol Length Info 101 2022-11-18 16:48:49.834484 10:226.67.19 10:226.67.244 NGAP/NAS-565 132 InitialUMEstage, Registration request 105 2022-11-18 16:48:56.08:1307 10:226.67.29 10:226.67.29 NGAP/NAS-565 142 DumlinkWASTransport, Authentication request 106 2022-11-18 16:48:56.08:1307 10:226.67.29 10:226.67.29 NGAP/NAS-565 134 DumlinkWASTransport, Authentication request 107 2022-11-18 16:48:56.08:1567 10:226.67.19 NGAP/NAS-565 134 SACK (Ack-1, Arund-16:384), UplinkWASTransport, Security mode command 107 2022-11-18 16:48:56.08:1569 10:226.67.19 NGAP/NAS-565 134 SACK (Ack-1, Arund-16:384), UplinkWASTransport, Security mode command 108 2022-11-18 16:48:50.09:136 10:226.67.19 NGAP/NAS-565 142 SACK (Ack-1, Arund-16:384), UplinkWASTransport, Security mode command 104 Prome 103: 142 bytes on wire (1136 bits), 142 10:226.67.19 NGAP/NAS-565 142 SACK (Ack-1, Arund-16:384), U								
<pre> 181 2022-11-18 16:48:49.834444 19.220.67.19 10.205.67.204 MGAP/NAS-565 122 InitialUEMessage, Registration request 183 2022-11-18 16:48:59.838077 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 DownlinkNASTransport, Authentiation request 185 2022-11-18 16:48:59.8074457 10.205.67.204 10.205.67.204 NGAP/NAS-565 142 DownlinkNASTransport, Authentiation response 186 2022-11-18 16:48:59.8074457 10.205.67.204 10.205.67.204 NGAP/NAS-565 142 DownlinkNASTransport, Security mode complete, Re 188 2022-11-18 16:48:59.8074457 10.205.67.204 10.205.67.204 NGAP/NAS-565 134 SACK (Ack-1, Arund-32768), DownlinkNASTransport, Security mode complete, Re 188 2022-11-18 16:48:59.8091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack-1, Arund-32768), DownlinkNASTransport, Security mode complete, Re 188 2022-11-18 16:48:59.8091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack-2, Arund-32768), DownlinkNASTransport, Security mode command 107 202.11.8 16:48:59.8091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack-2, Arund-32768), DownlinkNASTransport, Security mode command 107 202.10 Virtual LAN, PRI: 0, DEI: 0, 1D: 524 10 Internet Protocol Version 4, Src: 10.205.67.204, Dst: 10.206.67.19 Stream Control Transmission Protocol, Src Port: 38412 (38412) votication Protocol (DownlinkNASTransport (4) criticality: Ignore (1) v NGAP-POU: initiatingNessage (0) v IntiatingNessage (0) v Internet. NGAP-FOU: initiatingNessage (0) v Item 1: id-RAM-UE-NGAP-ID v Tem 0: id-AMF-UE-NGAP-ID v ProtocolIE: 5 items v Item 1: id-RAM-UE-NGAP-ID v ProtocolIE: Field </pre>								
<pre>103 2022-11-18 16:48:49.888077 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 DownlinkNASTransport, Authentication request 105 2022-11-18 16:48:50.074457 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 UplinkNASTransport, Authentication request 106 2022-11-18 16:48:50.074457 10.205.67.204 10.220.67.19 NGAP/NAS-565 134 SACK (Ack=1, Arund=32768), DownlinkNASTransport, Security mode command 107 2022-11-18 16:48:50.083769 10.220.67.19 10.205.67.204 NGAP/NAS-565 134 SACK (Ack=1, Arund=32768), DownlinkNASTransport, Security mode command 107 2022-11-18 16:48:50.091301 10.220.67.19 10.220.67.19 NGAP/NAS-565 134 SACK (Ack=1, Arund=32768), DownlinkNASTransport, Security mode command 107 2022-11-18 16:48:50.091301 10.220.67.204 NGAP/NAS-565 142 SACK (Ack=2, Arund=32768), DownlinkNASTransport, Security mode command 107 2022-11-18 16:48:50.091301 10.220.67.204 NGAP/NAS-565 142 SACK (Ack=2, Arund=32768), DownlinkNASTransport, Security mode command 108 2022-11-18 16:48:50.091301 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=2, Arund=32768), DownlinkNASTransport, Security mode command 108 202.10 Virtual LAM, PRI: 0, DEI: 0, DD: S24 7 Frame 103: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) 7 Ethernet II, Src: ExtremeN_36:58:06 (b0:27:cf:36:58:06), Dst: Ericscon 7b:26:ce (58:45:4c:7b:26:ce) 7 Boze.10 Virtual LAM, PRI: 0, DEI: 0, DD: S24 7 Internet Protocol Version 4, Src: 10.205.67.204, Dst: 10.220.67.19 7 Ethernet II, sec: ExtremeN_36:S9:06 (b0:37:cf:36:18:02), Dst Port: 38412 (38412) 7 NGAPP-POU: initiatingNessage (0) 7 InitiatingNessage (0) 7 InitiatingNessage (0) 7 Internet Verotocol Version 4, Src: 10.205.67.204 7 Item 0: id-AMF-UE-MGAP-ID 7 V protocollE: 5 Items 7 Item 0: id-AMF-UE-MGAP-ID 7 V protocollE: Field 7 Item 2: id-NASP-D0 7 V ProtocollE: Field 7 Second 2: Sec</pre>								
<pre>185 2822-11-18 16:48:50.051307 10.220.67.19 10.220.67.204 NGAP/NAS-5G5 142 UplinkNASTransport, Authentication response 186 2822-11-18 16:48:50.045376 10.220.67.204 NGAP/NAS-5G5 134 5ACK (Ack.1, Arwnd-32768), DownlinkWASTransport, Security mode command 187 2822-11-18 16:48:50.045376 10.220.67.19 NGAP/NAS-5G5 134 5ACK (Ack.1, Arwnd-32768), DownlinkWASTransport, Security mode command 187 2822-11-18 16:48:50.045376 10.220.67.19 NGAP/NAS-5G5 134 5ACK (Ack.1, Arwnd-32768), DownlinkWASTransport, Security mode command 187 2822-11-18 16:48:50.045376 10.220.67.19 NGAP/NAS-5G5 142 SACK (Ack1, Arwnd-32768), DownlinkWASTransport, Security mode command 182 2822-11-18 16:48:50.045376 10.220.67.19 NGAP/NAS-5G5 142 SACK (Ack2, Arwnd-32768), DownlinkWASTransport, Security mode command 182 2822-11-18 16:48:50.045376 10.220.67.19 NGAP/NAS-5G5 142 SACK (Ack2, Arwnd-32768), DownlinkWASTransport, Security mode command 182 2822.10 Virtual LAN, PRI: 0, DEI: 0, ID: 524 142 SACK (Ack2, Arwnd-32768), DownlinkWASTransport (1) 52 Stream Control Transmission Protocol, Src Port: 38412 (38412) V NGAPP.DU: initiatingMessage (0) 19 NGAPP.DU: initiatingMessage (0) 19 NGAPP.DU: initiatingMessage (0) 10 V malue 10 DownlinkWASTransport (4) 10 criticality: ignore (1) 20 Value 20 DownlinkWASTransport (4) 20 Item 9: id-AWF-UE-NGAP-ID 20 Item 9: id-AWF-UE-NGAP-ID 20 Item 2: id-NAS-PDU 20 V FotocolIE-Field 20 Item 1: id-NAS-PDU 20 V ProtocolIE-Field 20 Item 1: id-NAS-PDU 20 V ProtocolIE-Field 20 V ProtocolIE-Field</pre>								
<pre>166 2822-11-18 16:48:50.074457 10.205.67.204 10.220.67.19 NGAP/NAS-565 134 SACK (Ack=1, Arwnd-32768), DownlinkWASTransport, Security mode command 187 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 258 SACK (Ack=1, Arwnd-32768), DownlinkWASTransport, Security mode command 188 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=1, Arwnd-532768), DownlinkWASTransport, Security mode command 188 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 258 SACK (Ack=1, Arwnd-532768), DownlinkWASTransport, Security mode command 198 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=2, Arwnd-532768), DownlinkWASTransport, Security mode command 198 202.10 Virtual LAW, PRI: 0, DEI: 0, DD: 524 10 Internet II, Src: ExtremeN_36:58:06 (b0:27:cf:36:58:06), Dst: Ericsson_7b:26:ce (58:45:4c:7b:26:ce) 202.10 Virtual LAW, PRI: 0, DEI: 0, DD: 524 202.10 Virtual LAW, PRI: 0, DEI: 0, DD: 524 202.10 Virtual LAW, PRI: 0, DEI: 0, DD: 524 200 Internet Protocol Version 4, Src: 10.205.67.204, Dst: 10.220.67.19 201 Stream Control Transmission Protocol, Src Port: 38412 (38412) 201 Stream Control Transmission Protocol, Src Port: 38412 (38412) 201 KGAPP.POU: initiatingNessage (0) 201 viriatingNessage (0) 202 viriatingNessage (0) 203 viriat</pre>								
<pre>197 2422-11-18 16:48:50.085769 18.220.67.19 10.205.67.204 NGAP/NAS-565 258 SACK (Ack=1, Arwnd-16384), UplinkluASTransport, Security mode complete, Re 108 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=1, Arwnd-16384), UplinkluASTransport, Security mode complete, Re 108 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=1, Arwnd-16384), UplinkluASTransport, Security mode commlete, Re 108 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=1, Arwnd-16384), UplinkluASTransport, Security mode commlete, Re 108 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=1, Arwnd-16384), UplinkluASTransport, Security mode commlete, Re 108 202.1Q Virtual LAN, PRI 0, DEI: 0, ID: 524 16 Internet Protocol Version 4, Src: 10.205.67.204, Dst: Encisson_7b:26:ce (58:45:4c:7b:26:ce) 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port: 38412 (38412) NGAP/NAS-565 5 Stream Cortol Transmission Protocol, Src Port, Stream Cortol Transmission Protocol, Src Port, Stream Stream</pre>								
108 2022-11-18 16:48:50.091301 10.205.67.204 10.220.67.19 NGAP/NAS-565 142 SACK (Ack=2, Arwmd=32768), DownlinkNASTransport, Security mode command ************************************								
<pre>> Frame 103: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) > Ethernet II, Src: ExtremeN_36:58:06 (b0:27:cf:36:58:06), Dst: Ericsson_7b:26:ce (58:45:4c:7b:26:ce) > 802:1Q Virtual LAW, PRI: 0, DEI: 0, DI: 524 > Internet Protocol Version 4, Src: 10:205.67:204, Dst: 10:220.67.19 > Stream Control Transmission Protocol, Src Port: 38412 (38412) > MR Application Protocol (DownlinkWASTransport) > NRAP-POU: initiatingNessage (0)</pre>								
<pre>> Ethernet II, Src. ExtremeN_36:58:06 (b0:27:cf:36:58:06), Dst: Ericsson_7b:26:ce (58:45:4c:7b:26:ce) > 802.1Q Virual LAN, PRI: 0, DEI: 0, ID: 524 > Internet Protocol Version 4, Src: 10.205.67.204, Dst: 10.220.67.19 > Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412) > KoApl-POU: initiatingNessage (0)</pre>								
<pre>> Ethernet II, Src. ExtremeN_36:58:06 (b0:27:cf:36:58:06), Dst: Ericsson_7b:26:ce (58:45:4c:7b:26:ce) > 802.1Q Virual LAN, PRI: 0, DEI: 0, ID: 524 > Internet Protocol Version 4, Src: 10.205.67.204, Dst: 10.220.67.19 > Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412) > KoApl-POU: initiatingNessage (0)</pre>								
<pre>> 882.1Q Virtual LAN, PRI: 0, DEI: 0, DI: 524 > Internet Protocol Version 4, Src: 10.285.67.204, Dit: 10.220.67.19 > Stream Control Transmission Protocol, Src Port: 38412 (38412) > No Application Protocol (DownlinkWaSTransport) > No Application Protocol (DownlinkWaSTransport (4) criticality: ignore (1) > value > DownlinkWaSTransport > value > DownlinkWaSTransport > VerotocolIE: 3 items > Vitem 0: id-AMF-UE-INGAP-ID > ProtocolIE-Field > VerotocolIE-Field > VerotocolIE-Field</pre>								
<pre>> Interimet Protocol Version 4, Src: 10.205.67.204, Dst: 10.220.67.19 > Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412) > NG Application Protocol (DownlinkWASTransport) > NGAP-POU: initiatingNessage (0) > initiatingNessage (0) > initiatingNessage (0) > initiatingNessage (0) > volue > procedureCode: id-DownlinkWASTransport (4) </pre>								
<pre>> Stream Control Transmission Protocol, Src Port: 38412 (38412), Dst Port: 38412 (38412) > N6 Application Protocol (DownlinkWASTransport) > N6AP-PDU: initiatingNessage (0) > initiatingNessage (0) > initiatingNessage (0) > value > DownlinkWASTransport (4) > value > DownlinkWASTransport > value > value > DownlinkWASTransport > value > v</pre>								
<pre>v NGAp-DU: initiatingMessage (0) v NGAP-DU: initiatingMessage (0) v initiatingMessage procedureCode: id-DownlinkMASTransport (4) criticality: ignore (1) v value v DownlinkMASTransport v protocolIE: i items v Item 0: id-AMF-UE-NGAP-ID > ProtocolIE-Field > Item 1: id-RAN-UE-NGAP-ID v Item 2: id-MAS-PDU v Item 2: id-MAS-PDU v ProtocolIE-Field</pre>								
<pre>v NGAP-PDU: initiatinglessage (0) v initiatinglessage procedureCode: id-DownlinkNASTransport (4) criticality: ignore (1) v value v value v DownlinkNASTransport v protocolIE: 3 items v Item 0: id-AMF-UE-INGAP-ID > ProtocolIE: Field > Item 1: id-RAN-UE-NISAP-ID v Item 2: id-NAS-PDU v Item 2: id-NAS-PDU v ProtocolIE-Field</pre>								
<pre>v initiatingNessage procedureCode: id-DownlinkNASTransport (4) criticality: ignore (1) v value v DownlinkNASTransport v protocolIEs: 3 items v Item 0: id-ANF-UE-NGAP-ID > ProtocolIE-Field > Item 1: id-RAN-UE-NGAP-ID v Item 2: id-NAS-PDU v Item 2: id-NAS-PDU v ProtocolIE-Field</pre>								
<pre>criticality: ignore (1) vulue v DownlinkNASTransport v protocolIEs: 3 items v Item 0: id-AVF-VE-NGAP-ID > ProtocolIE-Field > Item 1: id-RAN-UE-NGAP-ID v Item 2: id-NAS-PDU v Item 2: id-NAS-PDU v ProtocolIE-Field</pre>								
<pre>vulue v DownlinkHASTransport v protocolIEs: 3 items v Item 0: id-AMF-UE-NGAP-ID > ProtocolIE-Field > Item 1: id-RAN-UE-NGAP-ID v Item 2: id-NAS-PDU v Item 2: id-NAS-PDU v ProtocolIE-Field</pre>								
<pre>v DownlinkMASTransport v protocollEr: 3 items v Item 0: id-AMF-UE-INGAP-ID</pre>								
<pre>v protocolIEs: '3 items v Item 0: id-AMF-UE-NGAP-ID > ProtocolIE-Field > Item 1: id-RAN-UE-NGAP-ID v Item 2: id-NAS-PDU v ProtocolIE-Field</pre>								
<pre>> Item 0: id-AMF-UE-NGAP-ID > ProtocollE-Field > Item 1: id-RAN-UE-NGAP-ID > Item 2: id-NAS-PDU < ProtocollE-Field</pre>								
<pre>> ProtocolIE-Field > Item 1: id-RAN-UE-MGAP-ID ~ Item 2: id-NAS-PDU ~ Trom Second E-Field</pre>								
> Item 1: id-RAN-UE-NGAP-ID > Item 2: id-HAS-PDU > ProtocollE-Field								
<pre>> Item 2: id-NAS-PDU > ProtocolIE-Field</pre>								
 ProtocolIE-Field 								
· /rotocolle-rield id: id-Nos-PDU (38)								
10: 10-M3-FDU (36) criticality: reject (0)								
✓ value								
NAS-PDU: 7e005600020000210119525fd0186fee995ce5364418139c2010a36da0071529800073e8								
V Non-Access-Stratum 56S (NAS)PDU								
V Plain NAS 5GS Message								
Extended protocol discriminator: 5G mobility management messages (126)								
0000 = Spare Half Octet: 0 0000 = Security header type: Plain NAS message, not security protected (0)								
doud = Security neader type / lain NAS message, not security protected (0) Message type: Authentication request (0x56)								
0000 = Spare Half Octet: 0								
✓ NAS key set identifier - ngKSI								
0 = Type of security context flag (TSC): Native security context (for KSIAMF)								
✓ ABBA								
Length: 2								
ABBA Contents: 0000								
 Authentication Parameter RAND - 5G authentication challenge 								
Element ID: 0x21								
RAND value: 0119525fd186fee995ce5364418139c								
 Authentication Parameter AUTN (UMTS and EPS authentication challenge) - 5G authentication challenge Element ID: 0x20 								
Length: 16								
⊂ engui: 10 √ AUTN value: a36da0071529800073682fd23f53b9dd								
SQN vor AK: abda80/1529								
ANF: 8000								
MAC: 73e82fd23f53b9dd								

Figure 10: AMF/Core Authentication Request

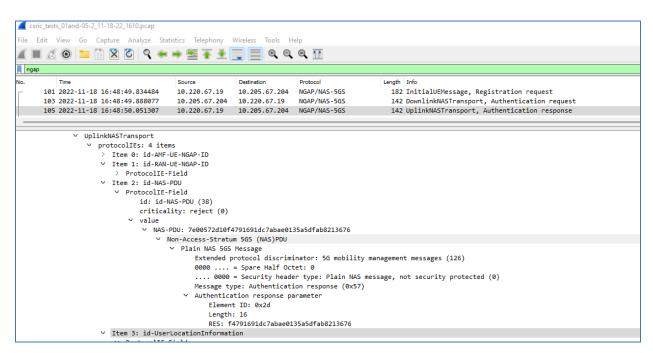


Figure 11: UE Authentication Response

csric_tests_01and-05-2_11-18-22_1610,pcap -								
ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
(■ 2 @ = 3 X 2 4 + ⇒ 2 7 1 2 = 0 9 9 9 1								
Ingao								
Time Source Destination Protocol Length Info 101 2022-11-18 16:48:49.83448 10.226.67.19 10.226.67.20 NGAP/IAS-565 152 InitialUMPessage, Registration request 103 2022-11-18 16:48:59.83807 10.226.67.20 NGAP/IAS-565 142 DownlinkHASTransport, Authentication request 105 2022-11-18 16:48:59.83807 10.226.67.204 10.826.67.204 NGAP/IAS-565 142 DownlinkHASTransport, Authentication reguest 106 2022-11-18 16:48:59.8074457 10.226.67.204 10.826.67.204 10.826.67.204 10.426.67.204 10.427.657 107 2022-11-18 16:48:59.8075103 10.226.67.19 10.826.67.204								
<pre>criticality: reject (0) value Value Mos-POU: 7e039c116b38007e005d20004f070f070e1360102 Value Mos-Access-Strutum 505 (MAS)POU v Security protected NAS 565 message Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0 0011 = Security header type: Integrity protected with new 565 security context (3) Message authentication code: 0x00011658 Sequence number: 0 v Plain NAS 565 Message Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0 vesage authentication code: 0x00011658 Sequence number: 0 vesage type: Security header type: Plain NAS message, not security protected (0) Message type: Security mede command (0x5d) vesage tidentifier: - ngKSI 0010 = Type of intEgrity protection algorithm: 128-56-IA2 (2) 0000 = Spare Half Octet: 0 vesage tidentifier: - ngKSI 00 = Type of security context flag (TSC): Native security context (for KSIAMF) 00 = Nye of security context flag (TSC): Native security context (for KSIAMF) 00 = Nye of security context flag (TSC): Native security context (for KSIAMF) </pre>								

Figure 12: Core Ciphering Algorithm in use – NULL ciphering

csric_tests_01and-05-2_11-18-22_1610.pcap								
Edit View Go Capture Analyze St	atistics Telephony Wireless Tools	Help						
>								
Time	Source Destination	Protocol	Length Info					
101 2022-11-18 16:48:49.834484 10.220.67.19 10.205.67.204 NGAP/NAS-555 182 InitialUEMessage, Registration request								
103 2022-11-18 16:48:49.888077 10.205.67.204 10.220.67.19 NGAP/NA5-565 142 DownlinkNASTransport, Authentication request								
105 2022-11-18 16:48:59.051307 10.228.67.19 10.226.67.204 NGAP/NG5-565 142 UplinkNASTransport, Authentication response 162 2022-11-18 16:48:59.067457 10.226.67.204 10.220.67.19 NGAP/NG5-565 134 SACK (Ack+1) Arnmd-32788). DownlinkNASTransport. Security mode command								
105 2022-11-18 16:48:50.074457	10.205.67.204 10.220.67.19 10.220.67.19 10.205.67.204							
107 2022-11-18 16:48:50.085769	10.220.67.19 10.205.67.204 10.220.67.19	NGAP/NAS-505/NAS-50 NGAP/NAS-5GS	S 258 SACK (Ack=1, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration reque 142 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command					
109 2022-11-18 16:48:50.100630		NGAP/NAS-5GS	142 SACK (ACK=2, Arwid=J6384), UplinkNASTransport, Security mode command					
113 2022-11-18 16:48:50.461164	10.205.67.204 10.220.67.19	NGAP / NAG- 503	180 SACK (ACK-2, A WHILE LODGE), OPTIMIZED AND AND AND A COMPLETE 182 InitialContextSetupRequest					
115 2022-11-18 16:48:50.517237	10.220.67.19 10.205.67.204		94 InitialContextSetupResponse					
116 2022-11-18 16:48:50.517261	10.220.67.19 10.205.67.204		914 UERadioCapabilityInfoIndication					
✓ Item 2: id-NAS	-PDU							
✓ Item 2: Id-WAS ✓ ProtocolIE								
	NAS-PDU (38)							
	lity: reject (0)							
✓ value								
	-PDU: 7e048be1ccbb007e005e770009	3515371501217124f17100	5f7e004171003601134010f0					
~	Non-Access-Stratum 5GS (NAS)PDU							
	Security protected NAS 5GS m	essage						
	Extended protocol discrim	minator: 5G mobility ma	anagement messages (126)					
0000 = Spare Half Octet: 0								
0100 = Security header type: Integrity protected and ciphered with new 5GS security context (4)								
Message authentication code: 0x8be1ccbb								
Sequence number: 0								
	 Plain NAS 5GS Message 							
	Extended protocol discrim		anagement messages (126)					
	0000 = Spare Half O							
			ssage, not security protected (0)					
	Message type: Security m	ode complete (0x5e)						
	✓ 56S mobile identity							
	Element ID: 0x77 Length: 9							
		indication: Even numbe						
	0 = Udd/even 101 = Type of i		a of identity digits					
	IMEISV: 3517351101217							
	 NAS message container 	421						
	Element ID: 0x71							
Element ID: 9x71 Length: 95								
	V Non-Access-Stratum 50	IS (NAS)PDU						
	V Plain NAS 5GS Mes							
			mobility management messages (126)					
		pare Half Octet: 0						
			lain NAS message, not security protected (0)					
		Registration request (
	✓ 5GS registrati		• •					
			t (FOR): No follow-on request pending					
		= 5GS registration typ	e: initial registration (1)					
V NAS key set identifier								
	V NAS key set id	lentifier						

Figure 13: Core Ciphering Algorithm in use –Uplink NAS Transport NULL ciphering

csric tests 01and-05-2 11-18-22 1610.pcap	
Edit View Co. Conturn Anthree St.	tatistics Telephony Wireless Tools Help
🔳 🖉 🙁 🚞 🚞 🕲 🖉 🖛	= 🗢 🕾 🗿 🕎 📃 🕘 Q. Q. Q. II
igap	
Time	Source Destination Protocol Length Info
106 2022-11-18 16:48:50.074457	18.205.67.204 18.220.67.19 NGAP/NAS-5G5 134 SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command
107 2022-11-18 16:48:50.085769	10.220.67.19 10.205.67.204 NGAP/NAS-5GS/NAS-5GS 258 SACK (Ack=1, Arwnd=16384), UplinkNASTransport, Security mode complete, Registration requ
108 2022-11-18 16:48:50.091301	10.205.67.204 10.220.67.19 NGAP/NAS-5GS 142 SACK (Ack=2, Arwnd=32768), DownlinkNASTransport, Security mode command
✓ value	I-UE-NGAP-ID: 1679000
✓ Item 2: id-NAS	
✓ ProtocolIE-	
	NAS-PDU (38)
	ality: reject (0)
✓ value	
V NAS	5-PDU: 7e03c2da75b1017e005d020004f070f070e157023601001904f070c040
~	Non-Access-Stratum 5GS (NAS)PDU
	V_Security_protected_NAS_S6S_message
—	Extended protocol discriminator: 5G mobility management messages (126)
	0000 = Spare Half Octet: 0
	0011 = Security header type: Integrity protected with new 5GS security context (3)
	Message authentication code: 0xc2da75b1
	Sequence number: 1
	 Plain NAS 56S Message
	Extended protocol discriminator: 5G mobility management messages (126)
	0000 = Spare Half Octet: 0
	0000 = Security header type: Plain NAS message, not security protected (0)
	Message type: Security mode command (0x5d)
	V NAS security algorithms
	0000 = Type of ciphering algorithm: 5G-EA0 (null ciphering algorithm) (0)
	0010 = Type of integrity protection algorithm: 128-5G-IA2 (2)
	0000 = Spare Half Octet: 0
	✓ NAS key set identifier - ngKSI
	 > UE security capability - Replayed UE security capabilities > IMETSV request
	Inclov request 110 = Element ID: 0xe-
	001 = JMEIS (request: IMEISV requested (1)
	 v NAS security algorithms - Selected EPS NAS security algorithms
	 Not security algorithms - selected ris nots security algorithms Element 10: 0x57
	Liment LD: 0437 0 = Spare bit(s): 0x00
	000 = Jpaie UI(5), 0000 .000 = Type of ciphering algorithm: EPS encryption algorithm EEA0 (null ciphering algorithm) (0)
	0 = Spare bit(s): 0x00

Figure 14: Core Ciphering Algorithm in use – Downlink NAS Transport NULL ciphering

Part 2: Using NEA2 Encryption

In the second part of the experiment, we changed the core setting to use NEA2, the 128-NEA2 cipher algorithm as shown in Figure 8 above. As above, the core and UE exchange an authentication request and response (Figure 15 and Figure 16). Figure 17 shows the downlink message indicating the NEA2 cipher algorithm is to be used. Subsequently, all information transmitted is encrypted, as indicated by the inability of the messages to be deciphered in Figure 18 and Figure 19.

_									
	⊆ csric_tests_01_prd2_11-18-22_1710.pcap — □								
File	ile Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help								
	🔳 🖉 🐵 🚞 🖺 🖹 🖉 🍳 🖛 🏓 🖺	🛉 👲 📃 🔳 🍳 e	. ∈. ∏						
, n	gap				X 🗆				
No.	Time Source Destination Protocol Length Info								
Г	137 2022-11-18 17:17:40.193924 10.220.67.19 10.205.67.204 NGAP/NA5-565/N48-565 210 InitialUEMessage, Registration request, Registration request								
	138 2022-11-18 17:17:40.196040	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	118 SACK (Ack=0, Arwnd=32768) , DownlinkNASTransport, Identity request				
	140 2022-11-18 17:17:40.308451	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	186 UplinkNASTransport, Identity response				
	142 2022-11-18 17:17:40.365217	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request				
	144 2022-11-18 17:17:40.428006	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	150 UplinkNASTransport, Authentication response				
	145 2022-11-18 17:17:40.439472	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	134 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command				
	V Item 1: id-RAN-UE-NGAN > ProtocolIE-Field	-10							
	✓ Item 2: id-NAS-PDU								
	ProtocolIE-Field								
	id: id-NAS-PDU	(38)							
	criticality: r								
	∨ value	(- <i>)</i>							
	 Value Nos-PDU: 7e0056010200002197fc0a687764137cc2419aa008cc5c73201027845dbc938b80004980 								
	 Non-Access-Stratum 565 (MAS)PDU 								
	V Plain NAS 565 Message								
	Extended protocol discriminator: 5G mobility management messages (126)								
	0000 = Spare Half Octet: 0								
				ssage, not security protected	(0)				
		Message type: Authentica							
		0000 = Spare Half O							
	v	NAS key set identifier -							
				(TSC): Native security context	t (for KSIAMF)				
		001 = NAS key :	et identifier: 1						
		ABBA Authentication Parameter	name of authoritations	(
	Č.	Element ID: 0x21	RAND - 56 authenticat	ion challenge					
			764137cc2419aa008cc5c7	2					
				thentication challenge) - 5G	authentication challenge				
		Element ID: 0x20	Horna (onito and cro au	chemicación charrenge) - 50	anchericitation chartenBe				
		Length: 16							
		 AUTN value: 27845dbc9 	38b80004980e604760cc4e	4					
		SON xor AK: 27845							
	AllF: 8000								

Figure 15: NEA2 AMF/CORE Authentication Request

marenr	DIDT.COM/DEISODAI/ODOLKI LIMO EOLU IS	avours/15/oneorive	aspy//d=%/Enerso	nal%zEgnaiki lima edil%z	HUGGUMENTS%/HUGGUMENTS%/HIEST%/HIER%/HEELY, 16/ 57 🇩 💶 🚢 🔹 📟
🧹 cs	ric_tests_01_prt2_11-18-22_1710.pcap				
File	Edit View Go Capture Analyze St	atistics Telephony	Wireless Tools H	elp	
	I 🖉 🛞 🚞 🗎 🕱 🏹 🔶	- 👄 🕾 🝝		Q. 11	
nga	P				
No.	Time 137 2022-11-18 17:17:40.193924 138 2022-11-18 17:17:40.30640 140 2022-11-18 17:17:40.308451 142 2022-11-18 17:17:40.365217 144 2022-11-18 17:17:40.428006 145 2022-11-18 17:17:40.43873 146 2022-11-18 17:17:40.43873		Destination 10.205.67.204 10.220.67.19 10.205.67.204 10.220.67.19 10.205.67.204 10.220.67.19 10.205.67.204	Protocol NGAP/NAS-5GS/NAS-5GS NGAP/NAS-5GS NGAP/NAS-5GS NGAP/NAS-5GS NGAP/NAS-5GS NGAP/NAS-5GS NGAP/NAS-5GS	Langh Info 210 InitialUEMessage, Registration request, Registration request 118 SACK (Ack-0, Arwnd-32768) , DownlinkHASTransport, Identity request 186 UplinkHASTransport, Identity response 142 DownlinkHASTransport, Authentication request 150 UplinkHASTransport, Authentication response 134 SACK (Ack-2, Arwnd-32768) , DownlinkHASTransport, Security mode command 222 SACK (Ack-2, Arwnd-16384) , UplinkHASTransport
	critica Value VAS	NAS-PDU (38) NIity: reject (0) -PDU: 7e012929a64 Non-Access-Strat		:c4200b607182669ad560873	cde9f
		Extended 0000 0001 Message a	protocol discrimi = Spare Half Oct = Security heade uthentication cod number: 16	nator: 5G mobility mana et: 0 r type: Integrity prote	
		0000 0000 Message t ✓ Authentic Elemen	 Spare Half Oct Security heade ype: Authenticati ation response pant ID: 0x2d 	r type: Plain NAS messa on response (0x57)	gement messages (126) ge, not security protected (0)
		rLocationInforma	311cc4200b6071826 tion	59ad560873cde9f	

Figure 16: NEA2 AMF/UE Authentication Response

csric_tests_01_prt2_11-18-22_1710.pcap		
File Edit View Go Capture Analyze St	atistics Telephony Wireless Tools	Help
	🔹 🔿 🔮 🕌 👤 📃 🔲 🍭 🤇	
ngap		
 Time 137 2022-11-18 17:17:40.193924 138 2022-11-18 17:17:40.196040 140 2022-11-18 17:17:40.306451 142 2022-11-18 17:17:40.306451 144 2022-11-18 17:17:40.428066 145 2022-11-18 17:17:40.428047 146 2022-11-18 17:17:40.448703 	10.220.67.19 10.205.67.204	NGAP/NAS-5GS 118 SACK (Ack-ø, Arund=32768), DownlinkNASTransport, Identity request 4 NGAP/NAS-5GS 186 UplinkNASTransport, Identity response NGAP/NAS-5GS 142 DownlinkNASTransport, Authentication request NGAP/NAS-5GS 150 UplinkNASTransport, Authentication response NGAP/NAS-5GS 150 UplinkNASTransport, Authentication response NGAP/NAS-5GS 150 UplinkNASTransport, Authentication response NGAP/NAS-5GS 134 SACK (Ack-2, Arund=32768), DownlinkNASTransport, Security mode command
critica v value RAM V Item 2: id-NAS V ProtocollE- id: id- critica v value v NAS	RAW-UE-NGAP-ID (85) hlty: reject (0) -UE-NGAP-ID: 16790010 -POU -Field NAS-POU (38) hlty: reject (0) -PDU: 7e037d273240007e005d22010	
	<pre>0000 = Spare Half (0011 = Security he Message authentication o Sequence number: 0 > Plain NAS 5GS Message Extended protocol discr: 0000 = = Spare Half (0000 = Security he Message type: Security n NAS security algorithms 0010 = Type of 0010 = Type of 0000 = Spare Half (NAS key set identifier 00.1 = Type of 001 = NAS key</pre>	<pre>message iminator: 56 mobility management messages (126) Octet: 0 ader type: Integrity protected with new 565 security context (3) code: 0x7d273240 iminator: 56 mobility management messages (126) Octet: 0 ader type: Plain NAS message, not security protected (0) mode command (0x5d) <u>ciphering algorithm: 128-56-E82 (2)</u> integrity protection algorithm: 128-56-IA2 (2) Octet: 0 - ngKSI security context flag (TSC): Native security context (for KSIAMF)</pre>

Figure 17: NEA2 Ciphering Command

_ c	sric_tests_01_prt2_11-18-22_1710.pcap				
File	Edit View Go Capture Analyze Si	tatistics Telephony	Wireless Tools H	elp	
	🔳 🖉 💿 🚞 🛅 🕱 🍝	1 A			
				✓ Ⅲ	
ng ng	ap				
No.	Time	Source	Destination	Protocol	Length Info
	142 2022-11-18 17:17:40.365217	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 DownlinkNASTransport, Authentication request
	144 2022-11-18 17:17:40.428006	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	150 UplinkNASTransport, Authentication response
	145 2022-11-18 17:17:40.439472		10.220.67.19	NGAP/NAS-5GS	134 SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
	146 2022-11-18 17:17:40.448703	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	222 SACK (Ack=2, Arwnd=16384) , UplinkNASTransport
	147 2022-11-18 17:17:40.455974	10.205.67.204	10.220.67.19	NGAP/NAS-5GS	142 SACK (Ack=3, Arwnd=32768) , DownlinkNASTransport, Security mode command
	148 2022-11-18 17:17:40.468290	10.220.67.19	10.205.67.204	NGAP/NAS-5GS	158 SACK (Ack=3, Arwnd=16384) , UplinkNASTransport
	150 2022-11-18 17:17:40.665721	10.205.67.204	10.220.67.19	NGAP	182 InitialContextSetupRequest
	151 2022-11-18 17:17:40.688484	10.220.67.19	10.205.67.204	NGAP	94 InitialContextSetupResponse
	✓ value				
		I-UE-NGAP-ID: 1679	0010		
	✓ Item 2: id-NAS				
	ProtocolIE				
		-NAS-PDU (38)			
		ality: reject (0)			
	✓ value				
				e6cd68/e4d†/2e2066b8	126f1de88b7c6b0f9898529cc
	0	Non-Access-Strat			
			ected NAS 5GS me		management messages (126)
			= Spare Half Oct		management messages (126)
					rotected and ciphered with new 5GS security context (4)
			<pre>uthentication cod</pre>		rotected and ciphered with new Sos security context (4)
		Sequence		ie: 0x6/50450/	
		 Plain NAS 565 			
				inator: Unknown (49)	
			5GS PD 49 (Unkno		
				otocol): Not a NAS 5	565 PD 49 (Unknown)]
			ot a NAS 5GS PD 4		
			everity level: En		
			roup: Protocol]		
	>	Data (84 bytes)			
	✓ Ttem 3: id-Use		ion		

Figure 18: NEA2 Uplink NAS Transport Ciphering – Uplink Transport Data is encrypted

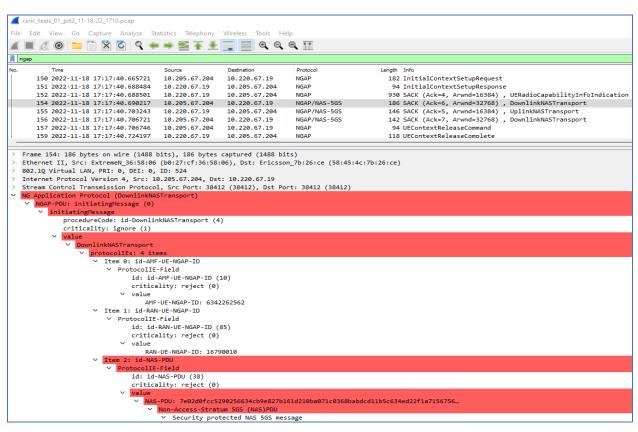


Figure 19: NEA2 Downlink NAS Transport Ciphering – Downlink Transport Data is encrypted

Success Criteria:

Only NAS messages without user identities (e.g. SUPI, IMEI, etc) are exchanged between smartphone and AMF prior to establishing an encrypted channel. These NAS messages may contain temporary identifiers (TMSI, GUTI, etc.).

After establishment of the encrypted channel, all NAS messages are encrypted, enabling user identity information to be safely exchanged. If the encrypted channel is disabled, messages containing user identities are exchanged between the UE and AMF without encryption.

Results

Condition	Status
Only non-user information is observable prior to NAS encryption	Only SUCI is
	transmitted
After NAS encryption, all NAS messages are encrypted	Messages are
	encrypted with NEA2
If the encrypted channel is disabled, messages containing user	Message details are
identities are exchanged between UE and AMF without encryption	visible with NEA0
Overall Test	Success

Test Case 2: CSRIC 7 WG 3 – RRC Signaling Confidentiality

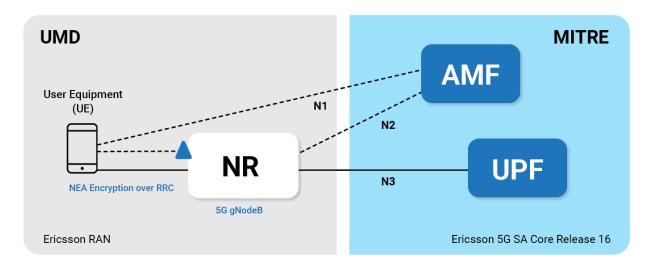


Figure 20: Test Case SA-02 Configuration

Test Case ID: TC-SA-02

Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the RRC signaling confidentiality, but optional for service providers to use. Given this standards requirement, CSRIC VII recommends protection of the RRC-signaling confidentiality. Only non-user identity related information shall be conveyed prior to security context being established.

This test involves first demonstrating the visibility of identity-related data when no encryption (NULL scheme) is used and then subsequently demonstrating the concealment of that data when RRC encryption is enabled.

Used	Test Point	Description and Use
	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
Х	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

Test points used:

This test has two parts: 1) with NEA0 (no encryption) and 2) with NEA2 activated to encrypt RRC signaling. Figure 21 shows the command line interface setting the RRC encryption on the RAN to use NULL (NEA0) as the first priority.

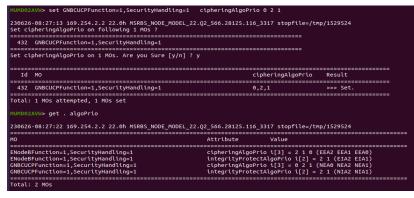


Figure 21: Setting RAN RRC encryption to NEA0

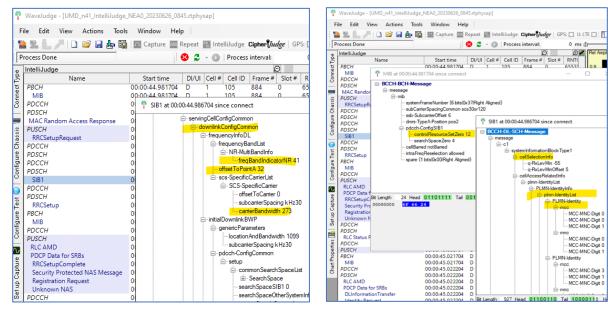


Figure 22: WaveJudge/IntelliJudge capture of N41 specifications

Figure 23: WaveJudge/IntelliJudge capture of PLMN information

Figure 22 and Figure 23 show the UE attach process as captured by the WaveJudge/IntelliJudge tool. Figure 24 and Figure 25 show WaveJudge captures of messages processed with the NEA0 (NULL) algorithm. Because the ciphering algorithm in use is NEA0, all the "security protected" messages can be read in clear text.

T	WaveJudge - [UMD_n41_I	intellibuuge_N								
Fil	le Edit View Actio	ons Tools	Window H	lelp						
	🗙 🛯 🥕 🗋 😂	🚽 📥 🛅 🕻	Cipher Judge	GPS: E	. U: LT	EDI			= 2	191 🖷
Pr	rocess Done			1 🐼			rocess int			0 ms
		Intellifier date		-						
_	Capture III Repeat 181	intelibudge	ms	ingg	jers //	Powe				
· r	IntelliJudge Name		Start tim		DI/UI	Cell #	Cell ID	Frame #	Slot #	RNT
	3101		00.00.44.90	0704	0	1	105	004	10	0000
	RRCSetup MIB		00:00:44.99 00:00:45.00		D D	1	105 105	885 886	0	2007 6553
I.	RLC AMD		00:00:45.00		Ŭ	1	105	886	4	2007
1	PDCP Data for SRBs		00:00:45.00		U	1	105	886	4	2007
	RRCSetupComplete		00:00:45.00		U	1	105	886	4	2007
ł	Security Protected NAS Registration Request	Message	00:00:45.00		UUU	1	105 105	886 886	4	2007
	Unknown NAS		00:00:45.00		ŭ	1	105	886	4	2007
J.	RLC Status PDU		00:00:45.00	6704	D	1	105	886	10	2007
L	MIB		00:00:45.02		D	1	105	888	0	6553
. [RLC AMD PDCP Data for SRBs		00:00:45.02 00:00:45.02		D D	1	105 105	888 888	1	2007
Ē	RRCSetupRequest at 0	0.00.44 08370								×
	UL-CCCH-Message	0.00.44.50570	A since connec							
	estat	Request lentity andomValue {3 plishmentCause	39 bits 0x58AFF3 • mo-Signalling	3E63 R	ight Alig	ned}				7. 7. 7.
	i mc Setup Req i mc Setup i ue-ld i u	Request lentity andomValue {3 plishmentCause e {1 bits 0x00 R	mo-Signalling ight Aligned}							7. 7. 7. 7.
	È nrcSetup Req È nrcSetup Cue la ue la ue spare [™] Security Protected N	Request lentity andomValue {3 plishmentCause {1 bits 0x00 R NAS Message	mo-Signalling light Aligned} at 00:00:45.003							33 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7.
	recSetup Req recSetup	Request lentity andomValue {3 plishmentCause {1 bits]0x00 R VAS Message NAS Message	• mo-Signalling ight Aligned} at 00:00:45.003							7. 7. 7. 7.
	recSetup Req recSetup	Request lentity andomValue {3 jlishmentCause e {1 bits]0x00 R NAS Message NAS Message bility manageme	e mo-Signalling light Aligned} at 00:00:45.003 ge ent messages	704 sin	ice con	nect	Octet Len	gth		
	recSetup Req recSetup	Request Jentity andomValue {3 JishmentCause e {1 bits 0x00 R NAS Message NAS Message bility management ator 14 => Rese	mo-Signalling light Aligned} at 00:00:45.003 ge ent messages erved For Extensi	704 sin	ice con	nect	Octet Len	gth		
	recSetup Req recSetup	Request lentity andomValue {3 jishmentCause {1 bits 0x00 R NAS Message NAS Message bility management stor 14 => Rese ype 1 => Integri	mo-Signalling light Aligned} at 00:00:45.003 ge ent messages erved For Extensi ity protected	704 sin	ice con	nect	Octet Len	gth		
	recSetup Req recSetup	Request Jentity andom Value {3 Jishment Cause a {1 bits 0x00 R VAS Message NAS Message bility manageme ator 14 => Rese ype 1 => Integri cation Code 0x IBER 8 % F	mo-Signalling light Aligned} at 00:00:45.003 ge ent messages erved For Extensi ity protected	704 sin ion Of T	ice con	nect To One (
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message NAS Message bility manageme ator 14 => Rese ype 1 => Integri cation Code 0x4 IBER 8	mo-Signalling ight Aligned) at 00:00:45.003 ge ent messages erved For Extensi ity protected 6667B1A6 Registration Re	ion Of T	The PD	nect To One (7. 7. 7. 7.
	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message NAS Message bility manageme ator 14 => Rese ype 1 => Integri cation Code 0x4 IBER 8	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages served For Extens ity protected <u>6667B1A6</u> Registration Re Registration R EPD 7 => 5G	704 sin ion Of T equest a S mobili	The PD at 00:00	nect To One (:45.0037	704 since	connect		×
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message NAS Message bility manageme ator 14 => Rese ype 1 => Integri cation Code 0x4 IBER 8	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages arved For Extens ty protected 6667B1A6 Registration Re Registration R Cogistration R	704 sin ion Of T equest a equest S mobili riminato	The PD at 00:00	nect To One (:45.0037	704 since	connect		×
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message NAS Message bility manageme ator 14 => Rese ype 1 => Integri cation Code 0x4 IBER 8	mo-Signalling ight Aligned) at 00:00:45.003 ge ent messages enved For Extens ty protected 6667B1A6 Registration Re Registration Re rim EPD 7 = 5 5G m Protocol Disc m Reserved OK	704 sin ion Of T equest a equest S mobili riminato	The PD The PD at 00:00 t ty mana r 14 =>	nect To One (:45.003) gement (Reserve	704 since messages d For Exte	connect ension Of 1	he PD To	× One Or
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plothmentCause = {1 bits 0x:00 R NAS Message bility management ator 14 => Reserved ype 1 => Integre cation Code 0xi BER 8 squest P F	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages enved For Extens ty protected <u>6667B1A6</u> Registration Re Registration Re rotocol Disc ··· Protocol Disc ··· Security Heac ··· Message Ider	ion Of T quest a equest S mobili iminato der Type	The PD at 00:00 t ity mana r 14 => e 0 => F	nect To One (:45.0037 gement Reserve Plain NAS	704 since messages d For Exte 6 message	connect ension Of 1	he PD To	× One Or
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message bility manageme ator 14 => Rese ype 1 => Integrisation Code 0x1 IBER 8 Producest	mo-Signalling ight Aligned at 00:00:45.003 ge ent messages arved For Extens ty protected 6667B1A6 Registration Re Registration Re restration Re reserved OK For Event Protocol Disc Reserved OK Security Head Message Ider message Ider ngKS1	ion Of T equest a smobili riminato der Type ntity 65	The PD at 00:00 t ity mana r 14 => e 0 => F e 0 => F e gi	nect To One (:45.0037 gement Reserve Plain NAS	704 since messages d For Exte 6 message	connect ension Of 1	he PD To	× One O
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message bility manageme ator 14 => Rese ype 1 => Integrisation Code 0x1 IBER 8 Producest	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages enved For Extens ty protected <u>6667B1A6</u> Registration Re Registration Re rotocol Disc ··· Protocol Disc ··· Security Heac ··· Message Ider	704 sin ion Of T equest a equest S mobili riminato der Type ntity 65 tion Typ	The PD at 00:00 t ty mana r 14 => e 0 => F => Regi	rect To One (:45.0037 gement Reserve Plain NAS stration I	704 since messages d For Exte 6 message Request	connect ension Of 1	he PD To	× One O
Bi	 mcSetupReq mcSetup ue-ld ue-ld spare * Security Protected N From EPD 7 => 5GS mole Protocol Discrimina Reserved OK Security Header Ty Message Authentic SEQUENCE_NUM Registration Res 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message bility management bility m	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages artved For Extens ty protected 6667B1A6 Registration Re Registration Re rotocol Disc … EPD 7 => 5G … Protocol Disc … Reserved OK … Security Head … Message Ider … ngKSI … SolGS Registrat … Follow-on … Type 1 =:	ion Of T equest a equest S mobili riminato der Type ntity 65 tion Typ > Initial	The PD at 00:00 t ty mana r 14 => e 0 => F egi e st Pend	rect To One (:45.0037) gement Reserve Plain NAS stration I stration I	704 since messages d For Exte 6 message Request	connect ension Of 1	he PD To	× 000000
Bi	Bit Length 576 Head 0	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message bility management bility m	mo-Signalling ight Aligned) at 00:00:45.003 ge ent messages enved For Extens ty protected 6667B1A6 Registration Re Registration Re Registration Re Registration Re Comparison Reserved OK Security Heat Message Ider ngKSI SGS Registrat Follow-on Type 1 =: SG Mobile Ide	704 sin ion Of T equest a S mobili riminato der Type ntity 65 tion Type Reque I Initial Jentity	The PD at 00:00 t ty mana r 14 => e 0 => F => Regi st Pend Registra	rect To One (:45.0037) gement Reserve Plain NAS stration I stration I	704 since messages d For Exte 6 message Request	connect ension Of 1	he PD To	× 000000
Bi	Geurity Protected For Security Protecte	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message bility management bility m	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages arved For Extensi ty protected 6667B1A6 Registration Re Registration Re Registration Re Registration Re Registration Re Security Hear message Ider follow-on motool bisc SGS Registrat follow-on motool is security C SGS Mobile Id UE Security C	704 sin ion Of T equest a S mobili riminato der Type ntity 65 tion Type Reque I Initial Jentity	The PD at 00:00 t ty mana r 14 => e 0 => F => Regi st Pend Registra	rect To One (:45.0037) gement Reserve Plain NAS stration I stration I	704 since messages d For Exte 6 message Request	connect ension Of 1	he PD To	× 000000
Bi	 ➡ rrcSetupReq ➡ rrcSetup ➡ ue-ld ➡ ue-ld ➡ ue-ld ➡ ue-ld ➡ spare * Security Protected N ➡ EPD 7 => 5GS mol ➡ Protocol Discrimina ➡ Reserved OK ➡ Security Header Ty ➡ Message Authentic ➡ SEQUENCE_NUM ➡ SEQUENCE_NUM ➡ Registration Re 	Request lentity andom Value {3 plishmentCause a {1 bits 0x00 R NAS Message NAS Message bility management ator 14 => Rese ype 1 => Integrised bility management bility managem	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages art option for Extense try protected 6667B1A6 Registration Re Registration Re rotocol Disc … EPD 7 => 5G … Protocol Disc … Reserved OK … Security Head … Message Ider … Message Ider … Follow-on … Type 1 =: 5GS Mobile Id … UE Security … IEI 46 … IEI 46 … Length 2	ion Of T equest a equest S mobili riminato der Type ntity 65 tion Typ > Initial dentity Capabilit bytes	The PD at 00:00 t ty mana r 14 => e 0 => F => Regi st Pend Registra	rect To One (:45.0037) gement Reserve Plain NAS stration I stration I	704 since messages d For Exte 6 message Request	connect ension Of 1	he PD To	× One O
Bi	 ➡ rrcSetupReq ➡ rrcSetup ➡ ue-ld ➡ ue-ld ➡ ue-ld ➡ ue-ld ➡ spare * Security Protected N ➡ EPD 7 => 5GS mol ➡ Protocol Discrimina ➡ Reserved OK ➡ Security Header Ty ➡ Message Authentic ➡ SEQUENCE_NUM ➡ SEQUENCE_NUM ➡ Registration Re 	Request lentity andom Value {3 pishmentCause a {1 bits 0x00 R NAS Message NAS Message bility management ator 14 => Rese ype 1 => Integrised bility management bility manageme	mo-Signalling ight Aligned} at 00:00:45.003 ge ent messages reved For Extens ty protected 6667B1A6 Registration Re Registration Re Reserved OSI Protocol Disc Reserved Nessage Ider ngKSI Sccurity Heac message Ider ngKSI SGS Registra Follow-on Type 1 =: SGS Mobile UE Security C IEI 46	704 sin ion Of T equest a s mobili riminato der Type neque leques leques leques s mobili der type neque lequest s mobili tion Type lequest ability	The PD at 00:00 t ty mana r 14 => e 0 => F => Regi st Pend Registra	rect To One (:45.0037) gement Reserve Plain NAS stration I stration I	704 since messages d For Exte 6 message Request	connect ension Of 1	he PD To	× One O

WaveJudge - [UMD_n41_IntelliJudge_NEA0_20230626_0845.rtphysap]

Figure 24: Unencrypted RRC messages

-	WaveJudge - [UMD_n41_IntelliJudge_N	EA0_20230626_0	J045.R	pitysap	1				
F	ile Edit View Actions Tools	Window H	elp						
1.1	🗶 🗽 🥕 🗋 🐸 📓 🗛 🕅 🖉	Cipher Judge	GPS: [) U: LT		□ FR •	*	I	// 🐖 1
E P	rocess Done			a .		rocess int			0 ms ①
1	Capture 📠 Repeat 🐘 IntelliJudge	ms	Trigg	ers »	Powe	er »>			
Ð	IntelliJudge								
Connect Type	Name Security Mode Complete	Start time		DI/UI	Cell #	Cell ID	Frame #	Slot #	RNTI
ect	Registration Request	00:00:45.218		ŭ	i	105	907	14	20074 -
- Lu	SecurityModeCommand	00:00:45.497	704	D	1	105	935	12	20074 -
0	UECapabilityEnquiry	00:00:45.497	704	D	1	105	935	12	20074 -
-	SecurityModeComplete	00:00:45.508		U	1	105	936	14	20074 -
	UECapabilityInformation	00:00:45.514		U	1	105	937	4	20074
Configure Chassis	DLInformationTransfer	00:00:45.524		D	1	105	938	6	20074 -
동	Security Protected NAS Message	00:00:45.524		D	1	105	938	6	20074 -
are	Registration Accept ULInformationTransfer	00:00:45.524		DU	1	105 105	938 939	6 4	20074 -
ığı	Security Protected NAS Message	00:00:45.533		Ŭ	1	105	939	4	20074 -
- ð	Registration Complete	00:00:45.533		ŭ	1	105	939	4	20074 -
-	DU C	00.00.45.535		š.	1	105		-	20074 -
	DL-DCCH-Message - message - c-1 - securityModeCommand - mc-TransactionIdentifier 0 - crticalExtensions - securityAddeCommand - securityAddeCommand - securityAddeCommand - securityAddeCommand - securityAddeCommand			- Prot		criminator	managem 14 => Rese		iges Extension (
		orithm nea0		- Mes SEG	sage Au UENCE		in Code 0x- R 1		ed and cipł
Bit L 000	id - securityConfigSMC id - securityAlgorithm 	onthm nea0 Algorithm nia2 704 since conner messages ed For Extension i S message, not s Accept	Bit Le	Mes	392 He 7E 0 13 4 00 0	ad 0111 2 48 2A 0 10 FF 0 02 15	n Code 0x R 1 4 1 11110 1	482A8FB	00011

Figure 25: Decipherable RRC messages when using NEA0

For the second part of the test, we set NEA2 as the first priority for RRC encryption for the RAN, as shown in Figure 26. Figure 27 and Figure 28 show WaveJudge windows indicating that, because the ciphering algorithm in use is NEA2, all the RRC and upper layer are security protected and the contents cannot be deciphered.

pheringAlgoPrio 2 1 0.	
2_566.28125.116_3317 stopfile=/tr	np/695942
cipheringAlgoPrio	Result
2,1,0	>>> Set.
2_566.28125.116_3317	np/695942
Attribute Value	
cipheringAlgoPrio i[3] = 2 1 0 integrityProtectAlgoPrio i[2] = cipheringAlgoPrio i[3] = 2 1 0	2 1 (EIA2 EIA1)

Figure 26: Setting RAN RRC encryption to NEA2

菅	WaveJudge - [UMD_n41_IntelliJudge_N	NEA2_20230626_0810.r	tphysap]	
F	ile Edit View Actions Tools	Window Help		
1.10	🛯 🗶 📙 🥕 🗅 🗀 😂 🔙 😓 🔖			
1.1		-		
: F	Process Done	1 😒	2 - 0	Process interval:
÷.	Capture In Repeat 101 IntelliJudge	ms Trigg	gers >> Po	wer >>
æ	IntelliJudge			
Connect Type	Name	Start time	DI/UI Cell	
ect	ULInformationTransfer	00:01:18.657735	U 1	105 573
E	Security Protected NAS Message	00:01:18.657735	U 1	105 573
8	Authentication Response DLInformationTransfer	00:01:18.657735 00:01:18.683735	U 1 D 1	105 573 105 576
_	Security Protected NAS Message	00:01:18.683735		105 576
~	Security Mode Command	00:01:18.683735		105 576
SSI	ULInformationTransfer	00:01:18.692735	U 1	105 577
ŝ.	Security Protected NAS Message	00:01:18.692735	ŭ i	105 577
æ	Unknown NAS	00:01:18.692735	Ū 1	105 577
<u> </u>	SecurityModeCommand	00:01:18.971235	D 1	105 605
Ē.	DLInformationTransfer	00:01:18.973735	D 1	105 605
_	SecurityModeComplete	00:01:18.987735	U 1	105 606
	DCCH-RRC	00:01:18.992735	U 1	105 607
st	DCCH-RRC	00:01:19.064235	D 1	105 614
÷-	SecurityModeComplete	00:01:19.072735	U 1	105 615
me	SecurityModeCommand at 00:01:13	8.971235 since connec	t	_
Chart Properties 🔢 Set up Capture 🔁 Configure Test 😮 Configure Chassis 📗		and MC		
opertie	PLInformationTransfer at 00:01:18.			
Chart Pr	DL-DCCH-Message , Data Underf Onessage One c1 One c1 One dInformation Transfer			
Ц	Padding/Extra Bytes , DataUnderflo	ow: Extra bytes at end of		je
	SecurityModeComplete at 00:01:18.	.987735 since connect		_
	UL-DCCH-Message			
	ie c1 ie securityModeComplete im rc-TransactionIdentifier	0		
	ecriticalExtensions	ete		

Figure 27: Protected RRC Messages

养	WaveJudg	o - FLIMD									
· ·	ile Edit	View	Actions	Tools	Window						
F	ie Edit					Help					
: 12	i 🗶 🔜	P 1	📂 🔛	😓 🗓	Cipher Judge	GPS:	🗆 U:			- m -	- 1
i P	rocess Don	e				1 🛛	2	- 🔘	Process in	terval:	
1	Capture	nn Repea	at 🔐 Inte	elliJudge	n	ns Trig	gers >	> Po	wer >>		
e e	IntelliJudg										
Connect Type		Na	ame		Start 1	time	DI/L	JI Cell	# Cell ID	Frame	#
De L		mationTra			00:01:18.		U	1	105	577	- 4
l S			d NAS Me	essage	00:01:18.		U	1	105	577	4
	Unknow	vn NAS /ModeCor	mmand		00:01:18.		D	1	105	605	4
		mationTra			00:01:18.		D	i	105	605	6
2019		ModeCor			00:01:18.	987735	Ū	1	105	606	1
Configure Chassis	DCCH-F				00:01:18.		U	1	105	607	4
2	DCCH-F				00:01:19.		D	1	105	614	7
l g		ModeCor	mplete		00:01:19.		U	1	105 105	615 633	4
Б.	DCCH-F				00:01:19.		D	1	105	678	1
\sim	DCCH-F				00:01:19.		ŭ	- i -	105	679	- i
\odot			ess Respo	nse	00:01:55.		Ď	i i	105	166	ō
88 D	CCH-RRC a				nest						
Ē		geClassExt	Error in s	subfield							
	·· message	geClassExt xtra Bytes	Error in s tension , Data Unde	subfield erflow: Ext	tra bytes at end	d of RRC	messa	ge			
* C	message message Padding/E CCH-RRC L-DCCH-N . message message	geClassExt at 00:01:1 dessage	Error in s tension , Data Unde 9.064235 : , Error in ktension	subfield erflow: Ext since cor subfield	tra bytes at end						
* C	- message - message - Padding/E DCCH-RRC - DCCH-RRC - message - message	geClassExt at 00:01:1 dessage ageClassEx Extra Bytes	Error in s tension , DataUnd 9.064235 : , Error in dension s , DataUnd	enflow: Ext since con subfield derflow: Ext at 00:01:	tra bytes at end nnect xtra bytes at en	id of RR(C messa				
* C	- message message Padding/E CCCH-RRC message mess	geClassExt xtra Bytes at 00:01:1 lessage , ageClassE Extra Bytes ityMode(CCH-Mes sssage c1 secu 	Error in a tension , Data Undo 9.064235 : , Error in dension , Data Undo Complete ssage , El mityModeCo rc-Transac priticalExter L. orticalExter	aubfield erflow: Ext since cor subfield defflow: E at 00:01: mor in su complete tionIdentifi nsions Statensions	tra bytes at end nnect ktra bytes at en 19.072735 sin abfield	d of RR(C messa ect	age		_	[
↑ □ ↑ □ □ □	I- message I- message I- Padding/1 DOCCH-RCC I- DOCCH-RCC I- DOCCH-RCC I- DOCCH-RCC I- Ressage I- Ressage	geClassExt txtra Bytes at 00:01:1 lessage geClassE txtra Bytes rityMode(C CCH-Mess ssage - c1 - c1 - cc - cc	Error in a tension , Data Undo 9.064235 : , Error in dension , Data Undo Complete ssage , El mityModeCo rc-Transac priticalExter L. orticalExter	aubfield erflow: Ext since cor subfield derflow: E at 00:01: mor in su pomplete tionIdentif sions Extensions Data Under	tra bytes at end nnect ktra bytes at en 19.072735 sin abfield ier 0 Future flow: Extra byte	d of RR(C messa ect	age			
3it Len 000000 000000	Inessage Inessage Padding/E CCH-RRC IL-DCCH-N Inessage Iness	geClassExt xtra Bytes at 00:01:1 lessage ageClassE Extra Bytes rityMode(CCH-Mes ssage - c1 - secu - secu - c1 - secu - c1 - secu - c1 - secu - secu - c1 - secu - s	Error in s tension , Data Undo 9.064235 ; Error in dension s , Data Undo Complete asage , Er antty ModeCo criticalExter ham criticalExter ham criticalExter a Bytes , E D1:19.7177 ge , Error	subfield erflow: Ext since cor subfield deflow: E at 00:01: mor in su pomplete tion/dentification Stensions DataUnder 35 since of in subfield	tra bytes at eno nnect ktra bytes at en 19.072735 sin abfield ier 0 iFuture filow: Extra byte connect	d of RR(ce conn es at end	C messa ect	sge C messa	ige		

Figure 28: Protected RRC Messages

Success Criteria:

RRC messages are observable over the RF channel when RRC encryption is disabled, and RRC messages are no longer observable when RRC encryption is enabled.

Results

Condition	Status
RRC messages are observable over the RF channel when RRC	Contents of RRC messages
encryption is disabled (through use of NEA0 algorithm)	are fully decipherable by
	WaveJudge
RRC messages are no longer observable when RRC	WaveJudge shows contents of
encryption is enabled (through use of NEA2 algorithm)	encrypted messages as "Extra
	bytes at end of RRC message"
Overall Test	Success

UMDMITREUser Equipment
(U)
User Plane
Confidentiality ProtectionNI
NI
S gNodeNI
NI
NI
S GNOdeEtcson RANEtcson SANEtcson SAN

Test Case 3: CSRIC 7 WG 3 – Access Stratum User Plane Confidentiality

Figure 29: Test Case SA-03 Configuration

Test Case ID: TC-SA-03

Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the user plane confidentiality, but optional for service providers to use. Given this standards requirement, CSRIC VII recommends user plane confidentiality protection over the access stratum be done at PDCP layer.

This test involves demonstrating that when confidentiality protection for the user plane is applied at the PDCP layer, no layers below PDCP are confidentiality-protected. User data sent via the UPF may be confidentiality protected.

This test also involves implementing and confirming user plane confidentiality protection over the access stratum at the PDCP layer. Layers below PDCP are not confidentiality-protected.

Test points used:

Used	Test Point	Description and Use
	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
Х	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

We were unable to capture user plane messages on the WaveJudge and, as a result, were unable to verify over-the-air encryption of user plane data.

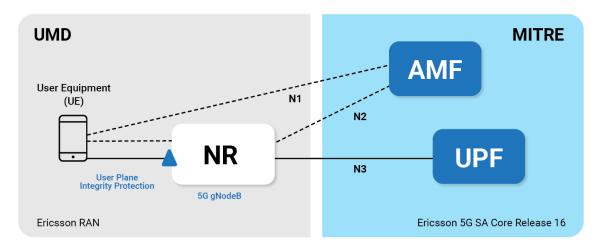
Success Criteria:

Once encrypted channel is established, user plane data will not be observable in the recorded data.

Confidentiality protection for the user plane is applied at the PDCP layer via 128-bit NEA algorithms.

Results

Condition	Status
When encryption is disabled, all UP data will be observable	Unable to capture user plane
	messages with WaveJudge
When the encrypted channel is established, UP data will not	Unable to capture user plane
be observable in the recorded data	messages with WaveJudge
Overall Test	Limited by Test Capability



Test Case 4: CSRIC 7 WG 3 – Access Stratum User Plane Integrity

Test Case ID: TC-SA-04 Description:

3GPP TS 33.501 requires UE to support integrity protection and replay protection of user data between the UE and the gNB, but the data rates at which it is supported are different between releases 15 and 16, and it is optional for service providers to use this feature.

CSRIC VII recommends that device OEMs and network infrastructure vendors support the Release 16 full rate capability, along with 128-NIA3 as defined in Annex D of 3GPP TS 33.501, and for operators to implement according to the service requirement. CSRIC VII recommends that user data integrity is mandatory for Release 16 U.S. deployments.

The Packet Data Convergence Protocol, as specified in TS 38.323 as between the UE and the NG-RAN, is responsible for user plane data integrity protection.

Figure 30: Test Case SA-04 Configuration

Test points used:

Used	Test Point	Description and Use			
	TP1-S	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop			
	TP1-MTP	TP1-MTPLaptop connected to Qualcomm MTP; QXDM allows access to low-level data			
Х	TP2	TP2 WaveJudge interface			
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)			
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"			
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"			
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC			
	TP7	CNOM tool accessing DMC messages			
	TP8	Applications running on application server in MITRE facility			

As with TC-SA-03, the WaveJudge/IntelliJudge was unable to capture user plane messages. As a result, we were unable to confirm over-the-air integrity protection. However, the PDU Establishment message, as shown in Figure 31, does indicate the intent to apply integrity protection at the full rate.

10.205.67.153 - Remote Desktop Connection

1	2 L / D 🖻 🖬 🕁 🖬	Capture III F	Repeat	⁰⁰₁ Inte	lliJudge	Cipher /////	dge GPS:	🗆 I): LTE 🗆 🚺 🎛 🕶 🖉
Pr	ocess Done	1	8 😂	- 0	Process	interval:		0 ms 🗅
e	IntelliJudge					Ð	£	
2	Name	Start time	DI/UI	Cell #	Cell ID	Frame #	Slot #	
art Properties 🌃 Set up Capture 🛃 Configure Test 🕥 Configure Chassis 📗 Connect Type	Name Security Protected NAS Message Registration Complete DLInformationTransfer Security Protected NAS Message Configuration Update Command ULInformationTransfer Security Protected NAS Message Uplink NAS Transport PDU Session Establishment Req RRCRelease RRCSetupRequest RRCSEtupReqUPRCS RRCSETUPRET RRCSETUPRET RRCSETUPRET RRCSETUPRET RRCSETUPRET	00:00:45:533704 00:00:45:533704 00:00:45:545204 00:00:45:545204 00:00:45:545204 00:00:45:728704 00:00:	U U D D U U U U U U U U U U U U U U U U	1 1 1 1 1 1 1 1 1 1 1 1 1 1	ported 0 = se	Frame # 939 940 940 958 958 958 958 958 958 958 958 958 958	Slot # 4 4 7 7 14 14 14 14 14 14 14 14 15 9D To One st tion for uplin	

Figure 31: WaveJudge capture of PDU Establishment message

Success Criteria:

Integrity protection for the user plane is applied full-rate at the PDCP layer.

Examine data collected by the RF monitoring tool for the user plane messages. Confirm the integrity check fields are populated.

Results

Condition	Status
Integrity protection for the user plane is applied full-rate at	PDU Establishment message
the PDCP layer	indicates integrity protection
	applied at full rate
Integrity check fields are populated	Unable to capture and read
	user plane messages over the
	air with WaveJudge
Overall Test	Limited by Test Capability

Test Case 5: CSRIC 7 WG 3 – SUPI/SUCI Privacy Enabled

Test Case ID: TC-SA-05-1

Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the SUPI/IMSI privacy; however, 3GPP allows for some exceptions where the Subscription Concealed Identifier (SUCI) may use the null scheme (i.e., the identity is not protected).

CSRIC VII recommends that devices and networks in the U.S. use IMSI privacy (SUCI) and not use the null scheme, except when the UE is requesting emergency services.

It is recommended that no other exceptions allowed by 3GPP in Release 16 (for null scheme SUCI) be used by devices or networks in the U.S. This may result in roaming 5G devices configured by operators from outside the U.S. being unable to connect to 5G SA networks, but that they use 4G LTE networks instead.

To avoid identifying a handset by its Subscription Permanent Identifier (SUPI), 5G uses the subscription concealed identifier (SUCI) to encrypt the SUPI to exchange identity information between the UE and 5G NR. SUPI/SUCI privacy is used for all services, except emergency services and non-authenticated roaming emergency calls.

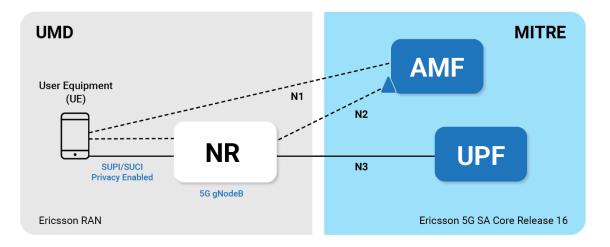


Figure 32: Test Case SA-05 Configuration

We used logs from CSRIC Test TC-SA-01 above, with highest priority set for NEA0 (null algorithm).

Test points used:

Used	Test Point	Description and Use
	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
Х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

Figure 33 shows the initial UE registration message in which the type of identity is SUCI. Figure 34 shows the uplink NAS transport message with registration request that also provides the type of identity as SUCI. Lastly, Figure 35 shows the downlink NAS transport message indicating the encryption algorithm to use is NEA0.

Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
II 🖉 🛛 🗀 🗋 🕱 🗳 🗣 🇯 🐨 🛊 🕎 📰 🔍 🔍 🍳 🍳 🦉	
80	
Time Source Destination Protocol Length	Info
101 2022-11-18 16:48:49 10.220.67 10.205.67 NGAP/NAS-5GS 182	InitialUEMessage, Registration request
103 2022-11-18 16:48:49 10.205.67 10.220.67 NGAP/NAS-5GS 142	DownlinkNASTransport, Authentication request
	UplinkNASTransport, Authentication response
	SACK (Ack=1, Arwnd=32768) , DownlinkNASTransport, Security mode command
	SACK (Ack=1, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration red
	SACK (Ack=2, Arwnd=32768) , DownlinkNASTransport, Security mode command
	SACK (Ack=2, Arwnd=16384) , UplinkNASTransport, Security mode complete
	InitialContextSetupRequest
	InitialContextSetupResponse
	UERadioCapabilityInfoIndication
	SACK (Ack=5, Arwnd=32768) , DownlinkNASTransport, Registration accept
.111 = NAS key set identifie	e: 7 0000 b0 27 cf 3e d4 06 58
SGS mobile identity	0010 08 00 45 a0 00 a4 00
SGS mobile identity Length: 54	0020 43 13 0a cd 43 cc 96
0 = Spare: 0	0030 5c 76 00 03 00 83 02
.000 = SUPI format; IMSI (0)	0040 00 3c 00 0f 40 6f 00
0 = Spare: 0	0050 31 10 00 26 00 43 42
001 = Type of identity: SUC	0060 10 f0 ff 02 0c 03 78
Mobile Country Code (MCC): United	0070 72 2T u7 a3 30 8a au
Mobile Network Code (MNC): TEST I	
Routing indicator: 0	0000 10 01 86 a2 12 d0 13
0010 = Protection scheme Id:	
Home network public key identifie	
	a7f2722fd7a3508aad12e3aa500508cea89cb781cc7e365b22f8a0_
	19cded0d7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc;
ECC ephemeral public key: 0378	19cded0d7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc;
ECC ephemeral public key: 0378 Ciphertext: 22f8a0614b	19cded0d7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc;
ECC ephemeral public key: 0378	19cded0d7f5a43a7f2722fd7a3508aad12e3aa500508cea89cb781cc;

Figure 33: UE with profile B – source core-side R6K

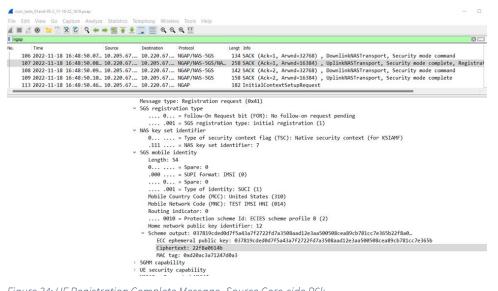


Figure 34: UE Registration Complete Message- Source Core-side R6k

csric_tests_01and-05-2_11-18-22_1610.pcap	-	
ile Edit View Go Capture Analy	ze Statistics Telephony Wireless Tools Help	
(🔳 🦪 🛛 🚞 🗎 🗙 🏹 🍕 🔶	* 🗯 🛪 🛓 🚍 🔳 🍳 🤤 🖽	
ngap		×
107 2022-11-18 16:48:50.08 108 2022-11-18 16:48:50.09	Source Destination Protocol Langl Info Lo. 200.567 10.220.67 NGAP/NAS-SGS 134 SACK (Ack=1, Arvmd=32768), DownlinklMASTransport, Security mode command Lo. 10.220.67 10.205.67 NGAP/NAS-SGS 134 SACK (Ack=1, Arvmd=16384), UplinklMASTransport, Security mode complete, Re Lo. 200.67 10.220.67 NGAP/NAS-SGS 142 SACK (Ack=2, Arvmd=32768), DownlinklMASTransport, Security mode command L. 10.220.67 10.205.67 NGAP/NAS-SGS 158 SACK (Ack=2, Arvmd=32768), DownlinklMASTransport, Security mode complete	gist
	Extended protocol discriminator: 56 mobility management messages (126) 0000 = Spare Half Octet: 0 0000 = Security header type: Plain NAS message, not security protected (0) Message type: Security mode command (0x5d) NAS security algorithms 0000 = Type of ciphering algorithm: 56-EA0 (null ciphering algorithm) (0) 0010 = Type of integrity protection algorithm: 128-56-124 (2) 00000 = Spare Half Octet: 0 NAS key set identifier - ngKSI 0.00 = HAS key set identifier: 0 UE security capability - Replayed UE security capabilities UESSUM - Spare bit(s): 0x00 001 = TWFESV request: INEESV requested (1) VIAS security algorithms - Selected EPS NAS security algorithms Element ID: 0x57 0 = Spare bit(s): 0x00 010 = Type of integrity protection algorithm: EPS integrity algorithm 128-ELA2 (2) Additional 55 security information	

Figure 35: NULL scheme in use - Source Core-side R6K

Success Criteria:

Successful registration with encrypted SUPI.

Results

Condition	Status
Use of SUCI by UE in registration process	Success
Successful registration	Success
Overall Test	Success

Test Case 6: CSRIC 7 WG 3 – IPsec on Transport Links

Test Case ID: TC-SA-06

Description:

3GPP TS 33.501 specifies mandatory (e.g., requires vendor support for) network security protection such as IPsec, but optional for service providers to use. Given this standards requirement, CSRIC VII recommends the use of IPsec or use of a tunneling technology for transport (e.g., VPN tunnels) for protection of network security.

This test involves demonstrating that when IPsec is used for confidentiality and integrity protection of user plane and signaling on the N1, N2, and N3 interfaces across the transport link, UP and CP traffic cannot be captured, modified, or injected with new packets.

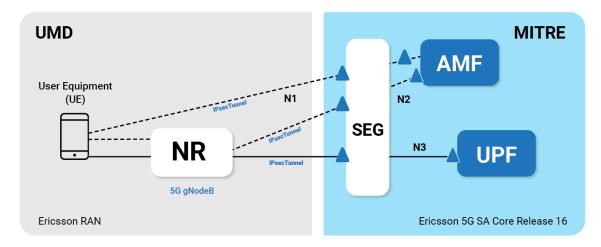


Figure 36: Test Case SA-06 Configuration

Test points used:

Used	Test Point	Description and Use
	TP1-SW	Wireshark running on laptop connected to Sierra Wireless card; captures packets originating at and destined to UE laptop
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
Х	TP3	Wireshark running on laptop connected to RAN-side R6K router; can capture packets inside the tunnel (encrypted packets when IPsec tunnel is enabled)
Х	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
Х	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
Х	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
	TP7	CNOM tool accessing DMC messages
	TP8	Applications running on application server in MITRE facility

Similar to the previous tests, Network Slice 2 and UE2 with profile B were used for this test. The UE used for Slice 2 was a Sierra Wireless Modem, which is connected and controlled by a laptop outside the Faraday Cage. IPsec for for Slice 2 and control traffic was turned on/off as and when required.

This test has two parts, attempting to capture, modify, and inject user and control plane traffic: 1) without an IPsec tunnel and 2) with an IPsec tunnel.

Part 1: Traffic Modification without Enabled IPsec Tunnel between BBU and Core-Side R6K For the first part of the test, we ensured that the IPsec tunnel for the transport channel between the RAN and the core was off.

The UE was then restarted and attached to the 5G core, as shown in Figure 37. The larger window in the figure shows the contents of an initial context setup request message captured on the untrusted transport between the RAN and core. The inset figure shows a message within the core regarding the registration of the UE with IMSI used for this test. Figure 38 shows logs of both control plane and user plane messages after UE registration and ping started to the DN server (192.168.59.146). These packets are clearly visible on the transport channel when the IPsec tunnel is down and traffic is unencrypted.

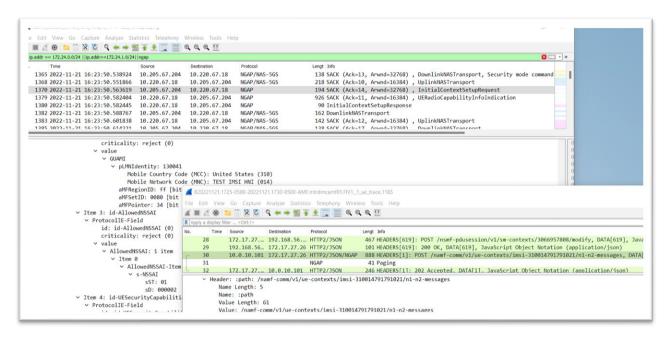


Figure 37: Packet captures at RAN-side switch and at the core showing UE registration over unencrypted transport

File Edit		re Analyze Statistic			
Current			arc == 128.8.46.80)) && !(eth.s		
lo.	Time	Source	Destination	Protocol	Length Info
12090	17:43:48.297457	10.220.67.18	10.205.67.204	SCTP	126 HEARTBEAT
12103	17:43:48.977029	10.220.67.18	10.205.67.204	NGAP/NAS-5GS/NAS	166 InitialUEMessage, Service request
12105	17:43:49.006529	10.220.67.18	10.205.67.204	NGAP	106 SACK (Ack=36, Arwnd=16384) , InitialContextSetupRespon
12109	17:43:49.062630	10.220.67.18	10.205.67.204	SCTP	62 SACK (Ack=38, Arwnd=16384)
12113	17:43:49.091145	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=336/20481, tt1=128
12114	17:43:49.092655	10.220.67.18	10.205.67.204	NGAP	110 PDUSessionResourceSetupResponse
12125	17:43:49.506190	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=337/20737, tt1=128
12144	17:43:50.497694	10.220.67.18	10.205.67.205	SCTP	126 HEARTBEAT
12148	17:43:50.526156	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=338/20993, tt1=128
12171	17:43:51.531162	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=339/21249, tt1=128
12189	17:43:52.571127	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=340/21505, tt1=128
12191	17:43:52.697440	10.220.67.18	10.205.67.204	SCTP	126 HEARTBEAT
12209	17:43:53.571175	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=341/21761, ttl=128
12228	17:43:54.591132	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	118 Echo (ping) request id=0x0001, seq=342/22017, tt1=128
12232	17:43:54.897701	10.220.67.18	10.205.67.205	SCTP	126 HEARTBEAT
10046	17.42.55 611007	170 04 1 0	103 169 50 146	GTD ATCHON	110 Erba (ning) namest id_000001

Figure 38: Ping messages captured on the untrusted transport link between the RAN and core

Subsequently, we used TP4, a laptop connected to the transport channel, to capture user plane traffic, modify that traffic, and inject it into the transport channel. The data captured was saved to a file (ping_111822.pcap), and we stopped pings from the UE. The modified data was injected using a laptop connected to the transport channel at the RAN-side switch (TP4), as shown in Figure 39Figure 39. To enhance the injection, the captured traffic is looped and replayed as quickly as possible using the loop and topspeed commands. Logs for the injected traffic are captured on the outgoing interface for the inject laptop (Figure 40), on the outgoing core-side R6K interface (Figure 41Figure 41), and in the ping responses displayed at the laptop connected to the UE (Figure 42).

F	daniel@daniel-Latitude-5520: ~/csric
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
aniel@daniel-Latitude-5520:~/csric\$ sudo tcpreplay ·	topspeed -i enp0s31f6 ping_111822.pcap
ctual: 122 packets (15456 bytes) sent in 0.000350 se	econds
ated: 44160000.0 Bps, 353.28 Mbps, 348571.42 pps	
tatistics for network device: enp0s31f6	
Successful packets: 122	
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
aniel@daniel-Latitude-5520:~/csric\$ sudo tcpreplay ·	
ctual: 122 packets (15456 bytes) sent in 0.000378 se	econds
ated: 408888888.8 Bps, 327.11 Mbps, 322751.32 pps	
tatistics for network device: enp0s31f6	
Successful packets: 122	
Failed packets: 0	
Truncated packets: 0	
Retried packets (ENOBUFS): 0	
Retried packets (EAGAIN): 0	
aniel@daniel-Latitude-5520:~/csric\$ sudo tcpreplay	
ctual: 122 packets (15456 bytes) sent in 0.000379 se	econds
ated: 40781002.6 Bps, 326.24 Mbps, 321899.73 pps	
tatistics for network device: enp0s31f6	
Successful packets: 122	
Failed packets: 0	
Truncated packets: 0 Retried packets (ENOBUFS): 0	
Retried packets (ENOBURS): 0 Retried packets (EAGAIN): 0	
aniel@daniel-Latitude-5520:~/csric\$	
ance (guance - Laccoude - 3520 - 7 car ics	

Figure 39: Injecting Unencrypted Captured Traffic – TP4 Laptop

ply.	a display filter <ctrl-></ctrl->									
	Time	Source	Destination		ength Info					
	1 2022-11-21 16:29:40.041038	172.24.1.2	192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, se				
		192.168.59.146	172.24.1.2	ICMP	60 Echo (ping) reply		eq=222/56832,)
		172.24.1.2	192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, se		a subsection of the second		
	4 2022-11-21 16:29:41.090242		172.24.1.2	ICMP	60 Echo (ping) reply		eq=223/57088,)
	5 2022-11-21 16:29:42.083563		192.168.59.146	ICMP	60 Echo (ping) request		eq=224/57344,	A DIA CONTRACT		
		192.168.59.146	172.24.1.2	ICMP	60 Echo (ping) reply		eq=224/57344,)
	7 2022-11-21 16:29:43.103313		192.168.59.146	ICMP	60 Echo (ping) request	id=0x0001, se				
	8 2022-11-21 16:29:43.190640	192.168.59.146	172.24.1.2	ICMP	60 Echo (ping) reply		eq=225/57600,			
	9 2022-11-21 16:29:44.122083		192.168.59.146	ICMP	60 Echo (ping) request		eq=226/57856,			
	10 2022-11-21 16:29:44.153991		172.24.1.2	ICMP	60 Echo (ping) reply		eq=226/57856,			
		172.24.1.2	192.168.59.146	ICMP	60 Echo (ping) request		eq=227/58112,			
	12 2022-11-21 16:29:45.169746	192 168 59 146	172.24.1.2	ICMP	60 Echo (ping) reply	id=0x0001, se	00-227/50112	++1-61 (n	and the design of the second s	

Figure 40: Injected outgoing traffic - Inject Laptop

Time	Source	Destination	Protocol	Length Info	
13 2022-11-21 17:33:19.098502	10.220.67.18	10.205.67.205	SCTP	130 HEARTBEAT	
14 2022-11-21 17:33:19.098679	10.205.67.205	10.220.67.18	SCTP	130 HEARTBEAT ACK	
15 2022-11-21 17:33:21.194222	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=227/58112, ttl=128 (no response fo	ound!
16 2022-11-21 17:33:21.194227	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=228/58368, ttl=128 (no response for	
17 2022-11-21 17:33:21.194229	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=229/58624, ttl=128 (no response for	ound!
18 2022-11-21 17:33:21.194230	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=230/58880, ttl=128 (no response for	ound!
19 2022-11-21 17:33:21.194232	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=231/59136, ttl=128 (no response for	ound!
20 2022-11-21 17:33:21.194235	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=232/59392, ttl=128 (no response for	ound!
21 2022-11-21 17:33:21.194236	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=233/59648, ttl=128 (no response for	
22 2022-11-21 17:33:21.194247	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=234/59904, ttl=128 (no response fo	
23 2022-11-21 17:33:21.194249	172.24.1.2	192.168.59.146	GTP <icmp></icmp>	122 Echo (ping) request id=0x0001, seq=235/60160, ttl=128 (no response fo	
24 2022-11-21 17:33:21.194251	172.24.1.2	192.168.59.146		122 Echo (ping) request id=0x0001, seq=236/60416, ttl=128 (no response fo	
25 2022-11-21 17:33:21.194253	172.24.1.2	192.168.59.146		122 Echo (ping) request id=0x0001, seq=237/60672, ttl=128 (no response fo	ound!
	172.24.1.2	239,255,255,250	GTD /SSDD>	265 M-SEARCH * HTTP/1.1	
26 2022-11-21 17:33:21.194280 27 2022-11-21 17:33:21.194282	172.24.1.2	192.168.59.146		122 Echo (ping) request id=0x0001, seq=238/60928, ttl=128 (no response fo	

Figure 41: Injected received traffic at core-side R6K

	🖉 🙁 🚞 🖺 🗶 🖛 🖷	* * * 🗶 💻		1 11							
Apply	y a display filter <ctrl-></ctrl->										
D.	Time	Source	Destination	Protocol	Length	Info					
	1 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)			seq=233/59648,	
	2 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)			seq=234/59904,	
	3 2022-11-21 17:33:21.630998	192.168.59.146	and the second se	ICMP		And a state of the second state of the	(ping)			seq=235/60160,	
	4 2022-11-21 17:33:21.630998	192.168.59.146		ICMP			(ping)		the second s	seq=236/60416,	
	5 2022-11-21 17:33:21.630998	192.168.59.146		ICMP			(ping)			seq=237/60672,	
	6 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=238/60928,	ttl=61
	7 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)			seq=239/61184,	
	8 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)			seq=240/61440,	
	9 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)		id=0x0001,	seq=241/61696,	ttl=61
	10 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=242/61952,	ttl=61
	11 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply		seq=243/62208,	
	12 2022-11-21 17:33:21.630998	192.168.59.146		ICMP			(ping)			seq=244/62464,	
	13 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=245/62720,	ttl=61
	14 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=246/62976,	ttl=61
	15 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=247/63232,	ttl=61
	16 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP			(ping)		id=0x0001,	seq=248/63488,	ttl=61
	17 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=249/63744,	ttl=61
	18 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=250/64000,	ttl=61
	19 2022-11-21 17:33:21.630998	192.168.59.146	172.24.1.2	ICMP	60	Echo ((ping)	reply	id=0x0001,	seq=251/64256,	ttl=61
	20 2022-11-21 17:33:21.630998	192.168.59.146		ICMP			(ping)			seq=252/64512,	
	21 2022 11 21 17.22.21 62000	100 100 50 140	170 04 1 0	TCHO	~~	raha /	(1	11 0.0001	252/64760	++1 C4

Figure 42: Injected traffic received at UE laptop

Part 2: Traffic Modification with Enabled IPsec Tunnel between BBU and Core-Side R6K

In the second part of the experiment, we turned on IPsec. As above, from the UE laptop, we issued continuous ping messages and captured packets on both the UE and the core-side R6K. Figure 44 shows packet captures of ping traffic outside the tunnel: at the UE and on the egress of the core-side R6K. These messages were not visible on the transport channel, only appearing as ESP packets. The encrypted packets were captured on the transport channel using the laptop connected to TP4. The messages were then modified and injected into the transport channel as shown in Figure 43.

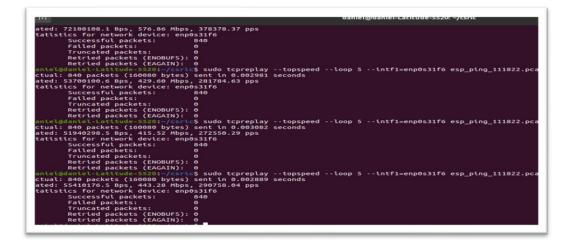


Figure 43: Injecting Encrypted Captured Traffic – TP4 Laptop

Test Results for 5G STB – CSRIC-Inspired SA Use Cases

CSRIC_test06	5-prt2_ipsec_UE2-laptop_11-21-22_1800.pcapng						_	- ×	
e Edit Viev	w Go Capture Analyze Statistics Tel	ephony Wireless Tools	Help						
	ے جے جے ای 🖾 🛣 📄 😑	🛃 📃 🔳 🔍	Q Q 11						
icmp							×	+	
Tin	ne	Source	Destination	Protocol	Length Info				
121 20	22-11-21 18:02:19.122127	172.24.1.3	192.168.59.146	ICMP	60 Echo (pi	ng) request	id=0x0001, s	eq=	1
122 20	22-11-21 18:02:19.158019	192.168.59.146	172.24.1.3	ICMP	60 Echo (pi	ng) reply	id=0x0001, s	eq-	
123 20	22-11-21 18:02:20.141664	172.24.1.3	192.168.59.146	ICMP	60 Echo (pi	ng) request	id=0x0001, :	eq=	
124 20	22-11-21 18:02:20.172928	192.168.59.146	172.24.1.3	ICMP	60 Echo (pi	ng) reply	id=0x0001, s	eq=	
	22-11-21 18:02:21.150127	172.24.1.3	192.168.59.146	ICMP	60 Echo (pi				
	22-11-21 18:02:21.167039	192.168.59.146	172.24.1.3	ICMP	60 Echo (pi		id=0x0001, s		
	22-11-21 18:02:22.169475	172.24.1.3	192.168.59.146	ICMP	60 Echo (pi				
	22-11-21 18:02:22 198250	192 168 59 146	172 24 1 3	TCMP	60 Echo (ni	ng) renly	id=avaaa1 a	eas	
129 20		0.pcap						_	
130 20		e Statistics Telephony	Wireless Tools Help						
131 20				2727					
132 20	📶 🔳 🖉 🐵 🚞 🗋 🛣 🖉	• 🖛 🖚 🚈 🔶 💌		. 10					
	gtp								\times
Frame 1: 6	No. Time	Source	e Desti	nation	Protocol L	ength Info			
Raw packet	5 2022-11-21 18:01:14.309	211 172.	24.1.3 192	168.59.146	GTP <ic< td=""><td>122 Echo (</td><td>ping) request</td><td>id=0x000</td><td>1, seq</td></ic<>	122 Echo (ping) request	id=0x000	1, seq
Internet F	6 2022-11-21 18:01:14.309	516 192.	168.59.146 172	24.1.3	GTP <ic< td=""><td>122 Echo (</td><td>ping) reply</td><td>id=0×000</td><td>1, seq</td></ic<>	122 Echo (ping) reply	id=0×000	1, seq
Internet (7 2022-11-21 18:01:15.329	194 172.	24.1.3 192	168.59.146	GTP <ic< td=""><td>122 Echo (</td><td>ping) request</td><td>id=0x000</td><td>1, seq</td></ic<>	122 Echo (ping) request	id=0x000	1, seq
	8 2022-11-21 18:01:15.329	446 192.	168.59.146 172	24.1.3	GTP <ic< td=""><td>122 Echo (</td><td>ping) reply</td><td>id=0x000</td><td>1, seq</td></ic<>	122 Echo (ping) reply	id=0x000	1, seq
	11 2022-11-21 18:01:16.349	980 172.	24.1.3 192	168.59.146	GTP <ic< td=""><td>122 Echo (</td><td>ping) request</td><td>id=0x000</td><td>1, seq</td></ic<>	122 Echo (ping) request	id=0x000	1, seq
	12 2022-11-21 18:01:16.349			24.1.3	GTP <ic< td=""><td></td><td>ping) reply</td><td>id=0x000</td><td></td></ic<>		ping) reply	id=0x000	
	13 2022-11-21 18:01:17.359	156 172.	24.1.3 192	168.59.146	GTP <ic< td=""><td>122 Echo (</td><td>ping) request</td><td>id=0x000</td><td>1, seq</td></ic<>	122 Echo (ping) request	id=0x000	1, seq
	14 2022-11-21 18:01:17.359	427 192.	168.59.146 172	24.1.3	GTP <ic< td=""><td></td><td>ping) reply</td><td>id=0x000</td><td></td></ic<>		ping) reply	id=0x000	
	17 2022-11-21 18:01:18.374			168.59.146	GTP <ic< td=""><td></td><td>ping) request</td><td></td><td></td></ic<>		ping) request		
	18 2022-11-21 18:01:18.374	295 192.	168.59.146 172	24.1.3	GTP <ic< td=""><td></td><td>ping) reply</td><td>id=0x000</td><td></td></ic<>		ping) reply	id=0x000	
	19 2022-11-21 18:01:19.394	799 172.	24.1.3 192.	168.59.146	GTP <ic< td=""><td>122 Echo (</td><td>ping) request</td><td>id=0x000</td><td>1. sea</td></ic<>	122 Echo (ping) request	id=0x000	1. sea

Figure 44: Ping traffic from UE laptop and egress of core-side R6K

The logs for injected packets were captured from the outgoing interface of the inject laptop at TP4 as shown in Figure 45. As observed, only ESP packets were captured. To distinguish between the actual ESP packets flowing through the encrypted tunnel from the modified injected ESP packets, we used the loop and topspeed commands to attempt to inject a high volume of ESP packets (2,490 packets) as quickly as possible.

Edit View Go Capture Analyze Statistics	lelephony Wireless lool	s Help				
🔳 🖉 😳 🚞 🛅 🔀 🌀 🔍 🖛 🌩 警	T 🛃 📃 🗨	e, e, 🎹				
sp						\times \rightarrow
Time	Source	Destination	Protocol	Length Info		
7 2022-11-21 18:13:26.762299107	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
8 2022-11-21 18:13:26.762310383	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
9 2022-11-21 18:13:26.762313377	10.220.67.18	10.205.67.200	ESP	202 ESP	(SPI=0xc3308779)	
10 2022-11-21 18:13:26.762316162	10.205.67.200	10.220.67.18	ESP	202 ESP	(SPI=0x1d2c0196)	
11 2022-11-21 18:13:26.762318909	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
12 2022-11-21 18:13:26.762321653	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
13 2022-11-21 18:13:26.762324272	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
14 2022-11-21 18:13:26.762326880	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
15 2022-11-21 18:13:26.762329431	10.220.67.18	10.205.67.200	ESP	202 ESP	(SPI=0xc3308779)	
16 2022-11-21 18:13:26.762332472	10.205.67.200	10.220.67.18	ESP	202 ESP	(SPI=0x1d2c0196)	
17 2022-11-21 18:13:26.762335136	10.220.67.18	10.205.67.200	ESP	186 ESP	(SPI=0xc3308779)	
18 2022-11-21 18:13:26.762337900	10.205.67.200	10.220.67.18	ESP	186 ESP	(SPI=0x1d2c0196)	
Identification: 0x0073 (115) > 000 = Flags: 0x0 0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 63 Protocol: Encap Security Payload (50) Header Checksum: 0xde06 [validation diss [Header checksum status: Unverified] Source Address: 10.220.67.18						
Destination Address: 10.205.67.200						
Encapsulating Security Payload						
ESP SPI: 0xc3308779 (3274737529) ESP Sequence: 711						



As shown in Figure 46, none of the injected packets or their decrypted version makes through to the UE or MITRE R6K during the test. Once the IPsec tunnel is established, traffic to and from the UE to the 5G core is encrypted, and it's not possible to see the contents of the messages. Even though it is possible to capture ESP packets, their contents are encrypted and unreadable, and when packets are modified and injected, they are dropped from either end of the tunnel end-points.

y a display filter <ctrl-></ctrl->						
Time	Source	Destination	Protocol	Length Info		
1 2022-11-21 18:14:38.031828	172.24.1.3	239.255.255.250	SSDP		H * HTTP/1.1	
2 2022-11-21 18:14:39.037248	172.24.1.3	239.255.255.250	SSDP		H * HTTP/1.1	
3 2022-11-21 18:14:40.055848	172.24.1.3	239.255.255.250	SSDP		H * HTTP/1.1	
4 2022-11-21 18:14:41.063101	172.24.1.3	239.255.255.250	SSDP	203 M-SEARC	H * HTTP/1.1	
csric_test_06_prt2_mitreR6K_11-21-22_18 File Edit View Go Capture Analy		'ireless Tools Help				-
Apply a display filter < Ctrl-/>	९ 🖛 🏓 🖺 🖉 보 📃		**			
No, Time	Source	Destin	-F	Protocol	Length Info	
88 2022-11-21 18:14:17.13			ation 20.67.19	SCTP		
89 2022-11-21 18:14:17.13			20.67.19	SCTP	130 HEARTBEAT_ACK 130 HEARTBEAT	
90 2022-11-21 18:14:19:33			20.67.19	SCTP	130 HEARTBEAT ACK	
91 2022-11-21 18:14:20.05			20.67.19	SCTP	130 HEARTBEAT	
92 2022-11-21 18:14:20.05			05.67.204	SCTP	130 HEARTBEAT ACK	
93 2022-11-21 18:14:21.53			05.67.205	SCTP	130 HEARTBEAT	
94 2022-11-21 18:14:21.53			20.67.19	SCTP	130 HEARTBEAT ACK	
95 2022-11-21 18:14:23.73			05.67.204	SCTP	130 HEARTBEAT	
96 2022-11-21 18:14:23.73			20.67.19	SCTP	130 HEARTBEAT ACK	
97 2022-11-21 18:14:25.93			05.67.205	SCTP	130 HEARTBEAT	
98 2022-11-21 18:14:25.93			20.67.19	SCTP	130 HEARTBEAT ACK	
99 2022-11-21 18:14:28.13			05.67.204	SCTP	130 HEARTBEAT	
100 2022-11-21 18:14:28.13			20.67.19	SCTP	130 HEARTBEAT ACK	
CSRIC_ 101 2022-11-21 18:14:30.33	10.220	.67.19 10.2	05.67.205	SCTP	130 HEARTBEAT	
			20.67.19	SCTP	130 HEARTBEAT ACK	
				SCTP	130 HEARTBEAT	
102 2022-11-21 18:14:30.33 103 2022-11-21 18:14:32.53		.67.19 10.2	05.67.204			
102 2022-11-21 18:14:30.33	3584 10.220		05.67.204 20.67.19	SCTP	130 HEARTBEAT ACK	
102 2022-11-21 18:14:30.33 103 2022-11-21 18:14:32.53	3584 10.220 3732 10.205	.67.204 10.2			130 HEARTBEAT_ACK 130 HEARTBEAT	

Figure 46: Observed Packets at UE and MITRE R6K after Injecting Packets on Encrypted Transport Channel

Success Criteria:

- 1. Unable to eavesdrop on UP and CP traffic across the transport link
- 2. Unable to modify UP and CP traffic across the transport link
- 3. Unable to inject UP and CP traffic across the transport link

Results

Condition	Status
Unable to eavesdrop on UP and CP traffic across	Success
the encrypted transport link	
Unable to modify UP and CP traffic across the	Success
encrypted transport link	
Unable to inject UP and CP traffic across the	Success
encrypted transport link	
Overall Test	Success

Test Case 7: CSRIC 7 WG 3 – Transport Layer Security for SBA Interfaces

Test Case ID: TC-SA-07

Description:

3GPP TS 33.501 specifies mandatory (e.g. requires vendor support for) transport layer security, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends the application of TLS for SBA interfaces and tunneling technology for transport when not using the SBA.

This test involves demonstrating that when TLS is used to provide protection for SBA interfaces in the 5G core, data packets cannot be captured, modified, or injected on the SBA interface.

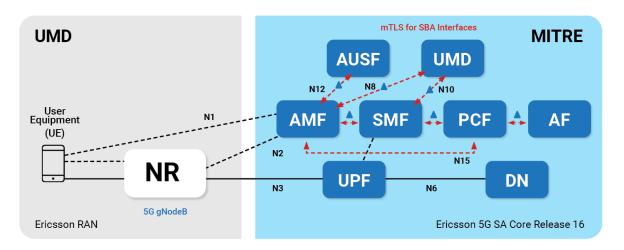


Figure 47: Test Case SA-07 Configuration

Test points used:

Used	Test Point	Description and Use
	TP1	Laptop connected to Sierra Wireless card and/or software-defined radio (SDR); Wireshark captures packets originating at and destined to UE laptop; other tools access SDR controls and data
	TP1-MTP	Laptop connected to Qualcomm MTP; QXDM allows access to low-level data
	TP2	WaveJudge interface
	TP3	Wireshark running on laptop connected to RAN-side R6K router; can be configured to capture packets outside the tunnel (i.e., before IPsec encryption or after IPsec decryption) or inside the tunnel (encrypted packets when IPsec tunnel is enabled)
	TP4	tcpdump running on laptop connected to port of RAN-side Pluribus switch used to capture, modify, and inject packets on the "untrusted link"
	TP5	tcpdump running on port of core-side R6K router inside the IPsec tunnel (encrypted packets when IPsec tunnel is enabled) used to monitor packets on the "untrusted link"
	TP6	tcpdump running on port of core-side R6K router outside the IPsec tunnel (i.e., before IPsec encryption or after IPsec decryption) used to monitor packets at the interface to the DMC
Х	TP7	CNOM tool accessing DMC messages, Ericsson transparent TCP proxy tool
	TP8	Applications running on application server in MITRE facility

This test case is comprised of two parts. For Part 1, the 5G core SBA network function (NF) interfaces are not configured with mutual transport layer security (mTLS)—rather, they utilize HTTP2. In Part 2, the 5G core SBA interfaces are configured with mTLS. Table 3 lists the mapped IP addresses used by the various NFs used for the SBA interfaces. Due the nature of the 5G core setup, some NFs (e.g., AMF) communicated on multiple IP addresses.

AMF	NRF	AUSF	UDM	SMF	TCP Proxy
172.17.152.165	192.168.56.143	192.168.56.138	192.168.56.137	192.168.56.129	172.17.208.251
172.17.95.197	192.168.56.143			192.168.56.131	
172.17.27.33					
172.17.152.146					
172.17.13.136					

Table 3: Network Function IP Addresses

For modification and insertion of traffic on the SBA interfaces, we used an Ericsson-provided TCP Layer Proxy Tool. The Proxy Tool was inserted between the various NFs and had the ability to intercept messages from producer (NRF) and its client, as shown in

Figure 48.



Figure 48: TCP Layer Proxy Setup

As shown in Figure 49, services requests (e.g., the GET operation) are made through the TCP Proxy Tool, where in this figure we have highlighted the AMF (172.17.152.146) requesting services from the TCP Proxy (172.17.208.251) using port 8080.

eam eq 4						
Time	Source	Destination	Protocol	Source Port E		
99 125.593716	172.17.152.146	172.17.208.251	HTTP2	43137	8080	124 Magic, SETTINGS[0], WINDOW_UPDATE[0]
100 125.593721	172.17.208.251	172.17.152.146	TCP	8080 4		72 8080 → 43137 [ACK] Seq=1 Ack=53 Win=62720 Len=0 TSval=973056555 TSecr=710274034
119 125.594785	172.17.208.251	172.17.152.146	HTTP2	8080 4		127 SETTINGS[0], SETTINGS[0], WINDOW_UPDATE[0]
121 125.594852	172.17.152.146	172.17.208.251	TCP	43137		72 43137 → 8080 [ACK] Seq=53 Ack=56 Win=62720 Len=0 TSval=710274036 TSecr=973056556
124 125.594928	172.17.152.146	172.17.208.251	HTTP2	43137		81 SETTINGS[0]
125 125.594931	172.17.208.251	172.17.152.146	TCP	8080 4		72 8080 → 43137 [ACK] Seq=56 Ack=62 Win=62720 Len=0 TSval=973056556 TSecr=710274036
149 125.622963	172.17.152.146	172.17.208.251	HTTP2	43137		188 HEADERS[1]: GET /nnrf-disc/v1/nf-instances?service-names=nudm-uecm&target-nf-type=UDM&requester-nf-type
150 125.622974	172.17.208.251	172.17.152.146	TCP	8080 4		72 8080 → 43137 [ACK] Seq=56 Ack=178 Win=62720 Len=0 TSval=973056584 TSecr=710274064
155 125.625225	172.17.208.251	172.17.152.146	HTTP2/JSON	8080 4		1463 HEADERS[1]: 200 OK, DATA[1], JavaScript Object Notation (application/json)
156 125.625302	172.17.152.146	172.17.208.251	TCP	43137		72 43137 → 8080 [ACK] Seq=178 Ack=1447 Win=61440 Len=0 TSval=710274066 TSecr=973056587
183 167.836927	172.17.152.146	172.17.208.251	HTTP2	43137		173 HEADERS[3]: GET /nnrf-disc/v1/nf-instances?service-names=nausf-auth&target-nf-type=AUSF&requester-nf-ty
184 167.836944	172.17.208.251	172.17.152.146	TCP	8080 4		72 8080 → 43137 [ACK] Seq=1447 Ack=279 Win=62720 Len=0 TSval=973098798 TSecr=710316278
189 167.839393	172.17.208.251	172.17.152.146	HTTP2/JSON	8080 4	\$3137	1223 HEADERS[3]: 200 OK, DATA[3], JavaScript Object Notation (application/json)
Represen Index: 6 V Header: :pat Name Len Name: :p Value Le	:h: /nnrf-disc/v1/nf- gth: 5 ath ngth: 117	instances?service-nam				requester-nf-type=ANF¹=ims1-310014791791001

Figure 49: Wireshark Capture of TCP Layer Proxy Communication with Network Functions

Part 1: Unencrypted SBA Interfaces

Tests for Part 1 were performed on February 27, 2023. There are three subparts to this test: (1) eavesdropping on SBA interfaces, (2) packet modification, and (3) packet injection.

<pre>=== mtrdmcamf01 erv@eric-pc-mm-controller-0 A</pre>	NCB ~ # gsh get_subscriber -imsi 310014791791001
Subscriber Data	
THE T	
IMSI Mahila Cubaaribaa ICDU Na	: 310014791791001
Mobile Subscriber ISDN No.	: 7917910001
IMEI	: 004403160428990
Radio Access Technology	: NGRAN
Mobility Management State	: RM-DEREGISTERED CM-IDLE
Time of Registration in AMF	
Time released	
RAT restrictions	: [EUTRA]
Forbidden areas	: []
	: Information not available
	: Information not available
Service area restriction	
Restriction type	: NOT_ALLOWED_AREAS
TACs	: []
Max num. of TAs	: Information not available
Security Context State	: Security Context without Secure exchange
5GMM Capability	: Information not available
In MICO Mode	: No
en rissiscence into the interite to no four	: false
Paging Proceed Flag	:
Last Visited Tracking Area [TAI]	:
Tracking Area List	:
Latest NG-RAN Node List (MCC-MNC-Size-gNBId)	: 001-001-24-100002
IMS VoPS	: Not supported
SMS over NAS Allowed	: false
Subscribed S-NSSAIs	
Default S-NSSAIs	: 1-1
Non Default S-NSSAIs	:
Registered S-NSSAIs	:
5G-GUTI	
PLMN Id	310-014
AMF Region Id	: 255
AMF Set Id	: 2
AMF Pointer	: 13
5G-TMSI	: 3758407710 (#E004C01E)
and the second	

Figure 50: SA-07 Subscriber details from MITRE 5G Core

Figure 51 shows both the UE trace files and the combined ITC trace files including similar traffic flows with NAS messages and SBA interface messages. In addition, the ITC trace file shows TCP handshakes on the SBA interface: HTTP2 SETTINGs and DATA frame messages.

From these captures, we can clearly read the messages on the SBA interface. Specifically, as shown in Figure 52 and Figure 53, we can eavesdrop on the TCP handshakes and HTTP2 frames messages through, during, and after the UE initial registration process. Looking deeply into HTTP2 HEADER frame messages we see that at Packet 448, the AMF requests AUSF services from NRF through an HTTP2 HEADERS GET frame. These messages expose multiple AMF IP addresses (172.17.152.146, 172.17.95.197, 172.17.27.33, and 172.17.152.165) through the establishment of successful TCP handshakes between other NFs such as NRF (192.168.56.143), SMF (192.168.56.129), AUSF (192.168.56.138), and UDM (192.168.56.137), as well as UE details such as the SUPI (IMSI: 310014790791001), all visible in Figure 53.

Test Results for 5G STB – CSRIC-Inspired SA Use Cases

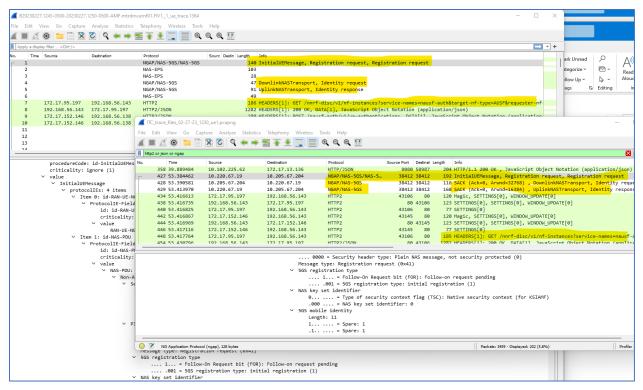


Figure 51: Test Case SA-07 traffic flows for combined ITC and UE trace files

📕 ІТС <u>.</u>	_trace_files_02-27-23	1230_ue1.pcapng			
File E	dit View Go C	apture Analyze Statist	ics Telephony Wireles	s Tools H	elp
	1 💿 🚞	े 🔀 🏹 🔍 🗰 🗉	• 🖭 🕌 보 📃 🛛	• •	e, III
(tcp.f	flags.syn==1 and tcp.flag	gs.ack==1) && !(ip.src == 10.10)2.225.62)		
No.	Time	Source	Destination	Proto: Lengt	th Info
	431 53.416362	192.168.56.143	172.17.95.197	TCP	76 80 → 43106 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=672073434 TSecr=1379474035 WS=256
	570 54.047591	192.168.56.129	172.17.27.33	TCP	76 7070 → 43075 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=131081165 TSecr=110021449 WS=256
	461 53.433648	192.168.56.138	172.17.27.33	TCP	76 80 → 43077 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=4251342230 TSecr=144785766 WS=256
	561 54.046910	192.168.56.129	172.17.152.165	TCP	76 7070 + 43049 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=3339134728 TSecr=1907729930 WS=256
	459 53.433593	192.168.56.138	172.17.152.146	TCP	76 80 → 43137 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=658490094 TSecr=2367796144 WS=256
	436 53.416663	192.168.56.143	172.17.152.146	TCP	76 80 → 43145 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=907850761 TSecr=612013779 WS=256
	3295 361.836579	172.17.152.146	10.0.10.115	TCP	76 8080 → 49744 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=2422291602 TSecr=1714658740 WS=256
	588 54.261012	172.17.152.165	10.0.10.115	TCP	76 8080 → 31351 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=3011720040 TSecr=1997809008 WS=256

Figure 52: Test Case SA-07 with no mTLS – AMF and other SBA NFs TCP Handshake, Source combined ITC trace file

Name: : path 0000 45 n0 00 nº ea a6 Value: /mmf-disc/v1/nf-instances?service-names-naust value: /mmf-disc/v1/nf-instances?service-names-naust Path sub segment: service-names-naust Path sub segment: service-names-naust Path sub segment: service-names-naust Path sub segment: service-names-naust Path sub segment: service-names-naust SM	449
449 53,416748 112,17,95,197 122,168,56,143 TCP 43186 89 66,43186 + 00 [ACK] Seq-53 Ack-56 kin-62728 Lene T Sval-1379474936 Steer-672873435 440 53,416748 122,17,95,197 122,168,56,143 172,17,95,197 TCP 69 43186 69 C4 4316 C4 43	449 0 0 0 47 07 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
440 53.416825 172.17.95.197 192.166.56.143 117.17.95.197 192.166.56.143 172.17.95.197 192.166.56.143 172.17.95.197 192.166.56.143 172.17.95.197 192.166.56.143 172.17.95.197 192.166.56.143 172.17.95.197 192.166.56.143 172.17.95.197 192.166.56.143 172.17.95.197 172.16.95.143 172.17.97.49.195.197.49.196.196.196.196.196.196.196.196.197.197.197.197.197.197.197.197.197.197	449 0 0 0 47 07 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
441 53.416346 192.168.56.143 172.17.55.197 TCP 80 43106 68 80 + 43196 (Arc)) 5ce-56.8cbc62 Minds2228 Long. TSuLa6720212435. Tseewei379474635 448 53.417760 192.168.56.143 172.17.55.197 TCP 80 43106 65 80 + 43196 (Arc)) 5ce-56.8cbc4278 Long. TSuLa6720212435. Tseewei379474635 449 53.417760 192.168.56.143 172.17.55.197 TCP 80 43106 55 80 + 43106 (Src) 5cc+57.8cbc179 Min.52720 Long. TSuLa672071436 (Src) 5cc+37.9474635 455 53.48076 192.168.56.143 172.17.55.197 HTTP2/JSON 80 43106 55 80 + 43106 (Src) 5cc+57.8cbc179 Min.52506 Long. TSuLa15794740635 455 53.480876 192.168.56.143 172.17.59.197 HTTP2/JSON 80 43106 1282 HEADERS[1]: 200 0K, DATA[1], JavaScript Object Notation (application/json) 455 53.480876 192.175.474563 152.174574563 15	449 0 0 0 47 07 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
448 53.417764 172.17.95.197 192.168.55.143 HTTP2 43106 80 4310 105 HADDR5(1)[1] 105 Interaction (1) Interaction (1	449 0 0 0 47 07 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
449 53.419790 132.163.65.143 172.17.95.197 TCP 88 43166 66 88 + 43166 TCP 804366 122.163.65.143 172.17.95.197 TCP 844366 122.146.26.117 116.62720 140.117 140	449 0 0 0 47 07 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
454 53.349796 122.168.56.143 172.17.56.197 HTTP2/250N 88 43166 1282 HEADERS[1] 202 '26' 05, DATA[1], JavaScript Object Motation (application/json) 455 53.48976 127 Life Script Data (Script Object Motation (application/json) 455 53.48976 127 Life Script Data (Script Object Motation (application/json) 455 53.48976 127 Life Script Data (Script Object Motation (application/json) 455 53.48976 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application/json) 456 55 127 Life Script Data (Script Object Motation (application) 457 Life Script Data (Script Object Motation) 457 Life Script Data (Scrip	449 0e a7 97 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
455 55,438013 127,127,95,197 192,165,56,143 TCP 43166 80 66 43166 + 30 [ACC] Seq-179 ACx-1270 Min-61696 Len-0 Tsval-137347496 TScc-r-6720734 Name Length: 5 Name Length: 19 9000 400 A 400 A 10 A 00 A 400 A 10 A 00 A 2 A 45 100 A 2 A 400 A 10 A 10 A 2 A 45 Value Length: 19 Value Length: 19 9000 400 A 400 A 10 A 10 A 2 A 45 Path sub segment: /nnrt-disc/1/1/nf-instances Path sub segment: service-names-mausf Mit HTTP2A Path sub segment: service-names-mausf Pit HTTP2A SH	0e a7 97 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
Name Length: 5 Name Longth: 10 Value Longth: 10 Path sub segment: Longth: 10	0e a7 97 be b9 88 00 00 08 00 40 00 40 06 49 fa ac 11 5f c5
Name: : path 0010 45 00 00 0 e a 65 Value Length: 119 Value Length: 119 Value /umf-disc/v1/nf-instances?service-names-nausf Path sub segment: /norf-disc/v1/nf-instances Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth	40 00 40 06 49 fa ac 11 5f c5
Name: : path 0010 45 00 00 0 e a 65 Value Length: 119 Value Length: 119 Value /umf-disc/v1/nf-instances?service-names-nausf Path sub segment: /norf-disc/v1/nf-instances Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth	40 00 40 06 49 fa ac 11 5f c5
Value Length: 119 Value Length: 119 Value Length: 119 Value Length: 119 Value Length: 107-dis/V1/nf-instances?service-names-nausf Path sub segment: service-names-nausf-auth Path sub segment: service-names-nausf-auth segment Segment service-names-nausf-auth segment Segment segment segment Segment segment segment Segmen	
v: joth:://mrf-disc/v1/nf-instances/set v1/e*name=-naus/ Path segment::/nnrf-disc/v1/nf-instances Path sub segment::service-name=-nausf-auth SM	
Path segment: /nnrf-disc/v1/nf-instances PRL*HTP20 Path sub segment: service-names-nausf-auth Path sub segment: ingre-inf-type-MJSF	
Path sub segment: service-names-nausf-auth Path sub segment: target-nf-type-AUSF	
Path sub segment: target-nf-type=AUSF	
Path sub segment: requester-nf-type=AMF	?\X1>~V?u.b
Path sub segment: supi=imsi-310014791791001aza.j.e@.q4%1h.@j.k[Z.aGJB.R12v.2.c.Z0("validtyPeriod":86400,"nfInstancesi":[("nfInstancesi:[("nfI	Status": "REGISTERED", "nfType": "AUSF", "pimnList":
[Unescaped: /nnrf-disc/v1/nf-instances/service-names] [[mmc1041/mmc11001]/mmc11001]/mmc11001]/mmc11091/mmc11991/mmc11991/mmc11991/mmc11091/mmc11001]/mml011991/mmc11001/mml011991/mml011991/mml011991/mml011991/mml011991/mml011991/mml011991/mmc11001/mml011991/mmc110011/mml011991/mmc110011/mml011991/mmc110011/mml011991/mmc110011/mml011991/mmc110011/mml011991/mmc111991/mmc	.mnc014.mcc310.3gppnetwork.org", "sNssais":[{"sd":"000001", "sst":1]
Representation: Literal Header Field with Incremental ("dart": "9999900000000","end": "99999999999"), ("dart": "11122500000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "1112250000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end": "1112250000000000","end": "111225000000000","end": "1112250000000000","end": "111225000000000","end": "111225000000000","end": "111225000000000","end	nfServices";[{"scheme";"http","ipEndPoints";[{"port";
Index: 4 80,"pv4Adversy1"192.08.56.138"))/vendors'1(1'aprUvendors'1'(1'a)"/serVersion110/1"/v1")/vision10/1"/v1"/vision10/1"/v1"/vision10/	11","serviceName":"nausf
Y Header: :nethod: GET	","pimnList":[{"mnc":"014","mcc":"310"},{"mnc":"001","mcc":"001"},
Name Length: 7 (mcf1997)mcf1257/mcf1257/mcf12807	":[{"sd":"000001","sst":1},{"sd":"000002","sst":1},{"sd":"000002","sst"
("start": "00100100000001","end": "001001999999999"),("start": "99999000000000","end": "311225000000000","end": "311225999999999"),("start": "311225000000000","end": "311225999999999"),("start": "311225000000000","end": "3112259999999999"),("start": "311225000000000","end": "3112259999999999"),("start": "311225000000000","end": "3112259999999999999"),("start": "311225000000000","end": "31122599999999999"),("start": "31122500000000","end": "311225999999999999"),("start": "311225000000000","end": "31122599999999999"),("start": "311225000000000","end": "311225999999999999"),("start": "311225000000000","end": "311225999999999999"),("start": "311225000000000","end": "311225999999999999"),("start": "311225999999999999"),("start": "3112259999999999999999999999999999999999	tart": "26283000000000", "end": "26283099999999"}]], "nfServices":
Value Length: 3 [['scheme': http://pEndPoint's[['port's5, 'pv4Addres' 192.16556.137', 'framport'; TCP']]/versions':	
Value: GET [[GapFulVersion'12.0./*gaPversionInUfin22*eppr/*2009/070670254432*])/HSpartosStatus' 1250_astronationation (Section 2014) (Section	(ST./e~.mf2:.]](b.
:method: del	
[Unescaped: GET]	JM", "pimnList":[{"mnc": "014", "mcc": "310"},{"mnc": "001", "mcc": "001 [/"edi-"000001" "edi-11, /"edi-"000007" "edi-11, /"edi-"000007" "edi
2}]/udmInfo":("routingIndicators":["0", 0000"],"gpsiRanges":[["start": "31001400000000","end": "31001499999999"]),"sup	piRanges":[{"start":"31001400000000","end":"310014999999999"},
	art":"262830000000000","end":"26283099999999"}]]},"nfServices":
[{"apiFullVersion":"1.1.0", ap/VersionInUn":"v1", exploy": 2030-07-06T02;54;322"31, "n[ServiceStatus": "REGISTERED", "serviceInstanceId": "nudm-uecm", "serviceName	e":"nudm-
	IZ.VO:0.". fD
Name: authority TBUBTEDIX-05	RED", "nfTvpe": "SMF", "plmnList": [{"mnc": "014", "mcc": "310"}], "sNss
<pre>Volde congent if</pre>	iff.pgw-s5gn.mcn-
Value: 192.168.56.143:80 [spundsepc.mrc14.mc13.0gppntvrok.org?], nfisivices "[[chems]"http://pEndlonis" [[chems]"http://pEndlonis" [[chems]"http://pEndlonis	serviceName": "nsmf-
:#uthor1ty: 192.106.30.143:00 (Usession 'Tigdn' 'intrdincent01.dnc.mc014.mc210.3gppnetwork.org')]]]/'nrf5upportedFeatures''12"]	
Representation: Literal Header Field with Incremental II client plus, 10 server plus, 19 terms.	
Today: 1	
Index: 1 View Content-Length: 9 Enfre conversion (StS Syster) V Show data as ASCII V	Strea

Figure 53: TCP stream showing SBA NFs' communication messages

Part 1.2: Modifying Traffic on the SBA Interfaces

For this part, we used the TCP Layer Proxy Tool to modify a message from one NF and transmit the modified packet to the client NF.

In Figure 54, the AMF requests SMF service through a GET frame via the TCP Proxy Tool (packet 229), and the tool relays this request to NRF (packet 231). Shown as an inset in the figure is the NRF response to the Proxy Tool containing the SMF IP address of 192.168.56.129 (packet 233).

However, as can be seen in Figure 55, rather than passing the message back to the AMF as-is, the Proxy Tool intercepts the message, modifies the SMF IP address to 192.168.56.131, and posts this modified HEADER frame to the AMF (packet 235). That message is received successfully by the AMF without generating an error.

đ	agon_with_modification	pcap				- 0	×
	Edit View Go Ca	oture Analyze Statisti	cs Telephony Wireless	Tools Help			
	I d o 📁 🗎	XC Q	**** U =				
							• +
	Time	Source	Destination	Protocol Se	surce Port Destinal L	endth Info	
	220 221.245484	172.17.208.251	172.17.13.136	HTTP2/JSON	8080 42471	602 HEADERS[9]: 201 Created, DATA[9], JavaScript Object Notation (application/ison)	
	222 221.257736	172.17.152.146	172.17.208.251	HTTP2	43136 8080	172 HEADERS[5]: GET /nnrf-disc/v1/nf-instances?service-names-nudm-uecm&target-nf-type=UDM&requester-nf-type=AMF&supi=imsi-310014791791001	
	224 221.257861	172.17.208.251	192.168.56.143	HTTP2	54794 80	172 HEADERS[5]: GET /nnrf-disc/v1/nf-instances?service-names=nudm-uecm&target-nf-type=UDN&requester-nf-type=AMF&supi=imsi-310014791791001	Zo
	225 221.259831	192.168.56.143	172.17.208.251	HTTP2/JSON	80 54794	1378 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)	LOC
	227 221.259930	172.17.208.251	172.17.152.146	HTTP2/JSON	8080 43136	1378 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)	
	229 221.731021	172.17.27.33	172.17.208.251	HTTP2	43072 8080	221 HEADERS[3]: GET /nnrf-disc/v1/nf-instances?service-names=nsmf-pdusession&target-nf-type=SMF&requester-nf-type=AMF&snssais=%58%78%22sst%22%3A1	Zo
	231 221.731175	172.17.208.251	192.168.56.143	HTTP2	54792 80	221 HEADERS[3]: GET /nnrf-disc/v1/nf-instances?service-names=nsmf-pdusession&target-nf-type=SMF&requester-nf-type=AMF&snssais=%SB%78%22sst%22%3A1	
	233 221.733835	192.168.56.143	172.17.208.251	HTTP2/350N	80 54792	974 HEADERS[3]: 200 OK, DATA[3], JavaScript Object Notation (application/ison)	
	Todex: 6						0
		: /mnrf-disc/v1/nf-	instances?service-nam	esensef-ndusessi	on&target-of-typ	ex\$#\$#cequester-nf-typex###&snssais=\$\$9\$70\$22sst\$22\$31\$2C\$22sd\$22\$14\$22\$000001\$22\$70\$%D&don=don-embh=stb1.mitre.net	
							Øue
							0
							0
			ances?service-names=n	smf-pdusession&ta	rget-nf-type=SM	<pre>%requester-nf-type=AMF8snssais=%58%78%22sst%22%3A%22%3A%22000001%22%7D%5D&dnn=dnn-embb-stb1.mitre.net</pre>	0
							0
	Path	segment: /nnrf-disc/	/v1/nf-instances		1		
	Path	sub segment: service	e-names=nsmf-pdusessic	n		Wireshark - Packet 233 - diagon_with_modification.pcap	- 1
	Path	sub segment: target.	-nf-type=SMF				
	Path	sub segment: request	ter-nf-type=AMF			Member: port	
	Path	sub segment: snssais	s=%58%78%22sst%22%3A1%	2C%225d%22%3A%22	00001%22%70%51	<pre>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/port:7070]</pre>	
	Path	sub segment: dnn=dnr	n-embb-stb1.mitre.net			[Member with value: port:7070]	
	[Unescape	d: /nnrf-disc/v1/nf	-instances?service-name	mes=nsmf-pdusessi	on&target-nf-t	Number value: 7070	
	Represent	ation: Literal Head	er Field with Increment	ntal Indexing - I	ndexed Name	Key: port	
	Index: 4			000000000000000000000000000000000000000		<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/port]</pre>	
	✓ Header: :meti	nod: GET				Member: ipv4Address	
	Name Leng	th: 7				<pre>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address:192.168.56.129]</pre>	
	Name: :me	thod				[Member with value: ipv4Address:192.168.56.129]	
	Value Len	gth: 3				String value: 192.168.56.129	
	Value: GE	т				Key: ipu4Address	
	:method:	GET				<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address]</pre>	
	[Unescape	d: GET]				Key: ipEndPoints	
	Represent	ation: Indexed Head	er Field			<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints]</pre>	
	Index: 2					 Member: versions 	
	✓ Header: :auti	nority: 10.108.204.4	17:8080			 Array 	
	Name Leng	th: 10				 Object 	
	Name: :au	thority				✓ Member: apiFullVersion	
	Value Len	gth: 18				[Path with value: /nfInstances/[]/nfServices/[]/versions/[]/apiFullVersion:1.1.2]	
	Value: 10	.108.204.47:8080				[Member with value: apiFullVersion:1.1.2]	
	:authorit	y: 10.108.204.47:80	88			String value: 1.1.2	
<pre>Minute for the fo</pre>							
	[Unescape	d: 10.108.204.47:80	68]			Key: apiFullVersion	

Figure 54: AMF request for SMF services via TCP Proxy Tool

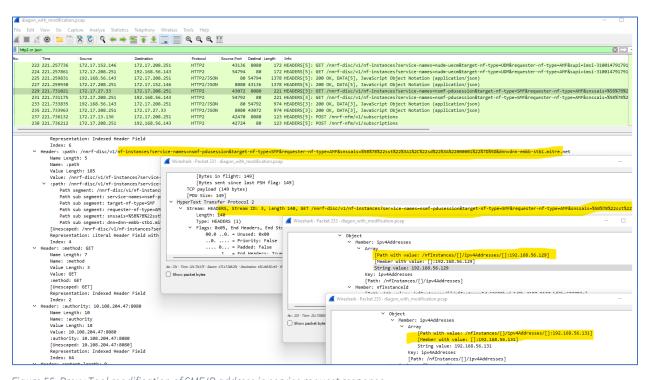


Figure 55: Proxy Tool modification of SMF IP address in service request response

Part 1.3: Injection of Traffic on the SBA Interface

Similar to Part 1.2 above, in Part 1.3 of the experiment, we again used the TCP Layer Proxy Tool, this time injecting a new packet into the SBA NFs' interface data stream. We attempted to insert additional packets into the data stream as additional TCP/HTTP2 messages.

Figure 56 shows the AMF (172.17.152.146) requesting SMF services from the NRF (192.168.56.143) by way of the TCP Proxy Tool (172.17.208.251), as seen in packets 219 and 220. The NRF replies to the Proxy Tool with the IP address for the SMF (packet 221), which is then passed on to the AMF (packet 223). However, in this instance, we saved the message relayed to the AMF, and inserted that duplicated packet into the SBA interface (packet 225). This message is successfully conveyed to the AMF. Because it is a duplicate packet, the AMF recognizes the extra packet and issues a GOAWAY frame message, telling the Proxy Tool and NRF to initiate a graceful shutdown of the HTTP2 connection.

agon_duplicated_packet.pcap	- 0
Edit View Go Capture Analyze Statistics Telephony Wireles	ss Tools Help
I 🖉 🕲 늘 🖹 🗙 🏹 🍳 ሩ 🗭 🖉 🖉 🗐	a a a a
Time Source Destination	Protocol Source Port Destinal Lenoth Info
217 185.595130 172.17.208.251 172.17.152.165	HTTP2 8080 43041 89 PING[0]
219 188.712690 172.17.152.146 172.17.208.251	HTTP2 43137 8080 221 HEADERS[5]: GET /nnrf-disc/v1/nf-instances?service-names=nsmf-pdusession&target-nf-type=SMF&r
220 188.712827 172.17.208.251 192.168.56.143	HTTP2 46294 80 221 HEADERS[5]; GET /mrf-disc/v1/nf-instances?service-names=nsmf-odusession&target-nf-type=SMR&r
221 188,714989 192,168,56,143 172,17,208,251	HTTP2/JSON 80 46294971 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)
223 188,715076 172,17,208,251 172,17,152,146	HTTP2/JSON 8080 43137 971 HEADERS[5]: 200 OK, DATA[5], JavaScript Object Notation (application/json)
225 188.715176 172.17.208.251 172.17.152.146	HTTP2/JSON 8080 43137 971 HEADERS[5]: 200 0K, DATA[5], JavaScript-Object Notation (application/json)
227 188.715483 172.17.152.146 172.17.208.251	HTTP2 43137 8080 89 GOAWAY[0]
229 188.715536 172.17.208.251 192.168.56.143	HTTP2 46294 80 89 GOAWAY[0]
235 188.716993 172.17.13.136 172.17.208.251	HTTP2 42464 8080 87 HEADERS[5]: POST /nnrf-nfm/v1/subscriptions
Path sub segment: dnn=dnn-embb-stb1.mitre.ne	
	names=nsmf-pdusession&target-nf-type=SMF&requester-nf-type=AMF&snssais=[{"sst":1,"sd":"000001"}]&dnn=dnn-embb-stbl.mitre.net]
Representation: Literal Header Field with Incre	
Index: 4	📕 Wireshark - Packet 223 - diagon_duplicated_packet.pcap — 🗆
✓ Header: :method: GET	
Name Length: 7	Key: port
Name: :method	<pre>[Path: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/port]</pre>
Value Length: 3	Member: ipv4Address
Value: GET	<pre>[Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address:192.168.56.129]</pre>
:method: GET	[Member with value: ipv4Address:192.168.56.129]
[Unescaped: GET]	String value: 192.168.56.129
Representation: Indexed Header Field Index: 2	Key: ipv4Address
Index: 2 V Header: :authority: 10.108.204.47:8080	🖉 Wireshark - Packet 225 - diagon_duplicated_packet.pcap —
Name Length: 10	- S. American -
Name: :authority	Member: ipv4Address
Value Length: 18	 rember: 1pv4Address [Path with value: /nfInstances/[]/nfServices/[]/ipEndPoints/[]/ipv4Address:192.168.56.129]
Value: 10.108.204.47:8080	[Path with Value: /htintsances/[]/https://acast.jpina/coints/[]/ipvaAddress:192.168.56.129] [Member with value: ipvAddress:192.168.56.129]
:authority: 10.108.204.47:8080	[member with value: 1pv+nduress:192.108.50.129] String value: 192.168.56.129
[Unescaped: 10.108.204.47:8080]	Key: ipv4Address
Representation: Indexed Header Field	<pre>representation and the second a</pre>
Index: 65	Key: ipEndPoints
Header: content-length: 0	<pre>rej. ipinicults [Path: /nfinstances/[]/nfServices/[]/ipEndPoints]</pre>
Name Length: 14	Member: versions
Name: content-length	~ Array
Value Length: 1	v Object
Value: 0	Wember: apiFullVersion
content-length: 0	[Path with value: /nfInstances/[]/nfServices/[]/versions/[]/apiFullVersion:1.1.2]
[Unescaped: 0]	[Member with value: apjfull/version:1.1.2]
Representation: Indexed Header Field	String value: 1.1.2
	Key: apfullversion
Index: 64	

Figure 56: Inserting duplicate message on the SBA interface

Part 2: mTLS on the SBA Interface

For the second part of the test, we repeated the same basic tests as Part 1 of this test after configuring mTLS on the 5G core SBA interface. With mTLS, each network function mutually authenticates with the others to form encrypted connections among them. These latter tests were conducted on June 1, 2023, and also used the TCP Layer Proxy Tool.

Part 2.1: Inability to Eavesdrop on the SBA Interfaces

For this experiment, we focused on the traffic between the SMF (192.168.56.129), NRF (192.168.56.143), and AMF (172.17.27.33). As shown in Figure 57, two SBA interfaces at IPs 172.17.27.33 (AMF) and 192.168.56.129 (SMF) perform TLS handshake, including the Client Hello, Server Hello, and Key Exchanges and Verifications (packets 14664-14673). Thereafter, upon successful key exchange, the mTLS tunnel is established between the two network functions. All traffic between them is subsequently encrypted, and we can no longer see or tell the underlying messages, as seen in Figure 58 in which the Application Data is shown as encrypted and undecipherable by Wireshark.

	t2_combined-itc-trace-files_0 Capture Analyze Statistics		Tools Help							
	🖹 🙆 ९ 🗢 🏓 🖀 👔									
.addr ==192.168.56.129										+ 1
Time	Source	Destination	Protocol	Source I	Destinatic	Length Info				
14661 11:49:03.6	8 <mark>5935 172.17.27.33</mark>	192.168.56.129	ТСР	43074	7070	76 43074 → 7070 [SYN]				
14662 11:49:03.6	86101 192.168.56.129	172.17.27.33	TCP	7070	43074	76 7070 → 43074 [SYN,	ACK] Seq=0 Ack=	L Win=62636 Len=0	MSS=8960 SACK_PERM	I TSval
14663 11:49:03.6	86120 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [ACK]	Seq=1 Ack=1 Win	=62720 Len=0 TSval	.=3929595204 TSecr=	-143207
14664 11:49:03.6	86992 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	291 <mark>Client Hello</mark>				
14665 11:49:03.6	87061 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 <mark>[ACK]</mark>	<mark>Seq=</mark> 1 Ack=224 W	in=62464 Len=0 TSv	al=1432070387 TSec	r=3929
14668 11:49:03.7	02449 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	2468 Server Hello, Certi	ficate, Server	(ey Exchange, Cert	ificate Request, S	erver
14669 11:49:03.7	02465 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [ACK]				
14671 11:49:03.7	21675 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	2331 Certificate, Client				
14672 11:49:03.7	21771 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [ACK]	Seq=2401 Ack=24	37 Win=60416 Len=0	TSval=1432070422	TSecr=
14673 11:49:03.7	25476 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	119 Change Cipher Spec,				
14674 11:49:03.7	25483 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [ACK]	Seq=2487 Ack=24	52 Win=60416 Len=0	TSval=3929595244	TSecr=
14675 11:49:03.7	25827 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	149 Application Data				
14676 11:49:03.7	25890 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [ACK]	Seq=2452 Ack=25	58 Win=60416 Len=0	TSval=1432070426	TSecr=
14677 11:49:03.7	25936 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	140 Application Data				
14678 11:49:03.7	25940 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [ACK]	Seq=2568 Ack=25	24 Win=60416 Len=0	TSval=3929595244	TSecr=
14679 11:49:03.7	26036 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	106 Application Data				
14680 11:49:03.7	26084 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [ACK]	Seq=2524 Ack=26	06 Win=60416 Len=0	TSval=1432070426	TSecr=
rame 14664: 291	bytes on wire (2328 b	its), 291 bytes ca	ptured (232	3 bits) o	n inter	face unknown, id 0	0000 00 04	30 01 00 06 0e 54	57 fc 23 a6 00 00	08 00
inux cooked capt	ture v1						0010 45 a0	01 13 f0 6c 40 00	40 06 88 7c ac 11	ι 1b 21
nternet Protocol	l Version 4, Src: 172.	17.27.33, Dst: 192	.168.56.129						70 27 e3 af 43 31	
ransmission Cont	trol Protocol, Src Por	t: 43074, Dst Port	: 7070, Sea	: 1, Ack:	1. Len	: 223			01 01 08 0a ea 38	
ransport Layer S	Security								da 01 00 00 d6 03	
TLSv1.2 Record	Layer: Handshake Pro	tocol: Client Hello)						ae e6 20 95 39 50	
	e: Handshake (22)								27 0e 70 76 88 cc	
Version: TL	S 1.2 (0x0303)								01 00 00 a7 00 00 64 6d 63 73 6d 66	
Length: 218									2e 6d 6e 63 30 31	
	rotocol: Client Hello								67 70 70 6e 65 74	
Handshak	e Type: Client Hello ((1)							00 18 00 16 06 03	
Length:									03 03 03 01 02 03	
	TLS 1.2 (0x0303)								00 3a 00 38 00 0e	
	6478bdef99e7add778aee6	209539509fe7f6c20d	85f9f671092	70e707688	cd7f		00e0 00 19	30 1c 00 0b 00 0c	00 1b 00 18 00 09) 00 0a
	ID Length: 0								00 06 00 07 00 14	
	uites Length: 6								00 01 00 02 00 03	
	uites (3 suites)								01 00 00 10 00 05	00 03
	ion Methods Length: 1						0120 02 68	32		

Figure 57: ITC trace file showing mTLS handshake

e Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Image: Capture Analyze Statistics Telephony Wi												
		2 4 🖛 🏓 🖀 🏠	<u>*</u> @ @ @									
.sti	eam == 208										X 🗆	·] +
	Time	Source	Destination	Protocol	Source I	Destinatic	Length Info					
4	673 11:49:03.7254	76 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	119 Change Cipher Sp	ec, Encrypte	d Handsha	ake Message		
4	674 11:49:03.7254	33 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [AC	K] Seq=2487	Ack=2452	Win=60416 Len=	=0 TSval=392959524	44 TSecr
4	675 11:49:03.7258	27 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	149 Application Data					
4	576 11:49:03.7258	0 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [AC	K] Seq=2452	Ack=2568	Win=60416 Len=	0 TSval=14320704	26 TSecr
.4	677 11:49:03.7259	36 192.168.56.129	172.17.27.33	TLSv1.2	7070	43074	140 Application Data					
ι4	678 11:49:03.72594	40 172.17.27.33	192.168.56.129	TCP	43074	7070	68 43074 → 7070 [AC	K] Seq=2568	Ack=2524	Win=60416 Len=	=0 TSval=392959524	44 TSecr
ι4	579 11:49:03.7260	36 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	106 Application Data					
14	580 11:49:03.72608	34 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [AC	K] Seq=2524	Ack=2606	Win=60416 Len=	=0 TSval=14320704	26 TSecr
14	581 11:49:03.72714	48 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	251 Application Data					
ι4	582 11:49:03.7272	02 192.168.56.129	172.17.27.33	TCP	7070	43074	68 7070 → 43074 [AC	K] Seq=2524	Ack=2789	Win=60416 Len=	=0 TSval=14320704	27 TSecr
ι4	583 11:49:03.72724	42 172.17.27.33	192.168.56.129	TLSv1.2	43074	7070	1461 Application Data					
4	584 11:49:03.72728	35 192.168.56.129	172.17.27.33	ТСР	7070	43074	68 7070 → 43074 [AC	K1 Sea=2524	Ack=4182	Win=59136 Len=	=0 TSval=143207043	28 TSecr
-	me 14683 · 1461 by	tes on wire (1168	hits) 1461 bytes	cantured (11688 bit	s) on i	sterface unknown id 0	0010	55 5h a9	16 17 03 03 05	5 6c dd a9 d6 58	5d 6e 0
	ux cooked capture		, , , , , , , , , , , , , , , , , , , ,	cupcurcu (11000 010		reer ruce unknown, 10 o					
			.17.27.33, Dst: 192	168 56 129				0060	61 e1 44	95 1f 30 74 cb	06 5b 6f e4 fd	e6 90 1
			rt: 43074, Dst Port			ck 252	1 len: 1393	0070	89 d1 bc	10 4e a7 f3 f9	9 d5 74 44 6a 5b	c4 00 5
	nsport Layer Secu		c. 45074, 0501010	. 7070, 504	. 2705, 1		, con 1999	0080	37 75 4a	45 b4 15 aa 13	3 98 7d 95 d1 32	1a 6a f
			ata Protocol: Hype	nToxt Transf	fon Broto	col 2					3 b5 2b 3d 8d 6d	
		Application Data (i i cxe ii uiisi		01 2					5 30 25 71 3e 1d	
	Version: TLS 1.		23)								bf 77 5f 3a 64	
	Version. 165 1.	2 (0,0303)									3 38 db 30 0e 03 36 20 ac 37 e6	
	Length: 1388											

Figure 58: Encrypted SBI traffic with mTLS – source ITC trace file, MITRE 5G Core

Part 2.2: Modifying Traffic on the SBA Interface

In this part, as in Parts 1.2 and 1.3, we used the TCP Proxy Layer Tool to attempt to modify the traffic stream from the NRF (IP address 192.168.56.143) and transmit the traffic to the SMF (IP address 172.17.208.231). The tool is transparent to the SBA interfaces. Also, because traffic between the SBA NFs is encrypted, and the TCP Proxy Tool actions are transparent, the ITC trace files do not show any interactions for the TCP Proxy Tool service or HTTP pod IPs as illustrated in Figure 59, where no messages appear when filtering on the relevant IP addresses. The logs from these IPs are only visible from the logs taken by the Proxy Tool.

	SRIC_7b-and-mTLS	t2_combined	d-itc-trace-files_06	-01-23_1100a	m.pcapng				_		×
File	Edit View Go	Capture An	alvze Statistics	Telephony	Wireless Tools Help						
	I 🖉 🕲 🚞 🛅	× 2 9	* * * * * *								
ip.a	ddr==172.17.208.23	1 ip.addr==1	0.108.204.47 ip.ad	dr==172.17.208	3.251				*		Hex Va
No.	Time	Source	Destination	Protocol	Source Destination Length	info					
-							_				
0 2	CSRIC_7b-and-m	TLS_t2_combine	ed-itc-trace-files_06-0	1-23_1100am.p	capng		Pa	ckets: 72224 * Displayed: 0 (0.0%)	Pr	ofile: STB	Profile

Figure 59: TCP Proxy Tool actions are transparent, source ITC trace file

Because data flowing through the TCP Proxy Tool is encrypted, the tool cannot identify what type of message any given packet corresponds to. Consequently, for data modification, the TCP Proxy Tool randomly selected packets to modify. The modification changed the last byte of data

to 0x00 for the selected packet. An example output of the Proxy Tool is shown in Figure 60. The figure also shows how the receiving node disconnects the TLS/TCP traffic stream when the modified packet is received. Subsequently, a new TCP client traffic connection is initiated, starting a new TLS stream in order to complete the failed operation. Figure 61, Figure 62, and Figure 63 show additional cases of the TCP Proxy Tool modifying encrypted packets. Every time the tool modifies the data, a TCP reset (RST) is sent, closing the connection between the sender and the recipient device, and informing the sender to create another connection and resend the traffic.

root@diagon-d4df7fdb-mctv9:/app# python diagon_with_modification2.py
('172.17.208.231', 64802) has connected
Modifying data ('172.17.208.231', 64802)!
Original data: b'\x17\x03\x00\x10\x95\xee\xea\x81\x82\xf1\x06(\x11\xc9N\x07e\x9b\xb5W\xca\xf5\x16\x01\x95\xf9\xba\xf3(\xf8'
Modified data: b'\x17\x03\x03\x00\x1a\x95\xee\xea\x81\x82\xf1\x06(\x11\xc9N\x07e\x9b\xb5W\xca\xf5\x16\x01\x95\xf9\ <mark>xba\xf3(\x00'</mark>
('172.17.208.231', 64 <mark>802) has disconnected</mark>
('172.17.208.231', 65338) has connected
('172.17.208.231', 64582) has connected
('172.17.208.231', 64737) has connected
('172.17.208.231', 64587) has connected
Modifying data ('192.168.56.143', 443)!
Original data: b'\x16\x03\x03\x02\x02\x00\x00\x03\x03\x82\x86\xfa\xc2[\xe3\xb3\xef\x08Fh\x1f\xcfY\x8e!\x18B!-aqY4\x0e\x02\x83\r\xec\xcd] \xfa\x9a./\xc4
\xae\xb79\xb8R\xab\xb4\xd6\xe6\xd4\xb6\xf3\xfb\xbc\x1e\xb8\xcc\xe1\x0c\xe2TV:rF\xfe\x9b\x13\x02\x00\x003\x00\$\x00\x1d\x00 \x1aVhvN\xb3\x19\xa8\x0b\x01
\xa0\xe5\x99\x8e\$*\x18\xc4\xbd\xf8\xc4\xf9\xfc\xee\xfe\x8a\xfb\x98]<\x9db\x00+\x00\x02\x03\x04\x14\x03\x03\x00\x01\x01\x17\x03\x03\x03\x08\x14\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x03\x04\x14\x14\x04\x14\x14\x04\x14\x14\x14\x14\x14\x14\x14\x14\x14\x1

Figure 60: Traffic modification using TCP Proxy Tool

Mitre	_diagon-pod-trace_c	ontinuous.pcapng.gz								
File Edi	t View Go Ca	oture Analyze Statist	ics Telephony Wir	eless Tools	Help					
	/ @ = 6	🖹 🏹 🔍 🦛 🖬		■ ⊕						
			/ 🚔 🐮 🖄 📑		~ ~					
tcp.por	t == 64802									
No.	Time	Source	Destination	Protocol		Destinat Le		nfo		
		2 172.17.208.231	172.17.208.251	TCP	64802			4802 → 8080 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=1094098240 TSecr=0 WS=256		
		9 172.17.208.251	172.17.208.231		8080 6			080 → 64802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
		0 172.17.208.231	172.17.208.251		64802			TCP Port numbers reused] 64802 → 8080 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=10941		
		7 172.17.208.251	172.17.208.231		8080 (080 → 64802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
		2 172.17.208.231	172.17.208.251	тср	64802			TCP Port numbers reused] 64802 → 8080 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=10941		
		8 172.17.208.251	172.17.208.231	TCP	8080 (080 → 64802 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
		0 172.17.208.231	172.17.208.251	тср	64802			TCP Port numbers reused] 64802 → 8080 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=10941		
		6 172.17.208.251	172.17.208.231	TCP	8080 6			080 → 64802 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSval=2208746256 TSecr=105		
		0 172.17.208.231	172.17.208.251	TCP	64802			4802 → 8080 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=1094165120 TSecr=2208746256		
		0 172.17.208.231	172.17.208.251	TCP	64802			4802 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=62720 Len=356 TSval=1094165121 TSecr=2208746256		
		8 172.17.208.251 9 172.17.208.251	172.17.208.231 172.17.208.231	TCP	8080 (8080 (080 → 64802 [ACK] Seq=1 Ack=357 Win=62464 Len=0 TSval=2208746257 TSecr=1094165121 080 → 64802 [PSH, ACK] Seq=1 Ack=357 Win=62464 Len=1566 TSval=2208746258 TSecr=1094165121		
705	5 12:20:55.24570	9 1/2.1/.200.251	1/2.1/.200.251	TCP	0000	04002				
							Wires	hark · Packet 3514 · Mitre_diagon-pod-trace_continuous.pcapng.gz		
		on wire (640 bits), 80 bytes captu	red (640 b:	its) on :	interfa				
> Linux cooked capture v2								ame 3514: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0		
> Internet Protocol Version 4, Src: 172.17.208.231, Dst: 172.17.208.251								nux cooked capture v2		
✓ Transmission Control Protocol, Src Port: 64802, Dst Port: 8080, Seq: 0, Len: 0					eq: 0, L0	en: Ø		ternet Protocol Version 4, Src: 172.17.208.251, Dst: 172.17.208.231		
	Source Port: 648						V Tr	ansmission Control Protocol, Src Port: 8080, Dst Port: 64802, Seq: 1, Ack: 1, Len: 0		
Destination Port: 8080						_		Source Port: 8080		
[Stream index: 1072] [Conversation completeness: Incomplete (37)]								Destination Port: 64802		
	TCP Segment Len							[Stream index: 1072]		
Sequence Number: 0 (relative sequence number)								[Conversation completeness: Incomplete (37)]		
Sequence Number (raw): 1407823150								[TCP Segment Len: 0]		
[Next Sequence Number: 1 (relative sequence number)]								Sequence Number: 1 (relative sequence number) Sequence Number (raw): 0		
Acknowledgment Number: 0								Sequence Number (raw): 0 [Next Sequence Number: 1 (relative sequence number)]		
Acknowledgment number (raw): 0								[Next Sequence Number: 1 (relative sequence number)] Acknowledgment Number: 1 (relative ack number)		
1010 = Header Lepgth: 40 bytes (10)								Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 1407823151		
> Flags: 0x002 (SYN)								0101 = Header Length: 20 bytes (5)		
Window: 62720								Flags: 0x014 (RST, ACK)		
	Calculated wind	ow size: 62720]					· · · ·	Mindow A		

Figure 61: TCP packet reset after data is modified, source TCP Proxy Tool logs

Modifying data ('172.17.208.231', 64737)
Original data: b'\x17\x03\x00\x13#\xd3\xb1N\x1b\xaf=ua?\x00MNm~\x82\xaf5\xa7'
Modified data: b'\k17\x03\x00\x13#\xd3\xb1N\x1b\xaf=ua?\x00MNm~\x82\xaf5\x00'
('172.17.208.231', 64737) has disconnected
Modifying data ('192.168.56.143', 443)!
Original data: b'\x17\x03\x03\x00\x9b/ <s\x9dul\xd0\xeev~\xc1\x89\xd5n\xb0\xfc\xf9"\xea\x05zh\n\xb0\xf1\xfbp\xc4\xae\xd6\xde\xe3\rla\xc05\xe5\xa1\xbc\n\x91< td=""></s\x9dul\xd0\xeev~\xc1\x89\xd5n\xb0\xfc\xf9"\xea\x05zh\n\xb0\xf1\xfbp\xc4\xae\xd6\xde\xe3\rla\xc05\xe5\xa1\xbc\n\x91<>
<pre>\xac\xaf\xcb\xde\xf4\x14\xc3\xe1b\x10\xa9?\xae\x898scY\$8\x93.\xa10K\x1d \xe2\xa7#\xde\xba\x9f6\xd50\xd1@\xd9sZ\xd6\xc1\x89T\x94\xb5b\x17\\"0\xe0\x1a\x16\xfc</pre>
\xca\x9df\xfa\xce\xfd\xb1\xbas*4D\xb1\xbas*4D\xb1\xb5\x04\xcc<\x85\x1e6\xd1cQhh\x0e\xf0;\xaa\n&7\x1c\xf5\xe6:\xb1\x02\x06\x9c&\r\x95\x8a\xaa\x88B\x16@J\x01\x05\x98'
Modified data: b \x17\x03\x00\x9b/<\$\x9duL\xd0\xeev~\xc1\x89\xd5\xb0\xfc\xf9"\xee\x05zH\\\xb0\x6\x4bp\xc4\xae\xd6\xde\xe3\rLA\xc05\xe5\xa1\xbc\n\x91
\xac\xaf\xcb\xde\xf4\x14\xc3\xe1b\x10\xa9?\xae\x898scY\$8\x93.\xa10K\x1d \xe2\xa7#\xde\xba\x9f6\xd5o\xd4I@\xd9sZ\xd6\xc1\x89T\x94\xb5b\x17\\"0\xe0\x1a\x16\xfc
\xca\x9df\xfa\xce\xfd\xb1\xbas*4D\xb1 >\xb5\x04\xcc<\x85\x166\xd1c0hh\x0e\xf0;\xaa\n&7\x1c\xf5\xe6;\xb1\x02\x06\x9c&\r\x95\x8a\xaa\x88\x16@]\x01\
(172.17.288.231', 65487) has disconnected
('172.17.208.231', 65192) has connected
Modifying data (172.17.208.231', 65192)
Original data: b'\x17\x03\x03\x03\x00\x1a\xa5\xcdU^\xd1cu\xe6\xb8q\xd5MXq\x95\x90\x16\xe6a\x960\x1e\xb6xe'
Modified data: b'\x17\x03\x03\x03\x04\x04\x04\xdx4\xdfx4\x04\x04\x04\x04\x04\x04\x04\x04\x04\x
('172'17' 208'231', 65192) has disconnected
('172,17,208,231', 64773) has connected
Modi fying data ('172.17.208.231', 64773)!
Original data: b'\x17\x03\x03\x03\x04\x06's\xc3P\xbcACfi82\xfaK4\x91\t\xe4*\x80jX\xea\x0f\\xbf\\xb9\xf01\xf4M\xeb\xa1'
Modified data: b (Ar(As)X03)X03)X00*S(As2F)XefA(XbcACf)32(XrfaK4)X91(1(Xe4*)X80)X(Xea)X0f(Xdf(Xb9)Xrfa1)XefA(X80)
(172,17,208,231,64773) has disconnected
(I/II//ROULEST) 04/75/ Has disconnected

Figure 62: Traffic modification using TCP Proxy Tool

p.stream eq 6917					X - + HexV
Packet list ∨ Narro	w & Wide 🗸 🗌	Case sensitive Hex value	 ✓ 7fbac 	:a00	Find Cancel
Time	Source	Destination Protocol	Source Port D		
21756 13:39:40.962489	172.17.208.251	192.168.56.143 TCP	53238	443	80 53238 → 443 [SYN] Seq=0 Win=62720 Len=0 MSS=8960 SACK_PERM TSval=193763350
21757 13:39:40.962540	192.168.56.143	172.17.208.251 TCP	443	53238	80 443 → 53238 [SYN, ACK] Seq=0 Ack=1 Win=62636 Len=0 MSS=8960 SACK_PERM TSva
21758 13:39:40.962546	172.17.208.251	192.168.56.143 TCP	53238	443	72 53238 → 443 [ACK] Seq=1 Ack=1 Win=62720 Len=0 TSval=1937633508 TSecr=26402
21761 13:39:40.962775	172.17.208.251	192.168.56.143 TLSv1.3	53238	443	428 Client Hello
21762 13:39:40.962797	192.168.56.143	172.17.208.251 TCP	443	53238	72 443 → 53238 [ACK] Seq=1 Ack=357 Win=62464 Len=0 TSval=2640279933 TSecr=193
21763 13:39:40.964069	192.168.56.143	172.17.208.251 TLSv1.3	443	53238	1638 Server Hello, Change Cipher Spec, Application Data
21764 13:39:40.964080	172.17.208.251	192.168.56.143 TCP	53238	443	72 53238 → 443 [ACK] Seq=357 Ack=1567 Win=61184 Len=0 TSval=1937633510 TSecr=
21773 13:39:40.966409	172.17.208.251	192.168.56.143 TLSv1.3	53238	443	2279 Change Cipher Spec, Application Data, Application Data, Application Data
21774 13:39:40.966443	192.168.56.143	172.17.208.251 TCP	443	53238	72 443 → 53238 [ACK] Seq=1567 Ack=2564 Win=60416 Len=0 TSval=2640279937 TSec
21775 13:39:40.966651	172.17.208.251	192.168.56.143 TLSv1.3	53238	443	491 Application Data, Application Data
21776 13:39:40.966668	192.168.56.143	172.17.208.251 TCP	443	53238	72 443 → 53238 [ACK] Seq=1567 Ack=2983 Win=60160 Len=0 TSval=2640279937 TSec
21777 13:39:40.966759	192.168.56.143	172.17.208.251 TLSv1.3	443	53238	96 Application Data
21778 13:39:40.966766	172.17.208.251	192.168.56.143 TCP	53238	443	72 53238 → 443 [ACK] Seq=2983 Ack=1591 Win=61184 Len=0 TSval=1937633512 TSecr
21779 13:39:40.966799 21780 13:39:40.966816	192.168.56.143 192.168.56.143	172.17.208.251 TCP 172.17.208.251 TCP	443	53238 53238	72 443 → 53238 [FIN, ACK] Seq=1591 Ack=2983 Win=60160 Len=0 TSval=2640279937 72 443 → 53238 [RST, ACK] Seq=1592 Ack=2983 Win=60160 Len=0 TSval=2640279937
Length: 1336 Encrypted Application Data: 6722407af30de4049620316baf589520ed4df521de6dd [Application Data Protocol: Hypertext Transfer Protocol] VTLSU13 Record Layer: Application Data Protocol: Hypertext Transfer Protocol Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 281 Encrypted Application Data: 1cd0450ccdae29519c270ad051587ce05f1ed9bf3c2cc [Application Data Protocol: Hypertext Transfer Protocol] VTLSU13 Record Layer: Application Data Protocol: Hypertext Transfer Protocol] VTLSU13 Record Layer: Application Data Protocol: Hypertext Transfer Protocol Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 69 Encrypted Application Data: 4bbee30ca24512bea1675a3924833bffe5cd223af3ad				> > > > > > > > > > > > > > > > > > >	Frame 21773: 2279 bytes on wire (18232 bits), 2279 bytes captured (18232 bits) of Linux cooked capture v. Linux cooked capture v. Linux cooked capture v. Internet Protocol Version 4, Src: 172.17.208.251, Dst: 192.168.56.143 Transmission Control Protocol, Src Port: 53286, Dst Port: 443, Seq: 357, Ack: 15 Source Port: 5328 Destination Port: 443 [Stream index: 6917] 860 16 ea 43 e3 a8 97 98 ce dd fd 6d 45 0c 7d e8 e2 870 8a 3f 43 e7 6f 75 2a d8 46 f5 d5 60 58 ff 6c d9 880 80 7 cd e1 45 60 d8 97 75 32 e6 56 c9 ea 25 e 43

Figure 63: TCP packet data modification, source TCP Proxy Tool logs

Part 2.3: Inserting Packets into SBA Traffic Stream

Similar to Part 2.2 above, in Part 2.3 of the experiment we again used the TCP Layer Proxy Tool to try and inject a new packet into the SBA NFs' interface data stream. In this case, the tool was programmed to duplicate packets randomly. Each duplicate packet is then inserted into the traffic stream and transmitted. As shown in Figure 64 and Figure 65, the TCP Proxy Tool duplicates data on the fly. We see from the logs that the TCP stream is disconnected by issuance of a [FIN,ACK] whenever the remote NF notices a duplicate packet.

\xe6\x98\x8a\xe7\'\x93\x98{\xb7\xc8\xafY\x92\xb1\x84\x85\x04i\xa0M\x14\x84\xb5\x11*\xfb\x9a|\xedQZ\xa6L\xd679\xd52\xc3\xf1\xfc\x95\xf4\x807\xc2\x91]\xce\xa6 \x1c\xd2J\xb9\xda\xa8\xe1\x1c\xd1\x0f@1b\x81-UTqB;\x0c\xc8\xe4P\xe8dx(\xd8\x1b\xf8\xb5\x9aR\xe1\xee\x0e\xa1\xbcQ|F\xa6\xdf\x01Q\x94\xb0\xabGG\xc9\xi \xac]\xe4 Duplicating packet!



b'\x17\x03\x03\x89\x800\x13F\xc7d\xbaT\xd5b\xdd\xb1\x11\x06\x93\x87H\xb7D\x82\xc8A'

b'\x17\x03\x03\x04\x64\xe5\x890\xd6\xa8"\x95xW\x99u\xc6\x99u\xa6\xfb\xd6\xca\x87\xadc\xd9%A\xb0\xba\x93+1\x86N\x87\x04\x80\x13\x96\x14\x94\x8b\xd2\x82\x0 \xab\x04cp\'\xb0\xf7\x021\xd7-\xf0"4\\\xb0\xb9\x93\xf3\xfde\x87\'\xefj\xe7\xae\x13\xc7\x82\xee\xd0\xd5cd \xf0\xc2\x04\xae\xb0\xf10Y\r\x80\x07\xd7\x88 \xa0H\xfb\x19!\xba\x91\xe1^*h\xfb\xa9\x83\xaf\xb1+\xd9\xcc\xf6gh\'\xce*S\x11\x19\xe5&\xccY]\xad6@#n\xf2eS\xccW\x95\xcb\xd1\x02\x120\xf8\xf9\xdfp\xe5L\rp \x8C\xd8\xd2\xd8\xd2\xd8\xcc\xa3\xdd.PM\xe6\x93i\xf5\xab\xafn\x11\xe0\xa1\x11\x95\xac\x1d\$s\x66\x14U1@\xb7\x17\x04\x9f\xca\xf9E\xa3\xc2D\x07g#\x81\xe3u\xdc\xc3\xafP \xe4\xa8\x89\x82\xc1\xc7\x88\xf1\xb17\xd4V\xcd\xaf\xb6\x94\xbcp\x04A\x9e-\x13\x9c\xd0\x9d\x14q\xeb\x01wf\x08\xef\xcdS'\xd5\xf2\xfe\xc0\xd4%\xadp\xc3?w\xa6\xac \xa9\xb9\xe1\x8fQ\xbc(\xd0]\x14\x11\x14\x07r\xb9u\x86\xf4\xb3\x06\x1d\x83\x902\xfc\xa9\x90 \x03\xa2\x94\xad ('172.17.208.231', 64878) has disc Original data:

b"\x17\x03\x01\xd7\xc7\xc6\xd1rm\xd2\xc9e\x03(\xe8;(\x82\xe5?\xfcf5\xa5;Z\x88M\x18\x92P\xd8\xd9\x91H\xd7E\x9c_\xa8i%\x82\xed\x0c\xbb\x9a\xe0\xd2\x89 \xf5bV,\x9e\xeb\x10\x02\xe6\x0b\x14*xx>\x12\xa0\r\xdf\xb0\x93\xd8\xff\x9d;g\x1b6s\xbcX\xe8\xe3B\tQe\xf9T\xc9n\xbe\xba\x1c\xcd)\x9f\xe2i\xb3\xd5\xfc\xce \x8f\x85\xcf\xed\r\xd0\xd3~RBg\xf3\xab\x92\x8ec\n0\xf34\xae\xb5WB#\xf5\xbfw,\x93\xaa^\xf0m\x82\x90\x9bPt\xa8\xda\x8d\xed\xe6\xa2\xc5\x14\x1bX\xb0\xcb\x98\x08



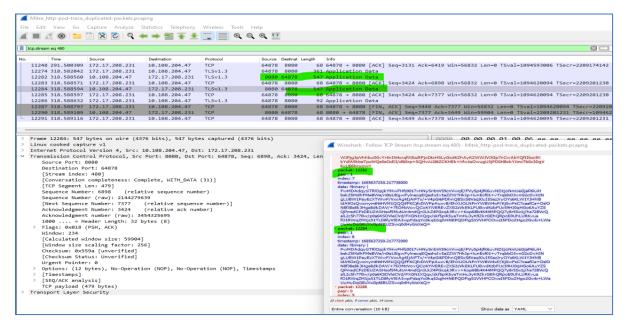


Figure 65: Inserted TCP packets, Wireshark view, source TCP Proxy Tool logs

Success Criteria:

- 1. Unable to eavesdrop on the SBA interfaces
- 2. Unable to modify traffic on the SBA interfaces
- 3. Unable to inject messages on the SBA interfaces

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

Results

Conclusions and Next Steps

This round of testing successfully verified the efficacy of employing security procedures recommended by the CSRIC VII WG3 report, implementing commercial hardware in a commercially-relevant SA configuration.

For each of the seven test cases described here, the tests successfully verified the efficacy of employing security procedures recommended by the CSRIC VII WG3 Report 2 recommendations for securing the 5G standalone network architecture. This verification of the CSRIC recommendations in a commercially-deployed environment is the first of its kind for 5G standalone networks. The test cases focused on confidentiality and integrity at multiple locations in the 5G system, including over-the-air between the UE and the RAN, for NAS signaling, for RRC signaling, over an untrusted backhaul, as well as on the Service-Based Architecture interface.

The first test case demonstrated that the implementation of NEA2 encryption on NAS messages enables user identity to be safely exchanged. With no encryption, as observed when setting the system to use the NULL NEA0 algorithm, messages containing user identities were exchanged between the UE and AMF in a way that message details were visible. However, when the NEA2 encryption algorithm was specified, all NAS messages were encrypted and undecipherable by an observer who does not have the correct encryption key. In addition, only non-user information was observable prior to NAS encryption, and user identity was transmitted via the SUCI.

The second test case considered confidentiality protection for RRC traffic. To test RRC confidentiality, Test Case 2 used an RF network monitoring tool to capture the messages transmitted over the air. First, this test demonstrated the visibility of identity-related data when no encryption (NULL scheme) was used for RRC messages. The captured data showed that the contents of RRC messages were fully decipherable by the RF monitoring tool. Second, the test demonstrated the concealment of the data when RRC encryption was enabled. In that test, the RF monitoring tool indicated the contents of the encrypted messages as "Extra bytes at end of RRC message," implying that there was additional data present in the packets, but the tool was unable to make sense of it.

The fifth test case addressed the CSRIC VII recommendation that devices and networks in the U.S. use IMSI privacy (SUCI) and do not use the NULL scheme, which could expose the IMSI/SUPI to an unauthorized entity. The test run on the 5GSTB demonstrated the use of the SUCI by the UE in the registration process and resulted in a successful registration.

The next test case reported here replicated tests performed previously for the NSA architecture, demonstrating that the implementation of an IPsec tunnel over an untrusted backhaul link prevents eavesdropping on both user plane and control plane traffic, as well as preventing modification and injection of false traffic designed to appear as originating from or destined to a valid UE. As with the NSA tests, use of the IPsec tunnel resulted in all traffic on the untrusted link appearing as encrypted ESP packets with no ability to read the contents. In addition, when attempting to modify and inject traffic into the transport link, the IPsec tunnel prevented all of the injected packets, or decrypted versions of them, from making it out of the tunnel to either the UE or the core-side router.

The final tests performed for this effort addressed security on the SBA interface, illustrating the benefits of mTLS among the multiple network functions. As such, there were two main parts to the test case: highlighting vulnerabilities without encryption; and demonstrating the protection provided by encrypting traffic on the SBA interface using mTLS. For the first part, it was shown that, without encryption, we were able to identify IP addresses for several network functions (AMF, AUSF, NRF, SMF, and UDM) as well as extracting user identity through the IMSI/SUPI. In addition, the tests demonstrated the ability to intercept messages between the NRF and AMF and modify the SMF IP address without producing an error when encryption was not used. It was also possible to insert duplicate packets on the SBA interface, which were received successfully

by the AMF and resulted in a GOAWAY command from the AMF. The second part, with mTLS enabled, encrypted traffic among the network functions. After being able to observe a successful TLS handshake between two network functions, all subsequently exchanged data were encrypted and undecipherable. Furthermore, attempts to modify and inject traffic on the SBA resulted in errors and tearing down the connection between the network functions.

The seven test cases summarized above validate a subset of the CSRIC VII WG3 recommendations. Validation of additional recommendations from WG3 Report 2 are anticipated when the available test tool capabilities are sufficient to run the appropriate tests and capture the required data. Some examples of required capabilities include the ability to alter a message after the integrity check is applied, as well as the ability to capture user plane traffic over the air, in order to demonstrate the efficacy of applying user plane integrity and of access stratum user plane confidentiality.

As new participants and the diversity of test cases grow in tandem, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security, including additional phases of network slicing tests. For future tests, the 5G Security Test Bed is exploring additional aspects of network function security, false base stations, roaming security, and 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 of Open Radio Access Network (RAN) to verify security recommendations.

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/.

Appendix: Acronyms

3GPP	3rd Generation Partnership Project					
5G STB	5G Security Test Bed					
AMF	Access and Mobility Management Function					
AUSF	Authentication Server Function					
BBU	Baseband Unit					
СИОМ	Core Network Operations Manager					
СР	Control Plane					
CSRIC	Communications Security, Reliability, and Interoperability Council					
CSWG	Cybersecurity Working Group					
DHS	Department of Homeland Security					
DMC	Dual-Mode Core					
eMBB	Enhanced Mobile Broadband					
eNB	e-Node B					
ESP	Encapsulating Security Payload					
FCC	Federal Communications Commission					
IKEv2	Internet Key Exchange Protocol Version 2					
IMEISV	International Mobile Station Equipment Identity Software Version					
IMSI	International Mobile Subscriber Identity					
IPsec	Internet Protocol Security					
ITC	Integrated Traffic Capture					
ITU	International Telecommunications Union					

ММЕ	Mobility Management Entity					
mTLS	Mutual Transport Layer Security					
MTP	Mobile Test Platform					
NAS	Non-Access Stratum					
NG-RAN	Next-Generation Radio Access Network					
NIST	National Institute of Standards and Technology					
NR	New Radio					
NRF	Network Repository Function					
NSA	Non-Standalone					
PDCP	Packet Data Convergence Protocol					
RAN	Radio Access Network					
RRC	Radio Resource Control					
SA	Standalone					
SBA	Service-Based Architecture					
SBI	Service-Based Interface					
SDR	Software-Defined Radio					
SEG	Security Gateway					
SUCI	Subscription Concealed Identifier					
SUPI	Subscription Permanent Identifier					
TAC	Technical Advisory Committee					
тс	Test Case					
ТСР	Transmission Control Protocol					
TLS	Transport Layer Security					

ТР	Test Point
TS	Technical Standards
UE	User Equipment
UP	User Plane
UPF	User Plane Function
VPN	Virtual Private Network
WG	Working Group