

Securing 5G:

Test Results Based on CSRIC VII NSA Recommendations

Document Overview

This document is the first 5G Security Test Bed (5G STB) Report, containing results from the 5G STB's first round of testing which evaluated use cases leveraging a commercially deployed 5G network architecture. The 5G STB is a collaborative endeavor between wireless providers, equipment providers, cybersecurity experts, and academia to demonstrate and validate how 5G security will work in an existence-proof, real-world setting, using commercial technology that can be found in any U.S. network. The 5G STB is designed to allow for rigorous, transparent, and replicable security use case testing and evaluation of 5G devices, network configurations, and software that may be used to secure wireless communications across 5G technologies.

The 5G Security Test Bed evaluates use cases leveraging an actual 5G network architecture built from a significant investment and in-kind contributions in state-of-the-art equipment. This report evaluates some of the 5G security recommendations developed by the Federal Communications Commission advisory group, CSRIC (Communications Security, Reliability, and Interoperability Council) made up of experts from government and industry. Additional tests and use cases are planned. For more information, or to participate in the 5G STB, please contact Harish Punjabi hpunjabi@ctia.org; (202) 845-5701), or visit https://5gsecuritytestbed.com/.

This report was created by the 5G Security Test Bed. The results were produced by 5G STB members and the University of Maryland, which serves as the Test Bed Administrator. The results have been reviewed by the 5G STB's Technical Advisory Committee.

The information contained in this report may not be reproduced without the express written consent of the 5G Security Test Bed.

5G STB and TAC Members

The 5G Security Test Bed is a membership effort open to federal agencies, private sector member companies, researchers, and academic institutions. The 5G STB's founding members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, CTIA, the MITRE Group, and SecureG; and academic partner the University of Maryland, which also serves as the Test Bed Administrator.

The 5G STB has a Technical Advisory Committee (TAC) made up of the 5G STB's founding 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.

Executive Summary

Following its formal launch in early 2022, the 5G Security Test Bed has completed its inaugural round of tests, with successful results. Using its private 5G network and testing facilities, the 5G STB assessed and verified the efficacy of key 5G network security recommendations made by the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) VII.

Specifically, CSRIC's Working Group 2 (WG2, "Managing Security Risk in the Transition to 5G") made several recommendations to improve security for traffic transmitted over non-standalone (NSA) networks, where the 5G network is built over a 4G Long Term Evolution (LTE) core to support both types of traffic. Because 5G NSA networks are built with both 4G and 5G components, CSRIC's recommendations aim to ensure 4G networks' existing vulnerabilities do not carry over to 5G wireless technologies. The 5G STB has executed three test cases to validate these recommendations.

Through the three test cases, the 5G STB tested encryption over an untrusted connection between the two main components of an NSA network—the 4G/5G radio access network (RAN) and the 4G LTE Evolved Packet Core (EPC)—as well as end-to-end encryption between user equipment (UE) and an external web server. It assessed protections for both user plane traffic (or UP traffic, which is the actual data being transmitted by the user) and control plane traffic (or CP traffic, which directs and controls how data is forwarded through the network).

The tests confirmed that when a non-standalone 5G network exchanges traffic over an untrusted backhaul connection—in other words, a connection between the Radio Access Network and the LTE Core that is not controlled by the mobile network operator—implementing CSRIC's NSA encryption recommendations provides strong security protections for the network traffic.

Of the 5G STB's tests:

- Two test cases assessed 5G traffic encryption through an Internet Protocol Security (IPsec) tunnel, and particularly its ability to protect user traffic and control traffic from threats such as eavesdropping, modifying, and injecting traffic on the untrusted connection.
- The third test case demonstrated the benefits of transport-layer security (TLS) encryption between an application on user equipment and an application server on the public internet.¹

¹ TLS is a standard for securing data that uses cryptography to encrypt and decrypt data exchanged between sender and recipient networks. The sending and receiving networks decrypt the data they exchange by using public and private keys ranging from 128 to 2048 bits long.

The 5G STB determined that all tests were successful. Specifically, the tests verified that by using an IPsec tunnel to encrypt traffic, eavesdroppers could not decipher, modify, or inject traffic transferred through the network. TLS encryption—which uses cryptography that can only be deciphered at the traffic's origin and destination networks with secret keys—further enhanced these protections.

On the other hand, the tests found that without encryption on an untrusted connection, an eavesdropper could read and manipulate all user traffic and control traffic passing between the RAN and the LTE core, resulting in various outcomes for each traffic type. Without the IPsec tunnel, user traffic that was captured, modified, and injected into the untrusted connection was generally accepted as valid and passed through to the RAN or the LTE core. In some cases, the LTE core identified the injected control traffic as problematic and sent ABORT messages to the RAN, which resulted in a terminated connection.

When an IPsec tunnel was used to encrypt traffic between the RAN and the LTE core, the tests confirmed that all packets of information were indecipherable. Control traffic could not be distinguished from user traffic, and the source and destination addresses of the original messages could not be determined—the encryption caused all traffic to appear as if it was originating and terminating at the IPsec tunnel endpoints. The tunnel also dropped any modified and injected traffic, which was not allowed to pass to either the RAN or the LTE core. The final test verified that end-to-end TLS encryption further obscured the contents of messages sent through the network, preventing eavesdropping, modification, and injection anywhere between the UE and the TLS endpoint on the public internet.

Given the 5G Security Test Bed's initial set of successful tests over 5G non-standalone architecture, future test cases will assess 5G standalone (SA) architecture, where a 5G network is built with only 5G components. Anticipated test case topics include CSRIC VII recommendations for the SA architecture, as well as network slicing and roaming security concerns.

Table of Contents

Document Overview	2
Executive Summary	3
Introduction – How the 5G Security Test Bed Advances 5G Security	6
Scope of Report	8
Background	8
Why CSRIC VII	8
CSRIC VII Working Group 2's Report and Recommendations for 5G Non-Standalone Architecture	9
Definition of Use Cases, Leading to Definition of Test Cases	
5G STB NSA Test Overview	12
Summary of Process and Findings	12
NSA Network Architecture and Test Configuration	14
Detailed Test Procedure	16
5G STB NSA Test Results	18
Test Case 1, TC-IPsec-01	18
Test Case 2, TC-IPsec-02	27
Test Case 3, TC-IPsec-03	36
Conclusions and Next Steps	43
Appendix: Acronyms	45
References	47

Introduction – How the 5G Security Test Bed Advances 5G Security

The 5G STB 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 it is further expanding its efforts through its new 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 STB reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. The 5G STB 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 FCC, among others.

The 5G STB Uses Real-World Equipment, Validating Real-World Applications

One of the 5G STB'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 5G STB'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 STB's initial focus is to validate the recommendations of the FCC's CSRIC advisory group, for both non-standalone and standalone network configurations. It 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 STB'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:

- Government and Enterprise Applications
 - o Building private 5G networks for enterprises and government.
 - Developing dynamic supply-chain verification technologies for uses such as logistics management.
 - Creating automated, reconfigurable factories and other automated factory processes.
 - Developing immersive extended reality (XR) applications, including augmented reality (AR), virtual reality (VR), and mixed reality (MR), for both consumers and enterprises.
- General Network Security Protections
 - Enhancing protections against international mobile subscriber identity (IMSI) catchers and "rogue" base stations used by cyber criminals.
 - o Enabling automatic, rapid threat detection and response.
 - Implementing a unified authentication framework that supports security across multiple network types (e.g., cellular and Wi-Fi).

• Smart City Applications

- o Enabling video for unmanned aerial systems (e.g., drones).
- Providing support for autonomous vehicles and related technology (e.g. connected cars and C-V2X standards).
- o Enabling high-resolution video surveillance systems using fixed cameras.

Scope of Report

Security Focus

This report addresses three use cases derived from the FCC's Communications Security, Reliability, and Interoperability Council VII December 2020 report, *Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture*.² The CSRIC VII report focused on the implementation of security protections in 5G NSA networks, which provide 5G service over a 4G Long Term Evolution (LTE) core. The report drew upon established findings from standards bodies and industry associations such as the Global System for Mobile Communications (GSMA), the European Telecommunications Standards Institute (ETSI), 3GPP, and NIST to develop its security recommendations.

The 5G STB report's scope is to evaluate and verify CSRIC VII's recommendations by investigating the security features associated with 5G network infrastructure, as well as the use of devices capable of accessing a 5G NSA architecture.

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 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.

² CSRIC VII WG2, Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture (Dec. 2020), <u>https://www.fcc.gov/file/20181/download</u>.

The FCC tasked CSRIC VII with evaluating the transition from the fourth generation of mobile networks (4G) to the fifth generation (5G) to ensure continued reliability, interoperability, and security. The evolution to 5G will take time, which means that new technology will coexist with legacy technology. This raises interesting and complicated issues for real-world network operators and equipment providers.

As one report explained, "[N]etwork upgrades do not happen overnight. A mobile network operator does not flash-cut from one generation of network technology to another. Rather, a new generation will coexist with prior generations for years, even decades."³ This is the reason operators, manufacturers, standards bodies, and regulators differentiate between "standalone" and "non-standalone" deployments of 5G—a non-standalone network architecture provides 5G service over a 4G LTE core, which enables both services to operate over the same network to limit customer disruption.

CSRIC VII's work resulted in several key reports and recommendations for enhancing security for non-standalone deployments. CSRIC recommendations do not often lead to testing, so industry and academia saw value in validating the effectiveness and achievability of CSRIC VII's recommendations.

CSRIC VII Working Group 2's Report and Recommendations for 5G Non-Standalone Architecture

The Need for 5G NSA Architecture

5G is an evolving global wireless standard that enables more types of devices to connect, delivers higher peak mobile data speeds, increases network capacity and availability, reduces latency, and provides a more uniform user experience to a broader customer base. 5G's unique architecture includes built-in security features, such as mutual authentication and end-to-end encryption that are not available in previous wireless network generations. Because 5G must coexist with 4G as network operators make the transition, it is necessary to establish standards that ensure the networks are interoperable and at the same time take advantage of 5G's enhanced security features.

3rd Generation Partnership Project (3GPP), a global partnership of telecommunications standards organizations, develops standards for mobile communications, including 5G networks. In doing so, 3GPP has built in backward and forward compatibility when possible, which ensures that network operators can provide both 4G LTE and 5G equipment and services to their users during the transition. As a result, many new 5G network deployments use both 4G

³ Jon Metzler, Security Implications of 5G Networks, UC Berkeley Center for Long-Term Cybersecurity at 7 (Sept. 2020), <u>https://cltc.berkeley.edu/wp-content/uploads/2020/09/Security_Implications_5G.pdf</u>.

LTE and 5G equipment. In these non-standalone, or NSA, networks, the radio portions of the system are 5G, but the core network is shared with LTE. Standalone, or SA, architectures are independent 5G networks using components built specifically for only 5G.

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. CSRIC's Working Group 2 (WG2, "Managing Security Risk in the Transition to 5G") released a December 2020 report, *Report on Review and Recommendation on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture* in December 2020.⁴ The report focused on the implementation of security in NSA networks that provide 5G service over a 4G LTE core. Within the 3GPP standards, TS 33.401 and 33.501 specified a security architecture of features and mechanisms for the 4G and 5G systems, respectively.

Several security features outlined in 3GPP TS 33.401 and 33.501 are mandatory for equipment vendors to implement in UE, but optional to deploy by 4G and 5G network operators. CSRIC VII WG2 looked at the optional security features and conducted a risk assessment and analysis on those measures, including: confidentiality and integrity for Non-Access Stratum (NAS) signaling,⁵ user plane confidentiality and integrity, radio resource control signaling, UE-configured radio technology, several identity and authentication elements, and network security (IPsec and TLS).

Based on its assessment, CSRIC VII WG2 made five recommendations:

- Communications sector members and stakeholders should adopt CSRIC-recommended best practices for hardware and software vendors that collaboratively address security by design principles.⁶
- Operators should use higher layer security protections, such as TLS, to mitigate user plane threats in non-standalone deployments.
- Operators should decide whether to add more security for control plane signaling messages based on customer requirements, risk analysis, and use cases.

⁴ CSRIC VII WG2, Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture (Dec. 2020), <u>https://www.fcc.gov/file/20181/download</u>.

⁵ "NAS signaling" carries the user data from the user equipment to the MME through the S1 pathway. ⁶ This recommendation was restated from a CSRIC V report. *See* CSRIC V WG6, Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network (Sept. 2016). <u>https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx</u>.

- When IPsec is used, operators should decide whether to deploy IPsec Tunnel Mode or Transport Mode over the S1-MME, S1-U, and management interfaces based on a risk analysis and use cases.⁷
- When using IPsec, operators should decide whether to deploy a Security Gateway for IPsec termination on the core network side.

Definition of Use Cases, Leading to Definition of Test Cases

CSRIC VII WG2 identified use cases associated with its five recommendations. In these use cases, the working group assessed options for protecting user plane integrity, control plane integrity, Based on these use cases, the 5G STB established and executed three test cases described in this report, as follows:

1. Confidentiality and Integrity on User Plane:

- a. <u>CSRIC Use Case:</u> CSRIC VII WG2 assessed options for protecting user plane integrity on 5G NSA networks when data is transmitted over an untrusted connection. Based on a risk analysis and use case requirements, network operators may decide whether and how to use encryption on untrusted connections to provide confidentiality over the S1-U interface. Options available to network operators include using IPsec Encapsulating Security Payload (ESP) encryption or an equivalent encryption technology such as MACsec, or proceeding with untrusted connections based on a risk analysis and by use case.
- b. <u>5G STB Test Case</u>: To demonstrate the application of this mitigation for the user plane, the 5G STB defined a test case that assessed IPsec encryption on the S1-U interface.

2. Confidentiality and Integrity on Control Plane:

- a. <u>CSRIC Use Case</u>: CSRIC VII WG2 assessed options for security on the control plane, including message security for the NAS signaling interface that carries the data between the UE and the MME. As with the user plane, network operators may decide whether and how to use encryption on untrusted connections to provide confidentiality over the S1-MME interface. Options available to network operators include using IPsec, MACsec, or other encryption technologies, or allowing untrusted connections based on a risk analysis and by use case.
- b. <u>5G STB Test Case</u>: To demonstrate the application of this mitigation for the control plane, the 5G STB defined a test case that assessed IPsec encryption over the S1-MME interface.

⁷ "S1" refers to the logical pathways that connect various parts of the 5G NSA network's LTE core to the RAN. The S1-MME is the control plane's pathway, while the S1-U is the user plane's pathway. The MME, or mobility management entity, is the part of the LTE core that manages mobile device operations such as subscriber authentication, roaming, and handovers to other networks.

3. TLS Implementation on User Plane:

- a. <u>CSRIC Use Case</u>: As highlighted in its earlier June 2020 report, CSRIC VII WG2 recommended higher layer security protections to mitigate user plane threats. In its December 2020 report, WG2 recommended these protections be based on application layer functionality—which controls how applications communicate with other applications and devices.
- b. <u>5G STB Test Case</u>: To demonstrate the application of this mitigation for the user plane, the 5G STB developed a test case for end-to-end TLS encryption through an IPsec tunnel at the application layer.

The 5G STB anticipates that further testing will look at CSRIC VII WG3 recommendations for the 5G standalone architecture,⁸ network slicing, subscriber privacy, and roaming security.

5G STB NSA Test Overview

Summary of Process and Findings

In order to validate CSRIC VII's 5G NSA network security recommendations, the 5G STB defined specific test cases that could demonstrate the efficacy of those recommendations and related use cases. As a result, each of the 5G STB's three test cases corresponds with a specific CSRIC recommendation and objective, as described in Table 1.

Test Case ID	Test Case Title	CSRIC Recommendation	Objective
TC-IPsec-01	CSRIC 7 WG 2 item -	CSRIC VII WG 2, Report 2:	User Plane Security – Higher
(Test Case 1)	IPsec on UP	7.2.2 User Plane	layer protection via S1-U
		Confidentiality and Integrity	interface confidentiality and
		over the S1-U	integrity using IPsec on an
		7.2.4 IPsec	untrusted link
TC-IPsec-02 (Test Case 2)	CSRIC 7 WG 2 item - IPsec on CP	CSRIC VII WG 2, Report 2: 7.2.3 NAS Signaling	Control Plane Security – Higher layer protection via
		Confidentiality and Integrity over the S1-MME	S1-MME interface confidentiality and integrity
		7.2.4 IPsec	using IPsec on an untrusted link

Table 1: 5G STB NSA High-Level Test Cases

⁸ CSRIC VII WG3, Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards (Sept. 16, 2020), <u>https://www.fcc.gov/file/19297/download</u>.

TC-IPsec-03	CSRIC 7 WG 2 item –	CSRIC VII WG 2, Report 2:	User Plane Security – Higher
(Test Case 3)	TLS on UP	7.2.2 User Plane	layer protection at
		Confidentiality and Integrity	application layer using end-
		over the S1-U	to-end TLS encryption
			through an IPsec tunnel

The 5G STB then developed detailed test plans with step-by-step procedures for setting up and executing tests, including defining specific test points, means of generating and capturing traffic, and other details. While the test results are provided in detail in a later section, Table 2 previews the high-level findings below.

Table 2: 5G STB NSA Test Case Result Summary

Test Case Title	Conclusion	Rationale
CSRIC 7 WG 2 item - IPsec on UP	Success	 When the IPsec tunnel is implemented on the untrusted link, an eavesdropper cannot read the user traffic transmitted over the link (it all appears as ESP-encrypted packets with source and destination addresses as the endpoints of the tunnel). The IPsec tunnel does not allow modified and injected packets to exit the tunnel.
CSRIC 7 WG 2 item - IPsec on CP	Success	When the IPsec tunnel is implemented on the untrusted link, an eavesdropper cannot read the CP traffic transmitted over the link (it all appears as ESP-encrypted packets with source and destination addresses as the endpoints of the tunnel).The IPsec tunnel does not allow modified and injected control packets to exit the tunnel.
CSRIC 7 WG 2 item – TLS on UP	Success	 When TLS encryption is implemented on the untrusted link, an eavesdropper cannot read the user traffic with or without IPsec encryption. This includes all capture points, not just those on the untrusted link. Adding IPsec to the untrusted link further obscures the traffic, preventing an eavesdropper from reading the source and destination of the TLS messages, as well as knowing which encapsulated packets are TLS. TLS encryption and IPsec encryption do not allow modified and injected packets to reach their intended destinations.

As presented in the table above, all three of the 5G STB's tests successfully validated CSRIC VII's recommendations for implementing IPsec and TLS encryption to protect user plane and/or control plane traffic travelling through 5G NSA networks.

NSA Network Architecture and Test Configuration

3GPP has defined multiple deployment options for 5G NSA networks. Figure 1 below shows 3GPP's NSA Options 3, 3a, and 3x, which all use E-UTRA New Radio – Dual Connectivity (EN-DC) with LTE serving as the Master Radio Access Technology (RAT) and the 5G New Radio (NR) serving as the Secondary RAT.

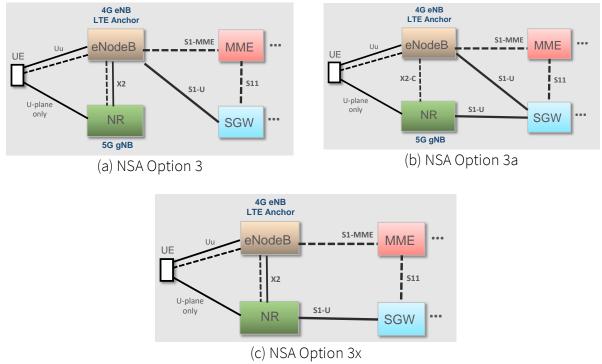


Figure 1: NSA Options

Option 3x is network operators' preferred choice because its direct connection between the 5G system's NR user plane and the LTE system's Evolved Packet Core (EPC) ensure minimal impact on existing networks. The test cases in this document use Option 3x.

Figure 2 shows how the configuration of Option 3x using the Security Gateway (SEG) for IPsec termination.

TLP:WHITE:5GSTB

5G STB Report Based on CSRIC VII Recommendations

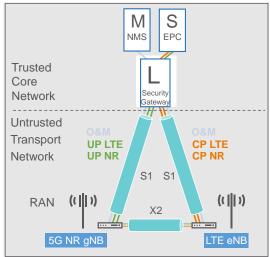


Figure 2: 5G NSA network configuration Option 3x, with SEG for IPsec termination

The physical network configuration used for the 5G STB's initial non-standalone tests consists of a radio access network (RAN) hosted at the University of Maryland and a 4G LTE Evolved Packet Core hosted at the MITRE Corporation in Virginia. Both installations are in secure facilities with safeguards and procedures to ensure the integrity and security of operations.

The connection between the RAN at UMD and the EPC at MITRE is transmitted over the internet and, therefore, for the scenarios considered here, is treated as an untrusted link⁹. Figure 3 shows the configuration for the NSA test cases. The 5G RAN, LTE RAN, and LTE EPC have been provided by Ericsson. The Ericsson EPC product is a combination SGW/PGW/UPF (serving gateway, packet data network gateway, and user plane function). It is configured as SGW/PGW for the purposes of the NSA test cases.

⁹ The connection between the two sites is actually protected by two additional security tunnels: both an IPsec tunnel between UMD campus and the MITRE network, protecting traffic over the internet; and a second tunnel between devices in the 5G STB enclaves to further limit access to appropriate personnel.

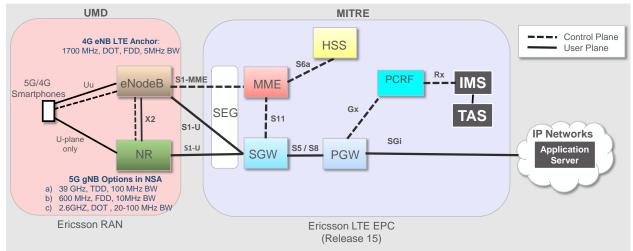


Figure 3: NSA Test Configuration for CSRIC Use Cases

Detailed Test Procedure

Figure 4 shows the test bed's relevant components, including test points (TP) for various tests. The routers shown at each location are Ericsson 6672 routers (referred to as R6672 or R6K for short) and serve as IPsec tunnel endpoints. The switches shown are each Pluribus Freedom 9372-X switches. For the purposes of these tests, the two switches are considered part of the "untrusted" backhaul link.

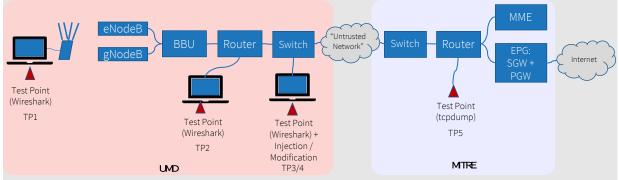


Figure 4: 5G Security Test Bed's Physical Connections and Test Points

The User Equipment (UE) being used in these tests consists of a Sierra Wireless EM9190 card connecting to a laptop by USB. Band 66 is used for LTE and N71 for 5G. For the user plane tests of Test Case 1, traffic is generated at the UE by running the ping command in a Windows Command Prompt, with a desired destination at IP address 8.8.8 (the address for Google's domain name server). For the control plane tests of Test Case 2, no user traffic is purposefully generated (although the Windows operating system creates some traffic). For the TLS test of Test Case 3, an HTTPS session is opened from a web browser on the UE laptop.

During the tests, packets are captured on each of the identified test points in Figure 4: at the UE, on the RAN-side R6K router, on the RAN-side Pluribus switch, and on the LTE core-side R6K router. These test points are identified with numbers as shown in the figure and described in more detail in Table 3, below. Packets captured at TP3 on the untrusted link are saved using tcpdump and then modified using Kali Linux and injected into the untrusted link at the same test point. Due to the manual process for starting and stopping packet captures, each set of packet captures starts and stops at a slightly different time. As a result, packets appearing at the beginning or end of the test point may not be present in all captures, and, consequently, counts of specific packets at each test point may differ slightly.

Table 3: Test Point Descriptions

Test Point	Description and Use
TP1	Wireshark running on laptop connected to UE; captures packets originating and terminating at UE laptop
TP2	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)
TP3	tcpdump running on laptop connected to the port of RAN-side Pluribus switch used to capture, modify, and inject packets on the untrusted link
TP4	Wireshark running on laptop connected to port of RAN-side Pluribus switch used to monitor packets on the untrusted link
TP5	tcpdump running on computer connected to core-side R6K router; configured to capture packets outside the tunnel (i.e., before IPsec encryption or after IPsec decryption) and inside the tunnel (encrypted packets when IPsec tunnel is enabled)

Wireshark was used to display and filter traffic. It is worth noting that the RAN encapsulates all packets with the GPRS Tunneling Protocol (GTP), so, when observing Wireshark captures, there is an outer Ethernet frame encapsulating a GTP-formatted packet, which itself contains the IP packet. When TLS is used, it encapsulates yet another packet, the encrypted version of the original packet.

While the 5G STB's objective is to verify the efficacy of recommended encryption procedures, we also demonstrate the ability to eavesdrop, modify, and inject packets when the traffic on the untrusted link is left unencrypted. For unencrypted user plane traffic, tcpdump was configured to capture only pings and ping responses (ICMP traffic); for unencrypted control plane traffic, tcpdump captured the naturally occurring control plane traffic, which is the S1 Application Protocol (S1AP) traffic transported over SCTP. When traffic on the untrusted link is encrypted, tcpdump only sees encrypted packets and cannot distinguish between user traffic and control traffic, so all traffic is captured and replayed. Furthermore, for UP test cases, because we can limit the traffic the UE puts on the network, it is straightforward to determine whether injected

traffic is dropped in the IPsec tunnel. However, because we have no control over the CP traffic generated by the RAN and LTE core, in order to make it clear whether or not injected CP packets are dropped, we inject over 1,000 false CP packets during a test and measure the differences in number of packets captured at each test point.

For cases implementing an IPsec tunnel, we used pre-shared keys (PSK) to establish the security association between the two tunnel endpoints. Note that the original use case called for signed certificates. However, the effort to establish the Public Key Infrastructure was deemed excessive for the purposes of these tests, which require encryption, regardless of the security association method.

5G STB NSA Test Results

Table 4 contains the configuration parameters used for the tests.

Table 4: RAN Configuration Parameters

RAT	Band	TDD/FDD	DL EARFCN	UL EARFCN	Bandwidth
LTE Anchor	B66	FDD	66786	132322	20 MHz
NR	N71	FDD	126900	136100	15 MHz

Table 5 shows the connectivity status at the start of the test, including the IP address assigned by the EPC to the laptop connected to the Sierra Wireless card.

Table 5: Modem Connection Details

Parameter	Value
Connection Mode	EN-DC
IP Address	172.18.0.3

Test Case 1, TC-IPsec-01

TC-IPsec-01 has two objectives: (1) to demonstrate that, without encryption on the untrusted link, it is possible to eavesdrop, modify, and inject data packets on the user plane; and (2) to verify that, with an IPsec tunnel between the RAN and LTE core, packets cannot be read, modified, or injected on the user plane.

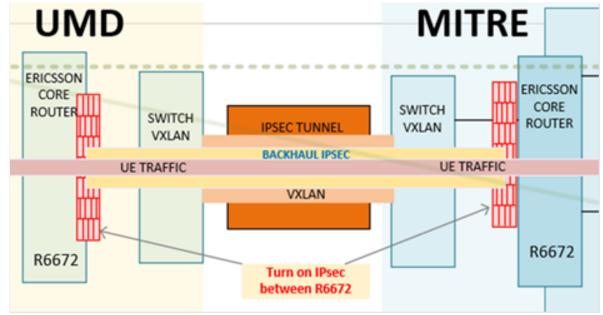


Figure 1: IPsec Tunnel Implementation

Objective 1: Verify ability to eavesdrop, modify, inject payload on UP

Figure 6 shows the traffic captured on the UE where Wireshark is used to display and filter traffic. In this figure, only ICMP (ping requests and replies) messages are shown. For reference on this and subsequent figures, Table 6 lists the files whose data are shown in the figures, along with a description of the contents.

test_1a_ping_noipsec_UE-device_050322.	pcapng			– 🗆 ×
ile Edit View Go Capture Analyz	e Statistics Telephony Wir	eless Tools Help		
a 🔳 🖉 🛞 📜 🛅 🗶 🔳 🔎	रे 🗢 👄 🖀 🝝 📃	📃 @, @, @, 🎹		
icmp				+
lo. Time	Source Destination	Protoc Length Info		
1 2022-05-03 13:28:06.463791	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9161/51491, ttl=128 (reply	in 2)
2 2022-05-03 13:28:06.494833	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9161/51491, ttl=51 (request	in 1)
3 2022-05-03 13:28:07.478576	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9162/51747, ttl=128 (reply	in 4)
4 2022-05-03 13:28:07.502732	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9162/51747, ttl=51 (request	in 3)
5 2022-05-03 13:28:08.493115	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9163/52003, ttl=128 (reply	in 6)
6 2022-05-03 13:28:08.526882	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9163/52003, ttl=51 (request	in 5)
7 2022-05-03 13:28:09.509008	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9164/52259, ttl=128 (reply	in 8)
8 2022-05-03 13:28:09.539130	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9164/52259, ttl=51 (request	in 7)
13 2022-05-03 13:28:10.539601	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9165/52515, ttl=128 (reply	in 14)
14 2022-05-03 13:28:10.554104	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9165/52515, ttl=51 (request	in 13)
15 2022-05-03 13:28:11.556462	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9166/52771, ttl=128 (reply	in 16)
16 2022-05-03 13:28:11.579000	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9166/52771, ttl=51 (request	in 15)
26 2022-05-03 13:28:12.570756	172.18.0.3 8.8.8.8	ICMP 60 Echo (ping) request	id=0x0009, seq=9167/53027, ttl=128 (reply	in 27)
27 2022-05-03 13:28:12.603691	8.8.8.8 172.18.0.3	ICMP 60 Echo (ping) reply	id=0x0009, seq=9167/53027, ttl=51 (request	in 26)
				>
Raw packet data Internet Protocol Version 4, Sr	rc: 172.18.0.3, Dst: 8.8.		{AD825110-5F39-4C2E-B476-1BEDA4D5C3EF}, id	10
Internet Control Message Protoc				
Type: 8 (Echo (ping) reques	t)			
Code: 0				
Checksum: 0x298a [correct]				
0010 08 08 08 08 08 08 00 29 0020 65 66 67 68 69 6a 6h 0030 75 76 77 61 62 63 64	6c 6d 6e 6f 70 71			
🔵 🍸 Code (icmp.code), 1 byte			Packets: 106 · Displayed: 44 (41.5%)	Profile: STB Profile

Figure 6: UE Packet Capture

Table 6: Test Case 1 Raw Data Files and Content Descriptions When IPsec Not Implemented

File Name	Contents
test_1a_ping_noipsec_UE-device_050322.pcapng	Ping packets captured at TP1, laptop
	connected to UE
ping050322.pcap	Captured ping traffic at TP3
mod_ping050322.pcap	Modified ping traffic
final_test_1a_ping_noipsec_testlaptop_050322.pcapng	Injected ping traffic at TP3
final_test_1a_ping_noipsec_pluribus_050322_mod.pcapng	Injected traffic captured at TP4 on
	outgoing interface to the core
test1A2-MITRE-r6k-noipsec-050322-1640.pcap	Traffic captured at TP5 on core-side
	ingress R6K interface from RAN
test1A2-MITRE-r6k-clear-050322-1640.pcap	Traffic captured at TP5 on core-side
	egress R6K interface toward internet

Figure 7 shows three Wireshark windows: one displaying contents of the PCAP file created by tcpdump on the untrusted link that captures transmitted packets to be later modified; one displaying the contents of the PCAP file that results from modifying those captured packets; and one that displays the packets observed on the Pluribus switch after the injection point (TP4). Each window's lower portion breaks down the packet highlighted in its upper portion. The modification that is implemented is changing the source MAC address of the message, which can be seen as Ericsson_8b:a0:50 (98:7a:10:8b:a0:50) in the first window and 66:0e:94:d3:a0:21 in both the modified and injected packet captures displayed in the second and third windows.

🗲 ping050322.pcap								
							×	
ile Edit View Go Capture Analyz								
(🔳 🖉 🛞 📜 🛅 🗙 🏹 🤇	९ 🖛 🏓 🚟 🐐 速 📃	••••						
ip.addr==8.8.8.8								
 Time 1 2022-05-03 13:29:00.749695 	Source Destination 172.18.0.3 8.8.8.8	Protocol Lengti Info	o (ping) request id=0>	0000 cos=0164/5335	0 **1-128 (pop)	v (10, 2)	^	
2 2022-05-03 13:29:00.754830	8.8.8.8 172.18.0.3			0009, seq=9164/5225				
7 2022-05-03 13:29:01.765661	172.18.0.3 8.8.8.8		o (ning) request id=0	0009. sea=9165/5251	5. ttl=128 (ren]	v in 8)		
8 2022-05-03 13:29:01.770683 9 2022-05-03 13:29:02.789693	8.8.8 mod_ping050322. 172.1;							
10 2022-05-03 13:29:02.794827	8.8.8 File Edit View		atistics Telephony Wireles					
20 2022-05-03 13:29:03.813692 21 2022-05-03 13:29:03.818940	172.1	📜 🛅 🔀 🎑 I 🔍 🔶	• 🍝 🖀 🛧 💽 📑	•••••				
22 2022-05-03 13:29:03.818940	172.1 ip.addr==8.8.8.8							× → • +
23 2022-05-03 13:29:04.835070		^ Sou		Protocol Lengtl Info				^
24 2022-05-03 13:29:05.837763 25 2022-05-03 13:29:05.842578					io (ping) request io (ping) reply		<pre>seq=9164/52259, t seq=9164/52259, t</pre>	
26 2022-05-03 13:29:06.857683	172.1: 7 2022-05-03	13:29:01.765661 172	2.18.0.3 8.8.8.8	GTP <icmp> 114 Ech</icmp>	o (ping) request	id=0x0009, :	eq=9165/52515, t	tl=128
27 2022-05-03 13:29:06.862873 28 2022-05-03 13:29:07.869659					o (ping) reply o (ping) request		eq=9165/52515, t eq=9166/52771, t	
					o (ping) request		seq=9166/52771, t	
Frame 1: 114 bytes on wire (912					o (ping) request		eq=9167/53027, t	
Ethernet II, Src: Ericsson_8b:a	a0:50 (9 <	13:29:03.818940 8.8	3.8.8 1/2.18.0.3	GIP KICMP> 114 ECr	o (ping) reply	1d=0x0009, 9	seq=9167/53027, t	>
> Destination: 66:0e:94:bc:80		ovtes on wire (912 bits	s), 114 bytes captured	(912 bits)				^
> Source: Ericsson_8b:a0:50 (Type: 802.1Q Virtual LAN (0)	(Solvall) Y Ethernet II,	Src: 66:0e:94:d3:a0:21	(66:0e:94:d3:a0:21), D		4a (66:0e:94:bc:	80:4a)		
802.1Q Virtual LAN, PRI: 1, DEI	1:0,10	n: 66:0e:94:bc:80:4a (:0e:94:d3:a0:21 (66:0e						
Internet Protocol Version 4, Sr User Datagram Protocol, Src Por	10. 192.	1Q Virtual LAN (0x8100						
GPRS Tunneling Protocol	> 802.10 Virtua	l LAN, PRI: 1, DEI: 0,						
Internet Protocol Version 4, Sr Internet Control Message Protoc	IC. 1/2.	Protocol, Src Port: 2	92.168.255.210, Dst: 19 152, Dst Port: 2152	2.168.8.104				
Type: 8 (Echo (ping) request	CO1	- Destaural						
	st) > GPRS Tunnelin	g Protocol						
Code: Ø	st) > GPRS Tunnelin; final_test_1a_ping_noipsec_test	-						- 0
Code: 0 Checksum: 0x2987 [correc	final_test_1a_ping_noipsec_test	aptop_050322_mod.pcapng	phony Wireless Tools H	elp				- 0
Code: 0 Checksum: 0x2987 [correc [Checksum Status: Good] Identifier (BE): 9 (0x00	final_test_1a_ping_noipsec_testl le Edit View Go Capture	aptop_050322_mod.pcapng Analyze Statistics Telep		elp •				- 0
Code: 0 Checksum: 0x2987 [correc [Checksum Status: Good] Identifier (BE): 9 (0x00 Identifier (LE): 2304 (0	final_test_1a_ping_noipsec_test le Edit View Go Capture	aptop_050322_mod.pcapng Analyze Statistics Telep						
Code: 0 Checksum: 0x2987 [correc [Checksum Status: Good] Identifier (BE): 9 (0x00 Identifier (LE): 2304 (0	final_test_1a_ping_noipsec_test le Edit View Go Capture I I C IIII IIIIIIIIIIIIIIIIIIIIIIIIIII	aptop_050322_mod.pcapng Analyze Statistics Telep						
Code: 0 Checksum: 0x2987 [correc [Checksum Status: Good] Identifier (BE): 9 (0x00 Identifier (LE): 2304 (0 Sequence Number (BE): 91 Sequence Number (LE): 52 No. [Response frame: 2]	final_test_la_ping_noipsec_test le Edit View Go Capture paddr==8.8.8 . Time 1 2022-05-03 16:41:46.1	aptop_050322_mod.pcapng Analyze Statistics Telep	Destination Protocol 8.8.8.8 GTP <icmp< td=""><td>Length Info > 114 Echo (pin</td><td></td><td></td><td>0/53795, ttl=128</td><td>(reply in 2</td></icmp<>	Length Info > 114 Echo (pin			0/53795, ttl=128	(reply in 2
Code: 0 Checksum: 0x2987 [correc [Checksum Status: Good] Identifier (BE): 9 (0x00 Identifier (LE): 2304 (Sequence Number (BE): 91 Sequence Number (LE): 52 No.	<pre>[final_test_la_ping_noipsec_test] le Edit View Go Capture [] [0.addr==8.8.8 . Time 1 2022-05-03 16:41:46. 2 2022-05-03 16:41:46.</pre>	aptop_050322_mod.pcapng Analyze Statistics Telep	Destination Protocol 8.8.8.8 GTP <icmp< td=""> 172.18.0.3 GTP <icmp< td=""></icmp<></icmp<>	Length Info > 114 Echo (pin > 114 Echo (pin	g) reply id=0	x0009, seq=917	0/53795, ttl=51	(reply in 2 (request in
Code: 0 Checksum: 0x2087 [correc [checksum Status: Good] Identifier (B2): 9 (0x06 Identifier (B2): 9 (0x06 Identifier (B2): 9 (0x06 Sequence Number (B2): 9 (0x06 Sequence Subters) Data (32 bytes) 00 66 0e 94 bc 80 4a	final_test_1a_ping_noipsec_test le Edit View Go Capture paddr=85.8.8 Tme 1 2022-05-03 16:41:46. 3 2022-05-03 16:41:47. 4 2022-05-03 16:41:47.	aptop_050322_mod.pcapng Analyze Statistics Teleg Source 548999936 172.18.0.3 554203815 8.8.8.8 560969849 172.18.0.3 560188398 8.8.8.8	Destination Protocol 8.8.8.8 GTP <icmp< td=""> 8.8.8.8 GTP <icmp< td=""> 8.8.8.8 GTP <icmp< td=""> 172.18.0.3 GTP <icmp< td=""></icmp<></icmp<></icmp<></icmp<>	Length Info > 114 Echo (pin > 114 Echo (pin > 114 Echo (pin > 114 Echo (pin	g) reply id=0 g) request id=0 g) reply id=0	x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51	(reply in 2 (request in (reply in 4 (request in
Code: 0 0 Checksum: 0x2087 [Correc [Checksum Status: Good] Identifier (BE): 9 (0x06 Identifier (BE): 3204 (0x06 Sequence Number (IE): 3304 Sequence Number (IE): 35 No. [Response frame: 2] Data (32 bytes) 000 66 0e 94 bc 380 4a	final_test_1a_ping_noipsec_test le Edit View Go Capture le Edit View	aptop_050322_mod.pcapng Analyze Statistics Telep Source 548999956 172.18.0.3 554203815 8.0.8.8 5569869849 172.18.0.3 56518988 8.8.8.8 55118388 172.18.0.3	Destination Protocol 8.8.8.8 GTP < CCMP	Length Info > 114 Echo (pin	g) reply id=0 g) request id=0 g) reply id=0 g) request id=0	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=128	(reply in 2 (request in (reply in 4 (request in (reply in 6
Code: 0 0 Code: 0 0 Checksum: 0x2087 [Correc [Checksum: Status: Good] Identifier (EB): 9 (0x04 Identifier (EB): 3044 (6 Sequence Number (EE): 52 No. [Response frame: 2] Data (32 bytes) > Data (32 bytes) 0 66 0e 94 bc 80 4a 10 088 00 45 38 00 60	Tinal_tett_la_ping_noipsec_test le Edit View Go Capture paddr=88.86 Ima Ima Ima 1 2022-05-03 16:41:46. 2022-05-03 16:41:47. 2 2022-05-03 16:41:47. 2022-05-03 16:41:47. 4 2022-05-03 16:41:47. 2022-05-03 16:41:47. 5 2022-05-03 16:41:47. 5 2022-05-03 16:41:47. 6 2022-05-03 16:41:47. 5 2022-05-03 16:41:47.	aptop_050322_mod.pcapng Analyze Statistics Telep Source Source S48999936 172.18.0.3 S54293815 8.8.8.8 S69969849 172.18.0.3 S66188398 8.8.8.8 S85110386 172.18.0.3 S96182704 8.8.8.8	Destination Protocol 8.8.8.8 GTP < CCMP	Langth Info > 114 Echo (pin	g) reply id=0 g) request id=0 g) reply id=0 g) request id=0 g) reply id=0	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=128 2/54307, ttl=51	(reply in 2 (request in (reply in 4 (request in (request in
Code: 0 0x287 [correc Checksum: 0x287 [correc [Checksum Status: Good] Identifier (BE): 9 (0x84 [Generative] Identifier (LE): 3344 (6 [Sequence Number (BE): 5] Sequence Number (LE): 53 No. [Response frame: 2] > Data (32 bytes) = 300 66 0e 94 bc 80 4a 10 08 00 45 38 000 60	final_test_1a_ping_noipsec_test le Edit View Go Capture le Edit View	sptop_050322_mod_pcapng Analyze Statistics Telep Source 5000000 172, 18, 0.5 172, 18, 0.5 554203815 8, 8, 8, 8 560069849 172, 18, 0.5 56108930 8, 8, 8, 8 55110386 172, 18, 0.5 590182704 8, 8, 8, 8 590182704 72, 18, 0.5 590182704 72, 18, 0.5 590182704 72, 18, 0.5 590182704 50, 27, 21, 8, 0.5 500182704 50, 27, 21, 30, 0.5 500182704 50, 5000000 50000000 50000000 50000000 50000000 50000000 50000000 50000000 50000000 50000000 50000000 500000000 500000000 5000000000 5000000000 5000000000 5000000000 5000000000 50000000000 5000000000000 5000000000000000000000 5000000000000000000000000000000000000	Destination Protocol 8.8.8.8 GTP < CCMP	Langth Info 114 Echo (pin	g) reply id=0 g) request id=0 g) reply id=0 g) request id=0 g) reply id=0 g) request id=0 g) request id=0	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=128	(reply in 2 (request in (reply in 4 (reply in 6 (request in (reply in 1
Code: 0 0 Checksum: 0x2087 [correc [Checksum: Status: Good] Identifier (EB): 3 0003 Identifier (ED): 3304 (6 Sequence Number (EE): 57 No. [Response frame: 2] Data (32 bytes) > Data (32 bytes) 000 66 0e 94 bc 80 4a 00 65 08 06 65	Inal_test_la_ping_noipsec_test le Edit View Go Copture mail Copture Copture Copture copture Copture Copture	aptop_050322_mod_pcapng Analyze Statistics Telep Source 5489999516 172,18,0.3 554203815 8,8,8,8 56060849 172,18,0.3 56108088 8,8,8,8 56080898 8,8,8,8 56110388 172,18,0.3 590182704 8,8,8,8 59078663 172,18,0.3 59078663 172,18,0.3 59086676 172,18,0.3 59086676 172,18,0.3 502866676 172,18,0.3 50286676 172,18,0.3 502866676 172,18,0.3 502866676 172,18,0.3 502866676 172,18,0.3 502866676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 50286676 172,18,0.3 5028676 172,18,0.3 5028	Destination Protocol 8.8.8.8 GTP < CICMP	Langth Info 114 Echo (pin	g) reply id=0 g) request id=0 g) reply id=0 g) request id=0 g) reply id=0 g) reply id=0 g) reply id=0 g) reply id=0 g) reply id=0	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=128 2/54307, ttl=128 2/54307, ttl=51 3/54563, ttl=128 3/54563, ttl=51 4/54819, ttl=128	(reply in 2 (request in (request in (request in (request in (request in (request in (request in 1)
Code: 0 0 Checksum: 0x2087 [correc [Checksum: Status: Good] Identifier (EB): 3 0003 Identifier (ED): 3304 (6 Sequence Number (EE): 57 No. [Response frame: 2] Data (32 bytes) > Data (32 bytes) 000 66 0e 94 bc 80 4a 00 65 08 06 65	Imal_text_la_ping_noipsec_text le Edit View Go Capture paddr=68.8.8 Image: Capture 1 2022-05-03 16:41:46. 2 2022-05-03 16:41:46. 4 2022-05-03 16:41:46. 2 0222-05-03 16:41:46. 2 0222-05-03 16:41:46. 2 0222-05-03 16:41:46. 10 2022-05-03 16:41:46. 11 2022-05-03 16:41:46. 12 2022-05-03 16:41:46. 12 2022-05-03 16:41:47.	aptop_050322_mod_pcapng Analyze Statistics Telep Source 542899995 172.18.0.3 554283815 6.8.6.8 566108039 6.8.6.8 597076663 172.18.0.3 590182764 6.8.6.8 597087665 172.18.0.3 592046561 8.8.8.6	Destination Protocol 8.8.8.8 GTP < CICWP	Longth Info 114 Echo (pin	g) reply id=0 g) request id=0 g) reply id=0	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=128 2/54307, ttl=51 3/54563, ttl=128 3/54563, ttl=51 4/54819, ttl=128	(reply in 2 (request in (request in (reply in 6 (reply in 6 (reply in 1 (reply in 1 (reply in 1 (reply in 1
Code: 0 0 Checksum: 0x2087 [correc [Checksum: Status: Good] Identifier (EB): 3 0003 Identifier (ED): 3304 (6 Sequence Number (EE): 57 No. [Response frame: 2] Data (32 bytes) > Data (32 bytes) 000 66 0e 94 bc 80 4a 00 65 08 06 65	final_text_la_ping_noipsec_text le Edit View Go Capture Josephane	statistics Telep Analyze Statistics Telep Source Source Source 542999936 172, 18, 0, 3 Source 554293815 8, 8, 8, 8 Source Source 56106398 8, 8, 8, 8 Source Source 562063815 8, 8, 8, 8 Source Source 56206384 7, 2, 18, 0, -3 Source Source 56206384 7, 2, 18, 0, -3 Source Source 592064654 1, 2, 18, 0, -3 Source Source 592064654 1, 2, 18, 0, -3 Source Source 520846441 1, 2, 18, 0, -3 Source Source 520846441 1, 2, 18, 0, -3 Source Source 5208444412 172, 18, 0, -3 Source Source 5208444412 172, 18, 0, -3 Source Source	Image: Second	C Infe 144 Echico (pin)	g) reply id=6 g) request id=6 g) request id=6 g) request id=6 g) request id=6 g) request id=6 g) request id=6 g) reply id=6 g) reply id=6 g) reply id=6 g) reply id=6	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 3/54563, ttl=128 3/54563, ttl=51 3/54563, ttl=51 3/4/54819, ttl=128 4/54819, ttl=128 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 1 (request in (reply in 2
Code: 0 0 Checksum: 0x2087 [correc [Checksum: Status: Good] Identifier (EB): 3 0003 Identifier (ED): 3304 (6 Sequence Number (EE): 57 No. [Response frame: 2] Data (32 bytes) > Data (32 bytes) 000 66 0e 94 bc 80 4a 00 65 08 06 65	Inal_tex_la_ping_noipsec_text le Edit View Go Capture main Co Capture Capture 1 2022-05-03 16:41:46. Capture 2022-05-03 16:41:47. Capture Capture 2022-05-03 16:41:47. </td <td>aptop_050322_mod_pcapng Analyze Statistics Telep Source Source Statestop</td> <td>Image: Constraints Operation B.8.8.8.8 GTP < CLCMP</td> B.8.8.8.8 GTP < CLCMP	aptop_050322_mod_pcapng Analyze Statistics Telep Source Source Statestop	Image: Constraints Operation B.8.8.8.8 GTP < CLCMP	Langth Infe 114 Echo (pin) 114 Echo (pin)	g) reply id=6 g) request id=6 g) reply id=6 g) request id=6	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code:0 0 Code:0 0 Checksum Status: Good] Identifier (B1): 300 Identifier (B1): 3304 (G Sequence Number (B2): 57 No. Response frame:12 1 > Data (32 bytes) 1 > 000 66 06 94 bc 80 4a 100 683 00 60	Inal_tex_ls_ping_noipsec_text le Edit View Go Capture lpsddr=#Edit Image: Capture Image: Capture Image: Capture lpsddr=#Edit Image: Capture Image: Capture Image: Capture lpsddr=#Edit Image: Capture Image: Capture Image: Capture lpsddr=#Edit 2022-05-03 16:41:46. 2022-05-03 16:41:47. 2022-05-03 16:41:47. 2022-05-03 16:41:47. 2022-05-03 16:41:47. 12:022-05-03 16:41:47. 12:022-05-03 16:41:47. 12:022-05-03 16:41:47. 12:0222-05-03 16:41:47. 12:022-05-03 16:41:47. 12:022-05-03 16:41:47. 12:0222-05-03 16:41:47. 12:022-05-03 16:41:41. 14:47. 12:0222-05-03 16:41:47. 12:022-05-03 16:41:41. 14:47. 12:0222-05-03 16:41:41. 16:41:41. 16:41:41. 16:41:41. 12:022-05-03 16:41:41. 16:41:41. 16:41:41. 16:41:41. 12:022-05-03 16:41:41	aptop_050322_mod_pcapng Analyze Statistics Telep Source Source Statestop	Image: Second	Langth Infe 114 Echo (pin) 114 Echo (pin)	g) reply id=6 g) request id=6 g) reply id=6 g) request id=6	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 3/54563, ttl=128 3/54563, ttl=51 3/54563, ttl=51 3/4/54819, ttl=128 4/54819, ttl=128 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 Checksum Status: Good Identifier (BL): 9 (9) vol Identifier (BL): 9 (9) vol Identifier (BL): 9 (9) vol Identifier (BL): 9 (9) vol Sequence Number (BL): 5 [Response frame: 2] Data (32 bytes) 000 66 0e 94 bc 80 4a 100 08 00 45 38 00 60 2 Internet Protocol Version 4: Proto	Inal_test_la_ping_noipsec_test le Edit View Go Capture lp_addr==0.100 Image: Capture Image: Capture Image: Capture lp_addr==0.100 Image: Capture Image: Capture Image: Capture lp_addr==0.100 Image: Capture Image: Capture Image: Capture Image: Capture lp_addr==0.100 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Capture Image: Capture lp_2022=05-03 Image: Capture Image: Capture Image: Captu	statistics Telep Analyze Statistics Telep Source Source Source 540999951 Source Source 554203815 8.8.8.8 Sobe96894 T.2.18.0.3 556108398 8.8.8.8 Sob96849 T.2.18.0.3 590182704 8.8.8.8 Sob966676 T.2.18.0.3 50204561 6.8.8.8 Sob966676 T.2.18.0.3 510018663 R.8.8.8 Sob966676 T.2.18.0.3 52104412 T.2.18.0.3 Sub41545 A.8.8.8 521044412 T.2.18.0.3 Sub41545 A.8.8.8 541165491 T.2.18.0.3 Sub41545 T.2.18.0.3 541165491 T.2.18.0.3 Sub41545 T.2.18.0.3 541165491 K.8.8.8 Sub41545 K.8.8.8	Destination Protocol 8.8.8.8 GTP < LCHP	Langth Info 114 Echo (pin) 114 Echo (pin)	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 Code: 0 Checksum 8x2987 [Correc Checksum 8x2987 [Correc [Checksum Status: Good] Identifier (BL): 9 (9x84) Identifier (BL): 39 (9x84) Identifier (BL): 58 (9x84) Sequence Number (BL): 58 (9x84) Identifier (BL): 58 (9x84) 000 66 00 94 bc 80 4a) 045 38 00 60 000 66 00 45 38 00 60 2 2 Internet Protocol Version 4: Protocol	final_text_la_ping_noipsec_text le Edit View Go Copture mail Copture Copture Copture 1 2022-05-03 I6:41:46. Cop22-05-03 I6:41:47. 1 2022-05-03 I6:41:47. Cop22-05-03 I6:41:47. 1 2022-05-03 I6:41:47. I:2022-05-03 I6:41:47. 1 2022-05-03 I	aptop.050322_mod.pc.apng Analyze Statistics Tele Source Source Source 540999951 7.2.18.0.3 Source 554203815 8.8.8.8 Sobores 5510386 7.2.18.0.3 Source 590182704 8.8.8.8 Sobores 590182704 8.8.8.8 Sobores 50204561 8.8.8.8 Sobores 502045621 7.2.18.0.3 Sobores 52104412 7.2.18.0.3 Sobores 52104412 7.2.18.0.3 Sobores 52104412 7.2.18.0.3 Sobores 541165491 17.2.18.0.3 Sobores 541165491 7.2.18.0.3 Sobores 541165491 7.2.18.0.3 Sobores 541165491 7.2.18.0.3 Sobores 54204412 7.2.18.0.3 Sobores 542165491 8.8.8.8 Sobores 542165491 1.2.18.0.3 Sobores 542165491 1.0.60000000000000000000000000000000000	Image: Constraints Image: Constraints Destination Protocol 8.8.8.8 GTP < CICMP	Image Image > 114 Echo (pin	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 • Code: 0 • Checksum Status: Good • Identifier (BL): 2304 (6) • Sequence Number (ED): 35 No. • Iteratifier (LL): 2304 (6) • Dota (32 bytes) • Dota (32 bytes) • Other (6) 06 30 80 00 Iteratifier Protocol Venion 4: Protocol Venion 4: Protocol Venion 4: Protocol	final_tex_la_ping_noipsec_text le Edit View Go Capture use Capture	aptop_050322_mod_pcapng Analyze Statistics Tele Source 548999936 172.18.0.3 554203815 8.8.8.8 560060840 172.18.0.3 56106398 8.8.8.8 58110356 172.18.0.3 56206367 172.18.0.3 502066678 172.18.0.3 502066678 172.18.0.3 502066678 172.18.0.3 521044412 172.18.0.3 521641845 6.8.8 541165491 172.18.0.3 54161845 6.8.8 54161845 6.8.8 54161845 6.8.8 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 55204541	Image: Second	Image Image > 114 Echo (pin	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 • Code: 0 • Checksum Status: Good • Identifier (BL): 2304 (6) • Sequence Number (ED): 35 No. • Iteratifier (LL): 2304 (6) • Dota (32 bytes) • Dota (32 bytes) • Other (6) 06 30 80 00 Iteratifier Protocol Venion 4: Protocol Venion 4: Protocol Venion 4: Protocol	Inal_tex_la_ping_noipsec_text le Edit View Go Capture le Edit View Go Capture le Dit View Capture <td>aptop_050322_mod_pcapng Analyze Statistics Tele Source 548999936 172.18.0.3 554203815 8.8.8.8 560060840 172.18.0.3 56106398 8.8.8.8 58110356 172.18.0.3 56206367 172.18.0.3 502066678 172.18.0.3 502066678 172.18.0.3 502066678 172.18.0.3 521044412 172.18.0.3 521641845 6.8.8 541165491 172.18.0.3 54161845 6.8.8 54161845 6.8.8 54161845 6.8.8 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 55204541</td> <td>Image: Constraint of the second sec</td> <td>Image Image > 114 Echo (pin > 114 Echo (pin</td> <td>g) reply id= g) request id= g) reply id= g) request id= g) reply id=</td> <td>x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917</td> <td>0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51</td> <td>(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2</td>	aptop_050322_mod_pcapng Analyze Statistics Tele Source 548999936 172.18.0.3 554203815 8.8.8.8 560060840 172.18.0.3 56106398 8.8.8.8 58110356 172.18.0.3 56206367 172.18.0.3 502066678 172.18.0.3 502066678 172.18.0.3 502066678 172.18.0.3 521044412 172.18.0.3 521641845 6.8.8 541165491 172.18.0.3 54161845 6.8.8 54161845 6.8.8 54161845 6.8.8 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 54161845 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 5520454141 172.18.0.3 55204541	Image: Constraint of the second sec	Image Image > 114 Echo (pin	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 Checksum 8x2987 [Correc [Checksum 8x2987 [Correc [Checksum 5x41us: Good] Identifier (E): 2046 (K Sequence Number (E): 55 Nota (32 bytes) Data (32 bytes) 2 Data (32 by	Inal_tex_la_ping_noipsec_text le Edit View Go Capture main Image: Ca	aptop.050322_mod.pc.apng Analyze Statistics Telep Source 5409999516 172.18.0.3 554203815 8.8.8.8 556108308 8.8.8.8 556108308 8.8.8.8 556108308 8.8.8.8 556108308 172.18.0.3 560108308 8.8.8.8 590182704 8.8.8.8 590182704 8.8.8.8 590182704 8.8.8.8 590182704 8.8.8.8 590182641 8.8.8 5004642 172.18.0.3 5104442 172.18.0.3 54034584 8.8.8.8 94:d3:a0:21 (66:0e:941 1, DET: 0, ID: 1001 n 4, Src: 172.18.0.3 FC Port: 1252, DSt Po	Image: Constraint of the second sec	Image Image > 114 Echo (pin	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 Checksum 8x2987 [Correc [Checksum 8x2987 [Correc [Checksum 5x41us: Good] Identifier (E): 2046 (K Sequence Number (E): 55 Nota (32 bytes) Data (32 bytes) 2 Data (32 by	final_tex_la_ping_noipsec_text le Edit View Go Capture le 2022-05-03 16:41:46. la 2022-05-03 16:41:46. la 2022-05-03 16:41:45. la 2022-05-03	aptop_050322_mod_pcapng Analyze Statistics Telg Source Source Source 548999936 172,18,0.3 Source 554203815 8,8,8,8 Source Source 56180398 6,8,8,8 Source Source 590182704 6,8,8,8 Source Source 50180398 6,8,8,8 Source Source 501976683 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 501986491 172,18,0,3 Source Source 50141845 6,8,8,8 Source Source 50141841 192,168,255 Source Source 61431280121 (66:0e:94:1) 1, 92,168,255 Source 701712152, Dst Poor Norce Source Source	Image: Constraint of the second sec	Image Image > 114 Echo (pin	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2
Code: 0 Checksum 8x2987 [Correc [Checksum 8x2987 [Correc [Checksum 8x2987 [Correc [Checksum 5x47133 [Correc [Checksum 5x47133 [Correc] Identifier (16): 2304 (1 Sequence Rubber (16): 55 Security 10 (10) (10) (10) (10) (10) (10) (10) (Inal_tex_la_ping_noipsec_text le Edit View Go Capture main Image: Ca	aptop_050322_mod_pcapng Analyze Statistics Telg Source Source Source 548999936 172,18,0.3 Source 554203815 8,8,8,8 Source Source 56180398 6,8,8,8 Source Source 590182704 6,8,8,8 Source Source 50180398 6,8,8,8 Source Source 501976683 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 50198647 172,18,0,3 Source Source 501986491 172,18,0,3 Source Source 50141845 6,8,8,8 Source Source 50141841 192,168,255 Source Source 61431280121 (66:0e:94:1) 1, 92,168,255 Source 701712152, Dst Poor Norce Source Source	Image: Constraint of the second sec	Image Image > 114 Echo (pin	g) reply id= g) request id= g) reply id= g) request id= g) reply id=	x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917 x0009, seq=917	0/53795, ttl=51 1/54051, ttl=128 1/54051, ttl=51 2/54307, ttl=51 2/54307, ttl=128 2/54563, ttl=128 3/54563, ttl=128 4/54819, ttl=51 5/55075, ttl=51 5/55075, ttl=51	(reply in 2 (request in (reply in 4 (request in (reply in 6 (request in (reply in 1 (request in (reply in 2 (request in (reply in 2

Figure 7: RAN-Side Captures on Untrusted Link: Eavesdropped/Captured Packets; Modified Packets; Injected Packets

Figure 8 and Figure 9 show the relevant packet captures when the ping is stopped on the UE, but the captured packets are modified and injected into the untrusted link. Figure 8 shows the packets captured at the output of the RAN-side switch facing the LTE core (TP4). Figure 9 shows the packet captures at the core-side router (TP5), which includes the traffic captured at the tunnel endpoint (ingress R6K interface) and on the interface toward the SGW/internet (egress/clear R6K interface). Note that, although the UE is not sending any ping packets, the same ICMP traffic is visible at all test points, and, specifically, the ping packets are completely decipherable on the untrusted link. Figure 9 further shows that modified ping packets are received on the ingress R6K interface on the core side, and ping packets (reply and request) are seen on the egress interface of R6K with the correct control codes.

final_test_1a_ping_noipsec_pluribus_050	0322_mod.pcapng				_	
File Edit View Go Capture Analy	ze Statistics Telephony Wir	eless Tools Help				
🖉 🔳 🖉 🕲 📜 🛅 🕱 🞑 🗎	९ 👄 👄 🖀 🖝 速 📃	📃 Q, Q, Q, 🎹				
ip.addr==8.8.8.8						× -> -> +
No. Time	Source Destination	Protocol Lengti Info				
498 2022-05-03 16:41:01.827788	172.18.0.3 8.8.8.8	GTP <icmp> 160 Echo</icmp>	(ping) request id=0x0	009, seq=9164/52259,	ttl=128 (reply in	500)
 500 2022-05-03 16:41:01.832830 	8.8.8.8 172.18.0.3	GTP <icmp> 160 Echo</icmp>	(ping) reply id=0x0	009, seq=9164/52259,	ttl=51 (request in	498)
514 2022-05-03 16:41:02.843743	172.18.0.3 8.8.8.8	GTP <icmp> 160 Echo</icmp>	(ping) request id=0x0	009, seq=9165/52515,	ttl=128 (reply in	516)
516 2022-05-03 16:41:02.848633	8.8.8.8 172.18.0.3	GTP <icmp> 160 Echo</icmp>	(ping) reply id=0x0	009, seq=9165/52515,	ttl=51 (request in	514)
549 2022-05-03 16:41:03.867612	172.18.0.3 8.8.8.8	GTP <icmp> 160 Echo</icmp>	(ping) request id=0x0	009, seq=9166/52771,	ttl=128 (reply in	551)
551 2022-05-03 16:41:03.872887	8.8.8.8 172.18.0.3	GTP <icmp> 160 Echo</icmp>	(ping) reply id=0x0	009, seq=9166/52771,	ttl=51 (request in	549)
580 2022-05-03 16:41:04.891746	172.18.0.3 8.8.8.8	GTP <icmp> 160 Echo</icmp>	(ping) request id=0x0	009, seq=9167/53027,	ttl=128 (reply in	582)
582 2022-05-03 16:41:04.896965	8.8.8.8 172.18.0.3	GTP <icmp> 160 Echo</icmp>	(ping) reply id=0x0	009, seq=9167/53027,	ttl=51 (request in	580)
592 2022-05-03 16:41:05.907542	172.18.0.3 8.8.8.8	GTP <icmp> 160 Echo</icmp>	(ping) request id=0x0	009, seq=9168/53283,	ttl=128 (reply in	594)
<						>
> Frame 498: 160 bytes on wire (Ethernet II, Src: 66:00:94:bc: > Internet Protocol Version 4, 5 > User Datagram Protocol, Src Pc > Virtual extensible Local Area > Ethernet II, Src: 66:00:94:bc: > Internet Protocol Version 4, 5 > User Datagram Protocol, Src Pc GPRS Tunneling Protocol > Internet Protocol Version 4, 5 > Internet Control Version 4, 5 > Internet Control Nessage Protocol	<pre>88:4a (66:0e:94:bc:88:4a) irc: 128.8.46.80, Dst: 10 irc: 59324, Dst Port: 4789 Network 88:4a (66:0e:94:bc:88:4a) irc: 192.168.255.210, Dst: ort: 2152, Dst Port: 2152 irc: 172.18.0.3, Dst: 8.8. ircl</pre>	<pre>, Dst: Cisco_ff:fc:68 (00 205.67.130 , Dst: 66:0e:94:d3:a0:21 192.168.8.104</pre>	ð:08:e3:ff:fc:68)		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
Type: 8 (Echo (ping) reque	st)					
0000 00 08 e3 ff fc 68 6 0010 00 92 f1 2b 00 00 02 f1 2b 00 00 02 f1 2b 50 00 00 00 02 f1 32 e7 b5 0 00 03 62 04 d3 2a e7 b5 0 03 03 03 03 03 03 04 d3 2a 04 d3 04 d5 38 00 60 04 b7 03 04 d5 38 00 60 04 b7 03 04 d5 38 04 60 04 b7 03 04 d5 24 a5 58 d7 45 60 04 04 d5 38 04 63 88 04 d6 d6 d6 a5 a5 a5 a5 a5<	0 11 8c 50 80 08 2e 0 7e 00 00 08 00 00 0 21 66 0e 94 bc 80 0 00 fd 11 28 12 c0 8 68 00 4c 86 42 30 0 3c 90 1e 00 00 80	50 0a cd 00 00 00 4a 08 00 a8 ff d2 ff 00 3c 01 ee 7d				

Figure 8: RAN-side Untrusted Link Capture on Outgoing Port Toward Core

									_ □	×
test1A2-MITRE-r6k-noipsec-050322-										^
File Edit View Go Capture Ar	alyze Statistics Te	lephony Wireless								
🥂 🔳 🖉 💿 📜 🛅 🗙 🗳	। 🤇 🖛 🌧 🖺	🛉 生 📃 📗	⊕, ⊖, 0	2. 11						
ip.addr==8.8.8.8										+
No. Time 191 2022-05-03 16:41:00.5127 193 2022-05-03 16:41:01.528	15 172.18.0.3 53 8.8.8.8 54 172.18.0.3 89 8.8.8.8 46 172.18.0.3 22 8.8.8 90 172.18.0.3 18 8.8.8 18 8.8.8	8.8.8.8 G 172.18.0.3 G 8.8.8.8 G 172.18.0.3 G	TP <icmp> TP <icmp> TP <icmp> TP <icmp> TP <icmp> TP <icmp> TP <icmp> TP <icmp> TP <icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp>	ngt Info 114 Echo (pin 114 Echo (pin	<pre>;) reply ;) request ;) reply ;) request ;) reply ;) request ;) reply</pre>	id=0x0009, id=0x0009, id=0x0009, id=0x0009, id=0x0009, id=0x0009, id=0x0009,	seq=9164/52259, seq=9164/52259, seq=9165/52515, seq=9166/52771, seq=9166/52771, seq=9167/53027, seq=9167/53027, seq=9168/53283,	ttl=51 (red ttl=128 (red ttl=51 (red ttl=128 (red ttl=51 (red ttl=128 (red ttl=51 (red	uest in 191) eply in 203) uest in 201) eply in 207) uest in 205) eply in 229) uest in 227)	^
233 2022-05-03 16:41:04.5979 235 2022-05-03 16:41:05.6006				114 Echo (pin 114 Echo (nin			seq=9168/53283, sea=9169/53539.			~
> Internet Protocol Vers: —		4:d3:a0:21), Ds r-050322-1640.pcap	st: Ericsson		ss Tools H					
	addr==8.8.8.8									
Phackerm Burdler Burdler 1 0000 98 7a 10 85 91 2 0010 08 00 45 38 06 - 2 0020 ff d2 c0 a8 08 - 2 2 ************************************	Time 10 2022-05-03 16: 12 2022-05-03 16: 10 2022-05-03 16: 12 2022-05-03 16: 14 2022-05-03 16: 16 2022-05-03 16: 16 2022-05-03 16: 16 2022-05-03 16: 16 2022-05-03 16: 17 202-05-03 16: 17 202-05-05-05-05-05-05-05-05-05	41:00.514948 41:01.525986 41:01.530786 41:02.549841 41:02.555148 41:03.573896	Source 172.18.0.3 8.8.8.8 172.18.0.3 8.8.8.8 172.18.0.3 8.8.8.8 172.18.0.3 8.8.8 172.18.0.3 8.8.8	172.18.0.3	Protocol GTP <icmp> GTP <icmp> GTP GT</icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp></icmp>	114 Echo 114 Echo 114 Echo 114 Echo 114 Echo 114 Echo 114 Echo	(ping) request (ping) reply (ping) request (ping) reply (ping) reply (ping) reply (ping) request (ping) reply	id=0x0009, id=0x0009, id=0x0009, id=0x0009, id=0x0009, id=0x0009,	seq=9164/52259, seq=9164/52259, seq=9165/52515, seq=9165/52515, seq=9166/52771, seq=9166/52771, seq=9167/53027,	, ttl: , ttl: , ttl: , ttl: , ttl: , ttl:
> E > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1 > 1	Code: 0 Checksum: 0x29 [Checksum Stat Identifier (BE Identifier (LE	Ericsson_85:91 J, PRI: 0, DEI: Version 4, Srcc cacol, Src Port btocol Version 4, Srcc tessage Protoco (ping) request; 86 [correct] us: Good]): 9 (0x0009)): 2304 (0x0009)	:c9 (98:7a:1 0, ID: 3704 : 192.168.25 : 2152, Dst : 172.18.0.3 1)	0:85:91:c9), 5.210, Dst: 1 Port: 2152 , Dst: 8.8.8.	Dost: fa:16: 92.168.8.10	3e:7a:b7:81	(fa:16:3e:7a:b7	::81)		
000 001 002	0 08 00 45 3		9f 00 00	91 c9 81 0 fb 11 39 2 00 4c 86 4	9 c0 a8					
0	test1A2-MITRE-r6k	clear-050322-1640.pca	p					Packets: 396	· Displayed: 60 (15.2%)	

Figure 9: Core-Side Untrusted Link Capture and Core-Side (Trusted) Router Capture

Objective 2: Verify inability to eavesdrop, modify, inject payload on UP

As organized in Figure 7 above, Figure 10 displays three windows: two PCAP files corresponding to the captured packets and modified packets (where, again, the MAC address has been modified), and one PCAP file corresponding to the capture of the injected packets at TP4. As can be seen in the figures, traffic is indistinguishable as it all appears as encrypted (ESP) packets. There are no ICMP packets indicated, nor is there any indication of what traffic is control plane traffic. The source and destination IP addresses shown in the Wireshark windows are those of the endpoints of the IPsec tunnel. For reference on this and subsequent figures, Table 7 lists the files whose data are shown in the figures along with a description of the contents.

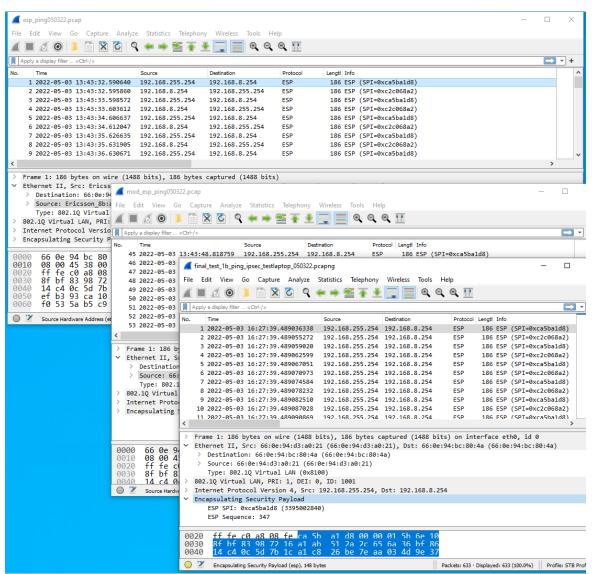


Figure 10: RAN-Side Untrusted Link Capture of Encrypted Traffic, Modification of Packets, and Injected Packets

Table 7: Test Case 1 Raw Data Files and Content Descriptions When IPsec Implemented on Untrusted Link

TLP:WHITE:5GSTB

5G STB Report Based on CSRIC VII Recommendations

File Name	Contents
esp_ping_050322.pcap	Captured ESP traffic at TP3
mod_esp_ping050322.pcap	Modified ESP traffic
final_test_1b_ping_ipsec_testlaptop_050322.pcapng	Injected ESP traffic at TP3
final_test_1b_ping_ipsec_pluribus_050322.pcapng	Injected traffic captured at TP4 on outgoing
	RAN-side switch interface toward LTE core
test1B-MITRE-r6k-ipsec-050322-1626.pcap	Traffic captured at TP5 on core-side ingress
	R6K interface from RAN
test1B-MITRE-r6k-clear-050322-1626.pcap	Traffic captured at TP5 on core-side egress
	R6K interface toward internet
final_test_1b_ping_ipsec_R6K_050322.pcapng	Traffic captured at TP2 on RAN-side ingress
	R6K interface

Figure 11 shows the packet captures at the port of the RAN-side switch that faces the LTE core (TP4) and at the core-side router (TP5). Again, we cannot distinguish between the traffic that exists, for example, due to control plane messages between the RAN and the core and the injected encrypted packets. We do know, though, that the injected packets, which contained ping packets from the UE, do not exit the IPsec tunnel. The third window in Figure 11 demonstrates this, showing that no packets arrive at the ping destination address, 8.8.8.8. That is, modified ESP packets are received on the ingress R6K interface on the core side (TP5), but ping packets are not seen on the egress interface (also TP5), which indicates that the modified and injected UP packets were dropped at the tunnel endpoint. In addition, Figure 12 shows traffic on the RAN-side R6K (TP2), filtered for IP address 8.8.8.8, indicating that no ICMP traffic exists outside the tunnel on the RAN side either. Specifically, 652 ESP packets are received at the core within the IPsec tunnel, but only 44 packets are detected on the egress R6K interface at the core. None of those packets are ICMP packets, which the injected traffic contained. On the RAN side, of the 105 packets captured on the ingress interface, none were ICMP packets.

TLP:WHITE:5GSTB

🔳 🖉 🛞 📙 🗎 🗙 🏹 🤇	• 🖛 🔫 🔛 .	v 💶 🔳 🔍 '	Q Q !		
sp					$\times \rightarrow \bullet$ +
Time	Source	Destination	Protocol	Lengtl Info	
81 2022-05-03 16:26:27.222328	192.168.255.254	192.168.8.254	ESP	232 ESP (SPI=0xca5ba1d8)	
82 2022-05-03 16:26:27.222328	192.168.255.254	192.168.8.254	ESP	232 ESP (SPI=0xc2c068a2)	
83 2022-05-03 16:26:27.222328 84 2022-05-03 16:26:27.222328	192.168.255.254 192.168.255.254	192.168.8.254 192.168.8.254	ESP	248 ESP (SPI=0xc2c068a2) 248 ESP (SPI=0xca5ba1d8)	
85 2022-05-03 16:26:27.222328		192.168.8.254	ESP	232 ESP (SPI=0xca5ba1d8)	
86 2022-05-03 16:26:27.222328	192.168.255.254	192.168.8.254	ESP	232 ESP (SPI=0xc2c068a2)	
	192.168.255.254	192.168.8.254	ESP	232 ESP (SPI=0xca5ba1d8)	
88 2022-05-03 16:26:27.222328		192.168.8.254	ESP	232 ESP (SPI=0xc2c068a2)	
89 2022-05-03 16:26:27.222328 90 2022-05-03 16:26:27.222328		192.168.8.254 192.168.8.254	ESP	232 ESP (SPI=0xca5ba1d8) 232 ESP (SPI=0xc2c068a2)	
test1B-MITRE-r6k-ipsec-050322-1626.pc		192.100.0.294	231		- 0
		Mondana Tl-	l.l.e.l.e		_
Edit View Go Capture Analyz			Help		
	९ 🗢 🔿 🖺 🗿	👱 📃 🔍	Q Q !		
Apply a display filter <ctrl-></ctrl->					
Time	Source	Destination	Protocol	Lengti Info	
14 2022-05-03 16:26:35.313439	192.168.255.254	192.168.8.254	ESP	202 ESP (SPI=0xca5ba1d8)	
15 2022-05-03 16:26:35.313441	192.168.255.254	192.168.8.254	ESP	186 ESP (SPI=0xc2c068a2)	
16 2022-05-03 16:26:35.313442 17 2022-05-03 16:26:35.313444	192.168.255.254 192.168.255.254	192.168.8.254 192.168.8.254	ESP ESP	186 ESP (SPI=0xc2c068a2) 186 ESP (SPI=0xc2c068a2)	
18 2022-05-03 16:26:35.313444	192.168.255.254	192.168.8.254	ESP	186 ESP (SPI=0xc2c068a2) 186 ESP (SPI=0xc2c068a2)	
19 2022-05-03 16:26:35.313448	192.168.255.254	192.168.8.254	ESP	202 ESP (SPI=0xca5ba1d8)	
20 2022-05-03 16:26:35.313457	192.168.255.254	192.168.8.254	ESP	202 ESP (SPI=0xc2c068a2)	
21 2022-05-03 16:26:35.313459	192.168.255.254	192.168.8.254	ESP	186 ESP (SPI=0xc2c068a2)	
22 2022-05-03 16:26:35.313471 23 2022-05-03 16:26:35.313473	192.168.255.254 192.168.255.254	192.168.8.254 192.168.8.254	ESP ESP	186 ESP (SPI=0xc2c068a2) 186 ESP (SPI=0xc2c068a2)	
24 2022-05-03 16:26:35.313476		192.168.8.254	ESP	186 ESP (SPI=0xc2c068a2)	
25 2022-05-03 16:26:35.313486	192.168.255.254	192.168.8.254	ESP	186 ESP (SPI=0xc2c068a2)	
26 2022-05-03 16:26:35.313488	192.168.255.254	192.168.8.254	ESP	122 ESP (SPI=0xc2c068a2)	
27 2022-05-03 16:26:35.313489	192.168.255.254	192.168.8.254	ESP	186 ESP (SPI=0xca5ba1d8)	
28 2022-05-03 16:26:35.313496	192.168.255.254	192.168.8.254	ESP	186 ESP (SPI=0xca5ba1d8)	
					>
Frame 19: 202 bytes on wire (1					
Ethernet II, Src: 66:0e:94:d3:		:a0:21), Dst: Eri	csson_85:91:d	5 (98:7a:10:85:91:d5)	
802.1Q Virtual LAN, PRI: 0, DE Internet Protocol Version 4, S		4. Dst: 192.168.8	.254		
Encapsulating Security Payload		.,			
a0 e8 e8 ef 92 3e e8 ec	- d5 73 71 0e	74 a0 66 14 4	lc		
b0 44 ff 73 00 2c a2 6c		d9 b0 20 41 7			
c0 3b 71 8a 29 0d f2 42	2 31 91 99				
test1B-MITRE-r6k-ipsec-050322-1626.pc	cap			Packets: 652 · Displayed: 652 (100.0%)	Profile: STB Profi
📕 🚄 test1B-MITRE-r6k-clear-050322-	1626.pcap				-
File Edit View Go Capture	Analyze Statistics	Telephony Wireless	Tools Help		
				TT	
	🎑 🔍 🔶 📄	= • × 📃	ଇ ର ର	• ==	
ip.addr==8.8.8.8					\boxtimes

Figure 11: RAN-Side Outgoing Link to Core; Core-Side Untrusted Link Capture of Encrypted Traffic; and Core-Side Capture at Trusted Router after Decryption

TLP:WHITE:5GSTB

	final_test_1b_p	ing_ipsec_R6K_	050322.pcapng							-		×
					eless Tools Help							
	. 🦉 🔘	🗎 🗙 🙆	م 🗢 🗢 🖀 🗿	۹ 📃 🛃	Q. Q. 🎹							
	addr==8.8.8.8										$\times \rightarrow$	- +
No.	Time		Sour	ce	Destination	Protocol	Lengt Info					
<												
			K 050322.ncanno					Packets: 105 · Displayed: 0 (0	.0%)	Prof	file: STR Pi	rofile

Figure 12: RAN-Side Router Packet Capture Showing No ICMP Packets to or from 8.8.8.8

Test Result

Success: When the IPsec tunnel is implemented on the untrusted link, an eavesdropper cannot read the traffic over the link (it all appears as ESP encrypted packets with source and destination addresses as the endpoints of the tunnel); modification and injection of packets fail to pass out of the tunnel. When IPsec is not implemented, the content of the packets on the untrusted link are decipherable, and injected packets appear to pass through to the internet.

Test Case 2, TC-IPsec-02

The objective of TC-IPsec-02 is to verify that, with an IPsec tunnel between the RAN and the LTE core, packets cannot be read, modified, or injected on the control plane. It also demonstrates that, in the absence of IPsec tunnel, injected control plane traffic gets passed through, although the core appears to reject some replayed packets.

Objective: Verify inability to eavesdrop, modify, or inject payload on CP

As in previous sections, Table 8 lists the files used to store packet captures where those file names are shown in the headers of the Wireshark windows.

Table 8: Test Case 2 Raw Data Files and Content Descriptions for Runs with and without IPsec Encryption on Untrusted Link

File Name	Contents
control050322.pcap	Captured control traffic at TP3
mod_control050322.pcap	Modified control traffic
final_test_2a_control_noipsec_testlaptop_050322.pcapng	Injected control traffic captured at
	TP4 on outgoing interface to LTE core
test2A-MITRE-r6k-noipsec-041922-1615.pcap	Traffic captured at TP5 on core-side
	ingress R6K interface from RAN
test2A-MITRE-r6k-clear-041922-1632.pcap	Traffic captured at TP5 on core-side
	egress R6K interface toward MME
final_test_2a_control_noipsec_R6K_050322.pcapng	Traffic from core captured at TP2 on
	RAN-side R6K trusted interface
mod_esp_control_050322.pcap	Modified ESP encrypted control traffic
final_test_2b_control_ipsec_testlaptop_050322.pcapng	Injected ESP encrypted control traffic
	at TP3
final_test_2b_control_ipsec_pluribus_050322.pcapng	Injected ESP encrypted control traffic
	captured at TP4 on outgoing interface
	to the core
test2B-MITRE-r6k-ipsec-050322-1628.pcap	ESP encrypted control traffic
	captured at TP5 on core-side egress
	R6K interface toward internet
test2B-MITRE-r6k-clear-050322-1628.pcap	Decrypted control traffic captured at
	TP5 on core-side egress R6K interface
	toward MME
final_test_2b_control_ipsec_R6K_050322.pcapng	Decrypted control traffic from core
	captured at TP2 on RAN-side R6K
	trusted interface

In Figure 13, the first window shows the captured packets from the natural operation of the system (in this case, control messages between the RAN and the LTE core), without the IPsec tunnel; the second window shows modified packets (here restricted to the control packets from the RAN address, 192.168.255.226, to the MME address, 192.168.8.136); and the third window shows the packets as captured on the switch on the untrusted link, which now includes injected packets. Unlike Test Case 1, where we stopped the UE pings, we are unable to stop the flow of control plane messages in the absence of the IPsec tunnel.

🚄 control050322.pcap					
				—	
File Edit View Go Capture An					
🛋 🔳 🖉 💿 📜 🛅 🗙 🙆	। ९ 🗢 🏓 🖺 👔	. 🛉 📑 🖬 🖉 🖻	L 🔍 🎹		
Apply a display filter <ctrl-></ctrl->					
No. Time	Source	Destination	Protocol	Lengtl Info	^
8 2022-05-03 13:31:38.1584 9 2022-05-03 13:31:48.7628			SCTP SCTP	130 HEARTBEAT_ACK 130 HEARTBEAT	
10 2022-05-03 13:31:48.7661		192.168.255.226	SCTP	130 HEARTBEAT_ACK	
11 2022-05-03 13:32:07.3026		192.168.255.226	SCTP	130 HEARTBEAT	
12 2022-05-03 13:32:07.3027 13 2022-05-03 13:32:19.4394		192.168.8.137 192.168.255.226	SCTP SCTP	130 HEARTBEAT_ACK 130 HEARTBEAT	
14 2022-05-03 13:32:19.4409			SCTP	130 HEARTBEAT_ACK	
15 2022-05-03 13:32:19.76294			SCTP	130 HEARTBEAT	
16 2022-05-03 13:32:19.7654 17 2022-05-03 13:32:26.8572		192.168.255.226 192.168.255.226	SCTP SCTP	130 HEARTBEAT_ACK 130 HEARTBEAT	
18 2022-05-03 13:32:26.8589			SCTP	130 HEARTBEAT_ACK	
19 2022-05-03 13:32:36.4907	91 192.168.8.136	192.168.255.226	SCTP	130 HEARTBEAT	
20 2022-05 mod_control05032	22.pcap				- 🗆
File Edit View O	Go Capture Analyze	Statistics Telephony \	Nireless Tools He	lp	
> Frame 1: 1 > Ethernet I) 🕅 🕅 🖉 🦳	🌰 📦 💇 🛣 🎍 🗖			
802 10 Vin				• 11	
> Internet P	<ctrl-></ctrl->	C -111-11	Destination	Destand 1 1 1 1	
V Stream Con No. Time 6 2022-05-03	13:31:36.172475	Source 192.168.255.226	Destination 192.168.8.136	Protocol Lengtl Info SCTP 130 HEARTBEAT_AC	к
bource	13:31:38.158274	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT	
Verific 8 2022-05-03	13:31:38.158458	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT_ACK	к
	13:31:48.762893 13:31:48.766127	192.168.255.226 192.168.255.226	192.168.8.136 192.168.8.136	SCTP 130 HEARTBEAT SCTP 130 HEARTBEAT ACH	v
0010 08 0 11 2022-05-03	13:32:07.302690	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT	r l
	13:32:07.302747	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT_ACH	к
Control	13:32:19.439478 13:32:19.440900	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT	v
	13:32:19.762942	192.168.255.226 192.168.255.226	192.168.8.136 192.168.8.136	SCTP 130 HEARTBEAT_ACH SCTP 130 HEARTBEAT	r.
	13:32:19.765496	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT_AC	к
	13:32:26.857215 13:32:26.858939	192.168.255.226 192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT	K
			192.168.8.136	SCTP 130 HEARTBEAT_ACH	N III
19 2022-05-03	15:52:56.490/91	192.168.255.226	192.168.8.136	SCTP 130 HEARTBEAT	
		192.108.255.226	192.168.8.136	SCTP 130 HEARTBEAT	— п ×
final_test_2a_control_noipsec_te	estlaptop_050322.pcapng			SCTP 130 HEARTBEAT	- 🗆 X
final_test_2a_control_noipsec_te File Edit View Go Capture	estlaptop_050322.pcapng Analyze Statistics	Telephony Wireless Too	ols Help	SCTP 130 HEARTBEAT	×
 ✓ final_test_2a_control_noipsec_te File Edit View Go Capture ✓ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	estlaptop_050322.pcapng	Telephony Wireless Too		SCTP 130 HEARTBEAT	
final_test_2a_control_noipsec_te File Edit View Go Capture	estlaptop_050322.pcapng Analyze Statistics	Telephony Wireless Too	ols Help	SCTP 130 HEARTBEAT	×
final_test_2a_control_noipsec_te File Edit View Go Capture File Edit View Go Capture File Edit View Go Capture Scipilsiap No. Time	estlaptop_050322.pcapng Analyze Statistics	Telephony Wireless Too	ols Help C C C T	Lengti Info	
<pre> final_test_2a_control_noipsec_te File Edit View Go Capture @</pre>	estlaptop_050322.pcapng Analyze Statistics Analyze Statistics Source 469040477 192.168.	Telephony Wireless Too Telephony Wireless Too Telephony Construction Destination 255.226 192.168	Protocol 1 .8.136 SCTP	Lengt [†] Info 130 HEARTBEAT	
final_test_2a_control_noipsec_te File Edit View Go Capture File Edit View Go Capture File Edit View Go Capture Scipilsiap No. Time	estlaptop_050322.pcapng Analyze Statistics Source 469040477 192.168. 469059370 192.168.	Telephony Wireless Too	Dis Help Protocol .8.136 SCTP .8.136 SCTP	Lengti Info	
✓ final_test_2a_control_noipsec_tw File Edit View Go Capture ✓ ● ● ● ● ● ● ● ●<	estlaptop_050322.pcapng Analyze Statistics Analyze Statistics Source 469040477 192.168. 4690659370 192.168. 469067227 192.168.	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168	Dis Help Q Q III .8.136 SCTP .8.136 SCTP .8.136 SCTP .8.136 SCTP .8.136 SCTP	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT 130 HEARTBEAT_ACK	
✓ final_test_2a_control_noipsec_te File Edit View Go Capture ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	Analyze Statistics Analyze Statistics Source 469040477 192.168. 469063370 192.168. 469063370 192.168. 46906227 192.168. 469070809 192.168.	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168	A A A A A A A A A A A A A A A A A A A	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK	
✓ final_test_2a_control_noipsec_tw File Edit View Go Capture ✓ ● ● <td>estlaptop_050322.pcapng Analyze Statistics</td> <td>Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168</td> <td>A C C C C C C C C C C C C C C C C C C C</td> <td>Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT 130 HEARTBEAT_ACK</td> <td></td>	estlaptop_050322.pcapng Analyze Statistics	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168	A C C C C C C C C C C C C C C C C C C C	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT 130 HEARTBEAT_ACK	
✓ final_test_2a_control_noipsec_tw File Edit View Go Capture ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ <t< td=""><td>Analyze Statistics Analyze Statistics Analyze Statistics Source 469040477 192.168. 4690659370 192.168. 469067227 192.168. 469067227 192.168. 469074737 192.168. 469074737 192.168. 46908211 192.168.</td><td>Telephony Wireless Too Telephony Wireless Too Telephony Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168</td><td>Dis Help Protocol III .8.136 SCTP .8.136 SCTP</td><td>Lengt Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK</td><td></td></t<>	Analyze Statistics Analyze Statistics Analyze Statistics Source 469040477 192.168. 4690659370 192.168. 469067227 192.168. 469067227 192.168. 469074737 192.168. 469074737 192.168. 46908211 192.168.	Telephony Wireless Too Telephony Wireless Too Telephony Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168	Dis Help Protocol III .8.136 SCTP	Lengt Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK	
<pre> final_test_2a_control_noipsec_tu File Edit View Go Capture im @ @ @ @ @ @ @ @ @ im @ @ ime 2 0222-05-03 16:18:00. 3 2022-05-03 16:18:00. 4 2022-05-03 16:18:00. 5 2022-05-03 16:18:00. 7 2022-05-03 16:18:00. 7 2022-05-03 16:18:00. 7 2022-05-03 16:18:00. 8 2022-05-03 16:18:00. 9 2022-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:18:00. 10 202-05-03 16:1</pre>	Statistics Analyze Statistics Image: Statistics Image: Statistics Image: Statistics <th< td=""><td>Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168</td><td>A C C C C C C C C C C C C C C C C C C C</td><td>Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_</td><td></td></th<>	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168	A C C C C C C C C C C C C C C C C C C C	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_	
✓ final_test_2a_control_noipsec_tw File Edit View Go Capture ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	Analyze Statistics ▲nalyze Statistics ▲69040477 192.168. ▲6906370 192.168. ▲69078714 192.168. ▲69082237 192.168. ▲6908052 192.168.	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168	A C A C A C A C A C A C A C A C A C A C	Lengt Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK	
final_test_2a_control_noipse_tu File Edit View Go Capture Image: State Image: State Image: State Image: State Image: State No. Time 2 2022-05-03 16:18:00. 3 2022-05-03 16:18:00. 4 2022-05-03 16:18:00. 5 2022-05-03 16:18:00. 6 2022-05-03 16:18:00. 7 2022-05-03 16:18:00. 7 2022-05-03 16:18:00. 8 2022-05-03 16:18:00. 8 2022-05-03 16:18:00. 10 2022-05-03 16:18:00. 10 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 16:18:00. 11 2022-05-03 <t< td=""><td>Source Analyze Statistics Image: Statistics Image: Statistics Image: Statistics Ima</td><td>Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168</td><td>A C C C C C C C C C C C C C C C C C C C</td><td>Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK</td><td></td></t<>	Source Analyze Statistics Image: Statistics Image: Statistics Image: Statistics Ima	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168 255.226 192.168	A C C C C C C C C C C C C C C C C C C C	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK 130 HEARTBEAT_ACK	
 ▲ final_test_2a_control_noipsec_tu File Edit View Go Capture ▲ W Go Capture ▲ W Go Capture ▲ Stop[stap No. Time 2 2022-05-03 16:18:00. 3 2022-05-03 16:18:00. 4 2022-05-03 16:18:00. 5 2022-05-03 16:18:00. 6 2022-05-03 16:18:00. 7 2022-05-03 16:18:00. 8 2022-05-03 16:18:00. 9 2022-05-03 16:18:00. 1 2022-05-03 16:18:00. 1 2022-05-03 16:18:00. 	stataptop_050322.pcapung Analyze Statistics Image: Statistics Image: Statistics Image: Statistics	Telephony Wireless Too Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255.256 192.1	A C A A A A A A A A A A A A A A A A A A	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130	
 final_test_2a_control_noipsec_tu File Edit View Go Capture im 20 (a) (a) (a) (a) (a) (a) (a) (a) (a) (a)	Analyze Statistics Analyze Statistics Image: Analyze Statistics Image: Analyze Statistics Image: Analyze Statistics Image: Analyze Source 46904477 192.168. 469065370 192.168. 469067227 192.168. 469078714 192.168. 46908621 192.168. 4690862237 192.168. 469086241 192.168. 46908625 192.168. 469086442 192.168. 469086442 192.168. 469087714 192.168. 469086422 192.168. 46908642 192.168. 469087714 192.168. 46908714 192.168. 46908714 192.168. 46908714 192.168. 46908714 192.168. 46908714 192.168. 46908714 192.168. 499143:a0:21 (66:0e: 192.168. 100 192.168. 100 192.168. 100	Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255	A C A A A A A A A A A A A A A A A A A A	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130	+
<pre>final_test_2a_control_noipsec_tu File Edit View Go Capture Site Capture Site Capture Site Capture Site Capture File Edit View Go Capture Site Capture Site</pre>	Analyze Statistics Analyze Statistics Image: Statistics Image: Statistics Image: S	Telephony Wireless Too Destination 255.226 192.168 255.226 192.168 255	e9 a8 bit Protocol 1.8.136 SCTP .8.136 SCT	Lengti Info 130 HEARTBEAT 130 HEARTBEAT_ACK 130	+

Figure 13: RAN-side Capture of Control Packets, Modified Control Packets and Injected Control Packets on Untrusted Link

Figure 14 and Figure 15 show the captures on the untrusted link (TP4 and TP5), as well as the egress of the core-side router (also TP5). Note that these captures show the presence of control traffic at roughly the same number as were captured on the RAN side. Modified control packets (SCTP and S1AP) are seen on the egress interface of R6K at both core and RAN sides. In addition, ABORT packets from the MME to the RAN are seen. These ABORT packets likely indicate that some of the injected packets did not pass an integrity or duplication check in the MME.

TLP:WHITE:5GSTB

final_test_2a_control_noipsec_pluribus_050322.pcapng	– 🗆 X
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
⊿ ■ ⊿ ⊛ 📕 🖹 🕱 🔇 ۹ 🗰 🔿 🛎 ∓ 🖢 🜉 🔲 ۹ ۹ ۹ ୩ 🎛	
sctp stap	X 🗆 🔹 +
No. Time Source Destination Protocol Lengt Info	^
153 2022-05-03 16:16:57.606503 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT 154 2022-05-03 16:16:57.606503 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT ACK	
154 2022-05-03 16:16:57.606503 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT_ACK 155 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT	
156 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT_ACK	
157 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT 158 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT	
159 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT	
160 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT_ACK 161 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT_ACK	
162 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT_ACK	
163 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT 164 2022-05-03 16:16:57.606888 192.168.255.226 192.168.8.136 SCTP 176 HEARTBEAT_ACK	
165 2022-05-03 16:16:57.607267 192.168.8.136 192.168.255.226 SCTP 110 ABORT	
166 2022-05-03 16:16:57.607267 192.168.8.136 192.168.255.226 SCTP 110 ABORT 167 2022-05-03 16:16:57.607267 192.168.8.136 192.168.255.226 SCTP 110 ABORT	
168 2022-05-03 16:16:57.607267 192.168.8.136 192.168.255.226 SCTP 110 ABORT	
1 contract of the second secon	- 🗆 X
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
I III E LOIR VIEW GO CAPTURE Analyze Statistics Interpriority Wireless Iools Field I III II III III III IIII IIII IIIIIIII	
No. Time Source Destination Protocol Lengt Info	
90 2022-05-03 16:17:03.671091 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
91 2022-05-03 16:17:03.671092 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT_ACK	
92 2022-05-03 16:17:03.671093 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT 93 2022-05-03 16:17:03.671094 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
94 2022-05-03 16:17:03.671095 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
000 95 2022-05-03 16:17:03.671096 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT_ACK 000 96 2022-05-03 16:17:03.671097 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
97 2022-05-03 16:17:03.671100 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
98 2022-05-03 16:17:03.671102 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT_ACK 99 2022-05-03 16:17:03.671103 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
100 2022-05-03 16:17:03.671104 192.168.25 192.168.8.1 SCTP 130 HEARTBEAT	
101 2022-05-03 16:17:03.671332 192.168.8 192.168.255 SCTP 64 ABORT 102 2022-05-03 1 <u>6:17:03.671437 192 168 8 192 168 255 SCTP 64 ABORT</u>	
103 2022-05-03 1 📶 test2A-MITRE-rők-clear-050322-1617.pcap	- 🗆 ×
104 2022-05-03 1 105 2022-05-03 1 File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
106 2022-05-03 1 📶 🗐 🧭 📕 🖺 🏹 🚱 🔍 🐳 🛸 🐨 🐔 💆 🥃 🔍 🔍 🔍 🏹	
107 2022-05-03 1 108 2022-05-03 1 sctp[slap	
No. Time Source Destination Protocol Lengt Info	^
Source port: 95 2022-05-03 16:17:03.668600 192.168.25 192.168.8.1 SCTP 130 HEARTBE Destination 96 2022-05-03 16:17:03.668600 192.168.25 192.168.8.1 SCTP 130 HEARTBE	
Destination 96 2022-05-03 16:17:03.6686600 192.168.25 192.168.8.1 SCTP 130 HEARTBE Verification 97 2022-05-03 16:17:03.6686601 192.168.25 192.168.8.1 SCTP 130 HEARTBE	
Association 98 2022-05-03 16:17:03.668601 192.168.25 192.168.8.1 SCTP 130 HEARTBE	
Checksum: 0 99 2022-05-03 16:17:03.668617 192.168.25 192.168.8.1 SCTP 130 HEARTBE 100 2022-05-03 16:17:03.668618 192.168.25 192.168.8.1 SCTP 130 HEARTBE	
0000 98 7a 10 101 2022-05-03 16:17:03.668618 192.168.25 192.168.8.1 SCTP 130 HEARTBE	
SI Application 102 2022-05-03 16:17:03.668619 192.168.25 192.168.8.1 SCTP 130 HEARTBE 103 2022-05-03 16:17:03.668848 192.168.8 192.168.255 SCTP 64 ABORT	EAT
104 2022-05-03 16:17:03.668964 192.168.8 192.168.255 SCTP 64 ABORT	
105 2022-05-03 16:17:03.669163 192.168.8 192.168.255 SCTP 64 ABORT 106 2022-05-03 16:17:03.669178 192.168.8 192.168.255 SCTP 64 ABORT	
107 2022-05-03 16:17:03.669237 192.168.8 192.168.255 SCTP 64 ABORT	
108 2022-05-03 16:17:03.669274 192.168.8 192.168.255 SCTP 64 ABORT 109 2022-05-03 16:17:03.669325 192.168.8 192.168.255 SCTP 64 ABORT	
105 2022 03-005 102-1005 132-1005 132-1005 101-1005 <	>
> Frame 103: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)	^
Ethernet II, Src: fa:16:3e:7a:b7:81 (fa:16:3e:7a:b7:81), Dst: Ericsson_85:91:c9 (> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3704	98:7a:10:85:91:c9)
Internet Protocol Version 4, Src: 192.168.8.136, Dst: 192.168.255.226	
 Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36422 (3 Source port: 36412 	36422)
Destination cost: 26400	~
0000 98 7a 10 85 91 c9 fa 16 3e 7a b7 81 81 00 0e 78 0010 08 00 45 a0 00 24 b8 f8 00 00 fe 84 79 01 c0 a8	^
0020 08 88 c0 a8 ff e2 8e 3c 8e 46 02 9b b9 27 f8 f6	×
O Z S1 Application Protocol: Protocol Packets:	218 · Displayed: 213 (97.7%) Profile: STB Profile
Figure 14: Captured Backets on Care facing Part of PAN side Switch: Care side Untrust	ad Link and Cara aida Trustad Da

Figure 14: Captured Packets on Core-facing Port of RAN-side Switch; Core-side Untrusted Link; and Core-side Trusted Router without IPsec Encryption on Untrusted Link

📕 fina	al_test_2	a_con	trol_n	oipseo	c_R6	K_050	0322.	.pca	png																		_			×
File E	dit Vie	ew G	o Ca	pture	e A	nalyz	ze S	Statis	stics	Tele	phor	ny	Wire	eless	Тоо	ls ⊢	lelp													
	1 0		1	8 🙆	Q	4		Ú.	<u> </u>				Ð		a T	Ē														
sctp								_	• •	× [=	-	-	•	•	•	-													× →	• +
No.	Time								C -1	irce				De	stinatio			Due	tocol		Lengt	Tafa								
,		05 0	10 10	.17.		0101	22				58.8	17	7				5.22							т						
L	2 2022																					HEAR			212					
	3 2022														2.16			SC				HEAR		I_AC	.К					
	5 2022										8.8						5.22					ABOR								
	7 2022										6.8						5.22					ABOR								
	8 2022										6.8						5.22					ABOR								
	9 2022										8.8						5.22					ABOR								
	0 2022										8.8						5.22					ABOR								
	1 2022										8.8						5.22					ABOR								
	2 2022										68.8						5.22					ABOR								
	3 2022	-05-0	3 16	:17:	06.	6459	931		19	2.10	6.8	.13	6	19	2.16	8.25	5.22	5 SC	ΓP		66	ABOR	Г							
<																													>	
> Eth > Int	me 2: ernet ernet eam Co	II, Prot	Src: ocol	Erio Ver:	csso sior	on_8 n 4,	b:a0 Sro	0:4a c: 1	a (98 192.1	8:7a	:10 8.1	:8b 37,	:a0: Dst	4a) :: 1	, Ds 92.1	t: E 68.2	rics 55.2	son_e 26	b:3e	:0e	(1c	90:be		_	•	93562-	-16F(C-478	31-8A	F1-B
<																														
_										-		_						_												
0000	1c 90																													
0010	00 70																b													
0020	ff e2								65 6			-					p`e													
0030 0040	00 50								48 9						· P · ·	- L	H	· p · · ·												
0040	00 00																													
0050	S1 App						00	00	00 0		0.00	,	, ao	,						Pac	:kets: 1	42 • Dis	olayed	: 113	(79.6%	6)		Profile	: STB F	Profile
_					_			_				-	_	_	_	_	_						_	-				_	_	-

Figure 15: RAN-side Router Capture of Injected Packets

Figure 16 and Figure 17 show the relevant packet captures when the captured packets are modified and injected into the untrusted link when IPsec encrypts traffic in the tunnel. Figure 16 shows the modified packets, the packets injected into the switch (TP3), and the capture from the outgoing port on the switch (TP4). Note that because all of these occur inside the IPsec tunnel, traffic is indistinguishable as it all appears as encrypted packets. There is no indication of what traffic is control plane traffic.

	d_esp_control050	322.pcap										_	
e E	dit View Go		e Statistics	Telepho	ny Wireles								
			र 🦛 🏓 🛛	2	<u>*</u>	Ð	୍ବ୍	1					
Appl	y a display filter <	Ctrl-/>											
	Time		Source		Destination		Protocol	Lengti I		_			
		5:21:11.189352	192.168.2		192.168.		ESP			I=0xcfa:			_
		5:21:11.189354	192.168.2		192.168.		ESP			I=0xcaa	•		
		5:21:16.670580 5:21:16.672462	192.168.2		192.168.		ESP ESP			I=0xcfa I=0xcaa			
		5:21:24.011725	192.168.2		192.168.		ESP			I=0xcaa			
		5:21:24.031450	192.168.2		192.168.		ESP			I=0xcfa			
7	2022-05-03 1	5:21:24.052486	192.168.2	55.254	192.168.	8.254	ESP	138 8	SP (SP	I=0xcaa	:e31f)		
8	2022-05-03 1	5:21:24.202405	192.168.2	55.254	192.168.	8.254	ESP	202 8	SP (SP	I=0xcaa	:e31f)		
		5:21:24.219142	192.168.2		192.168.		ESP			I=0xcfa	-		
		5:21:24.240428	192.168.2		192.168.		ESP			I=0xcaa			
		5:21:24.242339	192.168.2		192.168.		ESP			I=0xcaa			
		5:21:24.259018 5:21:24.280334	192.168.2		192.168.		ESP ESP			I=0xcfa I=0xcaa			
		5:21:24.282363	192.168.2		192.168.		ESP		-	I=0xcaa	-		
		5:21:24.325075	192.168.2		192.168.		ESP			I=0xcfa			
													>
_	Type: 802.10	Virtual LAN (0	x8100)										
030 040 050	ec 04 37	6a 1c 7d 9e 00 de ab 90 d9 ff 3e c5	7e h8	5f 1f	71 08 3 91 4c 3	5 29 5							
7	8					1 31 7	'b	Dackets: 738	• Displaye	H: 738 (100	0%)	Profile:	STR Pro
	IP Encapsulating	g Security Payload Secu ontrol_ipsec_testlapto	urity Parameters I	index (esp.s		1 31 7	'b	Packets: 738	• Displaye	d: 738 (100.	0%)	Profile:	STB Pro
	IP Encapsulating	g Security Payload Secu	urity Parameters I op_050322.pca	index (esp.s png	spi), 4 bytes		'b Tools He		• Displaye	d: 738 (100.	0%)	Profile:	
	IP Encapsulating	g Security Payload Secu ontrol_ipsec_testlapto	urity Parameters I op_050322.pca malyze Stati	index (esp.s png	spi), 4 bytes		Tools He		• Displaye	d: 738 (100.	0%)	Profile:	
Fi	IP Encapsulating final_test_2b_cc le Edit View	<u>security Payload Secu</u> ontrol_ipsec_testlapto Go Capture A	urity Parameters I op_050322.pca malyze Stati	index (esp.s png	spi), 4 bytes		Tools He	elp	• Displaye	d: 738 (100,	0%)	Profile:	
Fi	IP Encapsulating final_test_2b_cc le Edit View	<u>security Payload Secu</u> ontrol_ipsec_testlapto Go Capture A	urity Parameters I op_050322.pca unalyze Stati:	index (esp.s png	spi), 4 bytes ephony W		Tools He	elp		d: 738 (100,	0%)	Profile:	
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp . Time	<u>security Payload Secu</u> ontrol_ipsec_testlapto Go Capture A	urity Parameters I op_050322.pca analyze Stati:	index (esp.s png stics Tel	spi), 4 bytes ephony W	/ireless	Tools He	elp Q III	Ler	ngti Info	0%)		
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp . Time 12 2022-05 13 2022-05	 Security Payload Security Payload Security Interview (Security Payload Security Payload Security (Security Payload Security Payload Security Payload Security Payload Security (Security Payload Security Payload Secu	urity Parameters I op_050322.pca unalyze Statis 0 • • • • • • • • • • • • • • • • • • •	index (esp.s png stics Tel	spi), 4 bytes lephony W 55.254 55.254	/ireless	Tools He	Protocol ESP ESP	Ler 2 1	ngti Info 02 ESP 86 ESP	(SPI=0xc (SPI=0xc		□ () () () () () () () () () ()
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp . Time 12 2022-05- 13 2022-05- 14 2022-05-	Security Payload Security Introl_ipsec_testlapto Go Capture A Image: Capture interval Image: Capture interval Image: Capture interval 03 16:29:40.773 03 16:29:40.773 03 16:29:40.773 03 16:29:40.773	urity Parameters I op_050322.pca inalyze Statii Q @ = 1 50 094861 19 099230 19 105231 19	Index (esp.s png stics Tel	spi), 4 bytes lephony W	/ireless Destination 192.168. 192.168. 192.168.	Tools He 8.254 8.254 8.254 8.254	Protocol ESP ESP ESP	Ler 2 1 1	ngti Info 02 ESP 86 ESP 38 ESP	(SPI=0xc (SPI=0xc (SPI=0xc		f) f)
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp Imme Imme Imme 12 2022-05 13 2022-05 14 2022-05 15 2022-05	Security Payload Security ontrol_ipsec_testlaptic Go Capture A A B A A A B A B A B A B B B B B B B C B C B C B C B C B C B C B C B C B C C C C C C C C C C C C C C C C C C C C C C C C C C C C	unty Parameters 1 op_050322.pca analyze Stati:	Index (esp.s png stics Tel) 2.168.2) 2.168.2) 2.168.2) 2.168.2	ephony W	/ireless	Tools He 1 8.254 8.254 8.254 8.254 8.254 8.254	elp Q II Protocol ESP ESP ESP ESP ESP	Ler 2 1 1 2	ngti Info 02 ESP 86 ESP 38 ESP 02 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc		f) 2) f)
Fil	IP Encapsulating final_test_2b_cc le Edit View esp . Time 12 2022-05 13 2022-05 14 2022-05 15 2022-05 16 2022-05	Security Payload Security for the securety for the security for the securety for the securety for the	urity Parameters 1 op_050322.pca unalyze Statis Q	index (esp.s png stics Tel)))))))))))))))))))	spi), 4 bytes lephony W	Vireless Destination 192.168 192.168 192.168 192.168	Tools He a a 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Q III Protocol ESP ESP ESP ESP ESP ESP	Lee 2 1 1 2 1	ngti Info 02 ESP 86 ESP 38 ESP 02 ESP 38 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc		F) F)<
Fil	IP Encapsulating final_test_2b_coc le Edit View le 2022-05- 13 12 2022-05- 15 15 2022-05- 16 17 2022-05- 17	Security Payload Security Introl_ipsec_testlaptor Go Capture A Image: Image and the	urity Parameters 1 op_050322.pca analyze Statis Q (* * * 094861 19 099230 19 105231 19 110852 19 115644 19 125041 19	Index (esp.s png stics Tel) 2.168.2) 2.168.2) 2.168.2) 2.168.2	spi), 4 bytes lephony W 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254	/ireless	Tools H	elp Q Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Lee 2 1 1 2 1 4	ngti Info 02 ESP 86 ESP 38 ESP 02 ESP 38 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc		f) f) f) f) f) 2) 2) 2)
Fil	IP Encapsulating final_test_2b_ccc le Edit View le 2022-05- 14 12 2022-05- 15 16 2022-05- 16 17 2022-05- 18 18 2022-05-	Security Payload Security for the securety for the security for the securety for the securety for the	urity Parameters 1 op_050322.pca analyze Statis Q (* * 094861 19 099230 19 105231 19 110852 19 115644 19 125045 19	Index (esp.s png stics Tel)) 2.168.2) 2.168.2) 2.168.2) 2.168.2) 2.168.2) 2.168.2) 2.168.2) 2.168.2	spi), 4 bytes lephony W 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254	Vireless Destination 192.168 192.168 192.168 192.168	Tools He 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Q III Protocol ESP ESP ESP ESP ESP ESP	Lee 2 1 1 2 1 1 4 4	ngti Info 02 ESP 86 ESP 38 ESP 02 ESP 38 ESP 26 ESP 38 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc		f) f) f) f) f) f) f) f)
Fil	IP Encapsulating final_test_2b_ccc le Edit View Image: Comparison of the system esp Image: Comparison of the system 12 2022-05-13 13 2022-05-14 14 2022-05-16 15 2022-05-16 16 2022-05-16 17 2022-05-18 18 2022-05-18 19 2022-05-19	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Image and the i	rity Parameters I op_050322.pca analyze Statis Q Q (m) 094861 19 099230 19 105231 19 118642 19 115644 19 121081 19 122082 19	Index (esp.s png stics Tel vurce 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	ppi), 4 bytes lephony W 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254	Vireless Vir	Tools He 8 .254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Lee 2 1 1 2 4 4 1 6	ngti Info 02 ESP 86 ESP 38 ESP 02 ESP 26 ESP 38 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31	F) F)<
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp Image: Comparison of the system of	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Image and the i	nty Parameters 1 op_050322.pca analyze Statis Q	Index (esp.s png stics Tel stics Tel 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	ephony W 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254 55.254	Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168	Tools H 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Lee 2 1 1 2 4 4 1 6 6 6	ngti Info 02 ESP 86 ESP 38 ESP 02 ESP 38 ESP 26 ESP 66 ESP 66 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31	F)
Fi	IP Encapsulating final_test_2b_cc le Edit View esp Ime Ime 12 2022-05- 13 2022-05- 14 2022-05- 15 2022-05- 16 2022-05- 16 2022-05- 18 2022-05- 19 2022-05- 19 2022-05- 12 2022-05- 20 2022-05- 12 2022-05-	Security Payload Security ontrol_ipsec_testlaptic Go Capture A I Image: Capture A Image: Capture Image: C	rrity Parameters 1 op_050322.pca analyze Statis Q ← 094861 19 099230 19 105231 19 110652 19 115644 19 125085 19 125085 19 146672 19 15566 19	Index (esp.s png stics Tel stics Tel 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	ppi), 4 bytes lephony W Provide the second	Vireless Vir	Tools He 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Lee 2 1 1 1 2 1 1 4 4 1 6 6 6 6	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) f) f) f) f) f) f) f) f) f) f
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp Image:	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Comparison of the system Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03	rrity Parameters 1 op_050322.pca analyze Statis Q ← 094861 19 099230 19 105231 19 110652 19 115644 19 125085 19 125085 19 146672 19 15566 19	Index (esp.s png stics Tel stics Tel 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	spi), 4 bytes lephony W a	Vireless Vir	Tools He 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
Fi	IP Encapsulating final_test_2b_ccc le Edit View esp Image:	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Comparison of the system Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03	rrity Parameters 1 op_050322.pca analyze Statis Q ← 094861 19 099230 19 105231 19 110652 19 115644 19 125085 19 125085 19 146672 19 15566 19	Index (esp.s png stics Tel stics Tel 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	ppi), 4 bytes lephony W Provide the second	Vireless Vir	Tools He 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp Image: Comparison of the system of	Security Payload Security Go Capture A Image: Control in the security of the securety of the	nty Parameters 1 op_050322.pca analyze Stati Q ← ← 094861 19 099230 19 105231 19 110852 19 110852 19 126325 19 126325 19 135389 19 146646 19 151566 19 151566 19 157502 19 21 (66:0e:9	Index (esp.s png stics Tel e 2168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	spi), 4 bytes lephony W 55.254 55.	Vireless Vir	Tools He 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) f) f) f) f) f) f) f) f) f) f
Fil	IP Encapsulating final_test_2b_ccc le Edit View esp Image: Comparison of the system of	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Construction of the security of the securety of the security of the security of the security of the secur	rity Parameters 1 op_050322.pca inalyze Stati Q ← 1 0994861 19 099230 19 105231 19 115644 19 126325 19 126325 19 140646 19 146172 19 151566 19 157502 19 21 (66:0e:5 N (0x8100)	Index (esp.s png stics Tel index (esp.s produce 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2 22.168.2	spi), 4 bytes lephony W 55.254 55.	Vireless Vir	Tools He 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
Fil	IP Encapsulating final_test_2b_cc le Edit View esp Image:	Security Payload Security for the securety for the security for the securety for the securety for the	rity Parameters 1 op_050322.pca analyze Statis Q ← 1 094861 19 099230 19 105231 19 115644 19 126325 19 115644 19 126325 19 135389 19 146172 19 151566 19 157502 19 21 (66:0e:5 N (0x8100) , DEI: 0, JI	Index (esp.s png stics Tel e 22.168.2 2	spi), 4 bytes lephony W lephony	Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168	Tools H	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
Fil	IP Encapsulating final_test_2b_cc le Edit View Image: Edit <td>Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Comparison of the system Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03</td> <td>rity Parameters 1 op_050322.pca analyze Statis Q ← 1 Sc 094861 19 099230 19 105231 19 110852 19 110852 19 112684 19 126325 19 135389 19 135389 19 146646 19 146172 19 151566 19 157502 19 21 (66:00:5 N (0×8100) , DEI: 0, TI 4, Src: 192</td> <td>Index (esp.s png stics Tel e 22.168.2 2</td> <td>spi), 4 bytes lephony W lephony W lephony</td> <td>Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168</td> <td>Tools H</td> <td>elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP</td> <td>Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4</td> <td>ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP</td> <td>(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)</td> <td>aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31</td> <td>F) 2) F) F)<</td>	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Comparison of the system Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03	rity Parameters 1 op_050322.pca analyze Statis Q ← 1 Sc 094861 19 099230 19 105231 19 110852 19 110852 19 112684 19 126325 19 135389 19 135389 19 146646 19 146172 19 151566 19 157502 19 21 (66:00:5 N (0×8100) , DEI: 0, TI 4, Src: 192	Index (esp.s png stics Tel e 22.168.2 2	spi), 4 bytes lephony W lephony	Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168	Tools H	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
Fil	IP Encapsulating final_test_2b_ccc final_test_2b_ccc le Edit View Image: Im	Security Payload Security Introl_ipsec_testlaptor Go Capture A Image: Construction of the system Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 03 16:29:40.773 Image: Construction of the system Image: Construction of the system 04 100 100 100 100 100 100 <	rity Parameters 1 op_050322.pca analyze Statis Q ← 1 094861 15 099280 15 105231 15 105231 15 115644 15 121081 15 126325 15 126325 15 146172 15 151566 15 151566 15 151566 15 166:0e:5 N (0x8100) , DEI: 0, II 4, Src: 192 Load	Index (esp.s png stics Tel e 22.168.2 2	spi), 4 bytes lephony W lephony	Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168	Tools H	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
Fil	IP Encapsulating final_test_2b_ccc le Edit View imal_test_2b_ccc imal_test_2b_ccc le Edit View imal_test_2b_ccc imal_test_2b_ccc le Edit View imal_test_2b_ccc imal_test_2b_ccc ls 2022-05- 15 ls 2022-05- 19 ls 2022-05- 20 ls Source: Type: 80 802.1Q Virtt Internet Pro Internet Pro Encapsulatif ESP SPI:	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Comparison of the system Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03 16:29:40.773 Image: Comparison of the system Image: Comparison of the system 03	rity Parameters 1 op_050322.pca analyze Statis Q ← 1 094861 15 099280 15 105231 15 105231 15 115644 15 121081 15 126325 15 126325 15 146172 15 151566 15 151566 15 151566 15 166:0e:5 N (0x8100) , DEI: 0, II 4, Src: 192 Load	Index (esp.s png stics Tel e 22.168.2 2	spi), 4 bytes lephony W lephony	Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168	Tools H	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
 Fill No <	IP Encapsulating final_test_2b_ccc le Edit View Image: Edit </td <td>Security Payload Security Payload</td> <td>rity Parameters] op_050322.pca inalyze Statis Q ← 1 094861 19 099230 19 105231 19 105231 19 115644 19 12081 19 126325 19 140646 19 146172 19 157502 19 21 (66:0e:9 N (0x8100) , DEI: 0, II 4, Src: 192 Load 00327967) A 66 Øe</td> <td>Index (esp.s png stics Tel → 20168.2 22.168.2 23.168.2 24.168.2 25.1</td> <td>ephony W S5.254 S5</td> <td>Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168</td> <td>Tools H 8.254</td> <td>elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP</td> <td>Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4</td> <td>ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP</td> <td>(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)</td> <td>aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31</td> <td>F) 2) F) F)<</td>	Security Payload	rity Parameters] op_050322.pca inalyze Statis Q ← 1 094861 19 099230 19 105231 19 105231 19 115644 19 12081 19 126325 19 140646 19 146172 19 157502 19 21 (66:0e:9 N (0x8100) , DEI: 0, II 4, Src: 192 Load 00327967) A 66 Øe	Index (esp.s png stics Tel → 20168.2 22.168.2 23.168.2 24.168.2 25.1	ephony W S5.254 S5	Vireless Destination 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168 192.168	Tools H 8.254	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<
< <tr> Fill No > > > > 00</tr>	IP Encapsulating final_test_2b_cc le Edit View Image: Edit <td>Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Construction of the security of the secure secure secure security of the security of the security of the</td> <td>rity Parameters 1 op_050322.pca analyze Statis Q ← 1 Sc 094861 19 099230 19 105231 19 105231 19 110852 19 110852 19 1135389 19 126325 19 135389 19 146476 19 15566 19 15676 19 15776 19 157</td> <td>Index (esp.s png stics Tel → 100 22.168.2</td> <td>ppi), 4 bytes lephony W 55.254 55</td> <td>Vireless Destination 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168.</td> <td>Tools H 8.254 8.25</td> <td>elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP</td> <td>Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4</td> <td>ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP</td> <td>(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)</td> <td>aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31</td> <td>F) 2) F) F)<</td>	Security Payload Security Introl_ipsec_testlapt Go Capture A Image: Construction of the security of the secure secure secure security of the security of the security of the	rity Parameters 1 op_050322.pca analyze Statis Q ← 1 Sc 094861 19 099230 19 105231 19 105231 19 110852 19 110852 19 1135389 19 126325 19 135389 19 146476 19 15566 19 15676 19 15776 19 157	Index (esp.s png stics Tel → 100 22.168.2	ppi), 4 bytes lephony W 55.254 55	Vireless Destination 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168. 192.168.	Tools H 8.254 8.25	elp Protocol ESP ESP ESP ESP ESP ESP ESP ESP	Len 2 1 1 1 2 1 1 4 1 6 6 6 6 6 6 4	ngti Info 02 ESP 86 ESP 38 ESP 38 ESP 26 ESP 38 ESP 66 ESP 66 ESP 26 ESP 26 ESP	(SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc (SPI=0xc)	aace31 fa30a5 aace31 fa30a5 fa30a5 fa30a5 fa30a5 aace31 aace31 aace31 aace31	F) 2) F) F)<

Figure 16: RAN-side Capture of Encrypted Packets, Modified Packets, and Injected Packets on Untrusted Link

Figure 17 shows the packet captures at the core-side router (TP5) as well as on the trusted RANside router (TP2). Again, on the untrusted link, we cannot distinguish between the traffic that exists due to control plane messages between the RAN and LTE core and the injected encrypted packets. The decrypted traffic, both at the RAN and at the LTE core show agreement with respect to the control plane traffic. A count of the encrypted packets in the IPsec tunnel, when compared to the unencrypted traffic outside the tunnel indicates the injected packets have been dropped at the tunnel endpoints. Specifically, approximately 20,000 ESP packets (containing control pane traffic) were injected into the transport network, and approximately 14,000 packets were received on the ingress R6K interface at the LTE core. However, only 38 packets were received on the egress R6K interface at the core. Furthermore, of those 38 packets, only 6 were control packets (as can be seen in Figure 17). Similarly, on the RAN side (TP2), Figure 18 shows that the number of captured control packets when ESP traffic was being injected was 5.

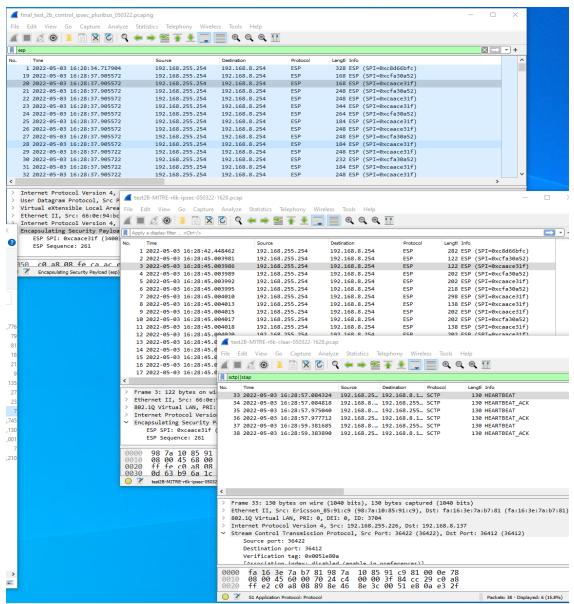


Figure 17: RAN-Side Outgoing Link to Core; Core-Side Untrusted Link Capture of Encrypted Traffic; and Core-Side Capture at Trusted Router after Decryption

TLP:WHITE:5GSTB

final_test_2b_control_ipsec_R6K_050322.pca	apng			_		×
File Edit View Go Capture Analyze S	tatistics Telephony Wi	reless Tools Help				
/ I () () I () () () () () () () () () () () () ()	🛎 주 速 📃 🔲 🔍	0,0,11				
sctp s1ap					\times	+ -
No. Time	Source	Destination	Protocol	Lengt Info		
107 2022-05-03 16:29:00.057876	192.168.255.226	192.168.8.137	SCTP	126 HEARTBEAT		
108 2022-05-03 16:29:00.060421	192.168.8.137	192.168.255.226	SCTP	126 HEARTBEAT_ACK		
111 2022-05-03 16:29:00.951648	192.168.8.136	192.168.255.226	SCTP	126 HEARTBEAT		
112 2022-05-03 16:29:00.951755	192.168.255.226	192.168.8.136	SCTP	126 HEARTBEAT_ACK		
116 2022-05-03 16:29:02.358414	192.168.8.137	192.168.255.226	SCTP	126 HEARTBEAT		
<						>
> Ethernet II, Src: Fricsson_eb:ae > Internet Protocol Version 4, Src Stream Control Transmission Prot Source port: 36422 Destination port: 36412 Verification tag: 0x0051e80a [Association index: disabled Checksum: 0xe32f90fa [unverif [Checksum Status: Unverified] > HEARTBEAT chunk (Information: > Chunk type: HEARTBEAT (4) Chunk flags: 0x00 Chunk lagth: 80 > Heartbeat info parameter (1)	: 192.168.255.226, ocol, Src Port: 36 (enable in preferer ied] 76 bytes) [nformation: 72 byt	Dst: 192.168.8.137 122 (36422), Dst Port: ces)]				
0000 98 7a 10 8b a0 4a 1c 90 be 0010 00 70 24 c4 00 00 40 84 cb						
0020 08 89 8e 46 8e 3c 00 51 e8						
0030 00 50 00 01 00 4c 0a 8a f8						
0040 00 00 00 00 00 00 c0 a8 08						
0050 00 00 00 00 00 00 00 00 00	00 00 00 00 00 c0 a	8				~
S1 Application Protocol: Protocol				Packets: 116 · Displayed: 5 (4.3%)	Profile: STB F	rofile

Figure 18: RAN-Side Router Interface Packet Captures of Decrypted Control Traffic

Test Result

Success: When the IPsec tunnel is implemented on the untrusted link, (1) an eavesdropper cannot read the control plane traffic over the link (it all appears as ESP-encrypted packets with source and destination addresses as the endpoints of the tunnel) and (2) modified and injected control packets fail to pass out of the tunnel. When IPsec is not implemented, the contents of the packets on the untrusted link are decipherable. Also, without IPsec encryption, some injected control packets appear to be rejected by the MME as indicated by ABORT messages.

Test Case 3, TC-IPsec-03

The objective of Test Case 3, TC-IPsec-03 is to demonstrate the efficacy of end-to-end TLS encryption over the 5G NSA network.

Objective: Verify inability to eavesdrop, modify, or inject payload on UP

As in previous sections, Table 9 lists the files used to store packet captures where those file names are shown in the headers of the Wireshark windows.

Table 9: Test Case 3 Raw Data Files and Content Descriptions for Runs with and without IPsec Encryption on Untrusted Link

Filename	Contents
test_1a_tls_noipsec_UE-device_050323.pcapng	TLS traffic generated at UE device, captured at TP1
final_test_3a_tls_noipsec_testlaptop_050322.pcapng	Injected traffic without IPsec encryption on the untrusted link, injected at TP3
final_test_3a_tls_noipsec_pluribus_050322.pcapng	Captured injected traffic at TP4 on outgoing interface toward LTE core when traffic is not encrypted on the untrusted link
final_test_3a_tls_noipsec_R6K_050322.pcapng	Traffic captured on ingress interface RAN- side R6K – only TLS traffic generated or received by the UE during this test
test3A-MITRE-r6k-noipsec-050322-1622.pcap	Traffic captured on core-side ingress R6K interface from RAN when traffic is not encrypted on the untrusted link
test3A-MITRE-r6k-clear-050322-1622.pcap	Traffic captured on core-side egress R6K interface toward internet when traffic is not encrypted on the untrusted link
mod_esp_tls050322.pcapng	Modified IPsec-encrypted TLS traffic
final_test_3b_tls_ipsec_testlaptop_050322.pcapng	Injected TLS traffic with IPsec encryption on the untrusted link
final_test_3b_tls_ipsec_pluribus_050322.pcapng	Captured injected TLS traffic on outgoing interface toward LTE core with IPsec encryption on the untrusted link
test3B-MITRE-r6k-ipsec-050322-1630.pcap	IPsec encrypted TLS traffic captured on core-side ingress R6K interface from RAN
test3B-MITRE-r6k-clear-050322-1630.pcap	IPsec decrypted TLS traffic captured on core-side egress R6K interface toward internet
final_test_3b_tls_ipsec_R6K_050322.pcapng	Actual TLS traffic sent/recevied by UE captured at trusted interface of RAN-side R6K

Figure 19 shows the Wireshark windows with the traffic generated at the UE (TP1), injected traffic on the untrusted link (TP3), and traffic captured on the untrusted link as it heads toward the LTE core (TP4). TLS messages appear as TLS in the three packet captures with no ability to look inside to determine the contents. Figure 20 shows the same information captured on the coreside router (TP5). Specifically, 311 injected TLS packets were captured on the ingress R6K router interface at the core, and 376 TLS packets were seen on the egress interface of that router. In contrast, Figure 21 shows that only three TLS packets were generated by the UE and one TLS packet was received by the UE (identified by IP address 172.18.0.3), suggesting that the many

other packets observed in Figure 19 and Figure 20 were dropped due to being malformed encrypted packets injected as part of the test.

and them do capture i	Analyze Statistics Tele	phony Wireless To	ols Help				
🔳 🖉 💿 📙 🛅 🔀 🕻	ة 🛸 🗢 🌾 ا	👲 📃 📃 e	B. Q. Q. 🎹				
5							
Time	Source	Destination	Protocol	Lengtl Info			_
75 2022-05-03 13:38:50.25	208 172.18.0.3	65.55.44.109	TLSv1.2	539 Application Da	ata		
79 2022-05-03 13:38:50.269		172.18.0.3	TLSv1.2	194 Application Da			
83 2022-05-03 13:38:50.28		172.18.0.3	TLSv1.2	194 Application Da			
97 2022-05-03 13:38:50.940		20.50.201.200	TLSv1.2	425 Application Da			
06 2022-05-03 13:38:51.059 08 2022-05-03 13:38:51.16		20.50.201.200 172.18.0.3	TLSv1.2 TLSv1.2	311 Application Da			
11 2022-05-03 13:38:51.942		20.50.201.200	TLSv1.2	469 Application Da 412 Application Da			
25 2022-05-03 13:38:52.11		20.50.201.200	TLSv1.2	557 Client Hello			
30 2022-05-03 13:38:52.203		20.50.201.200	TLSv1.2	437 Application Da	ata		
31 2022-05-03 13:38:52.22	2062 20.50.201.200	172.18.0.3	TLSv1.2	1072 [TCP Previous	segment not captured] , Igno	ored Unknown Record	
43 2022-05-03 13:38:52.309		172.18.0.3	TLSv1.2	469 Application Da			
67 2022-05-03 13:38:52.33	616 172.18.0.3	65.55.44.109	TLSv1.2	133 Client Key Exc	change, Change Cipher Spec, E	Encrypted Handshake Message	
							>
Frame 331: 1072 bytes on w	ire (8576 bits), 10	72 bytes captured	(8576 bits) on int	terface \Device\NPF_{	AD825110-5F39-4C2E-B476-1BED	A4D5C3EF}, id 0	
Raw packet data							
Internet Protocol Version							
Transmission Control Proto	col, Src Port: 443,	Dst Port: 57740,	Seq: 5193, Ack: 51	18, Len: 1032			
Transport Layer Security V Ignored Unknown Record							
> [Expert Info (Warni	ng/Protocol): Ignor	ed Unknown Record]					
final_test_3a_tls_noipsec_test							- 0
		T 1 1 1 1 1 1 1					
File Edit View Go Captu		lelephony Wireless					
📶 🔳 🙋 💿 📜 🛅 🔰	र् 🎑 🤍 🔶 🗎	2 🛉 生 其 📘	••••				
tis							× →
No. Time		Source	Destination	Protocol	Lengti Info		
1776 2022-05-03 16:20		172.18.0.3	20.50.201.200	GTP <tlsv1.2></tlsv1.2>	611 Client Hello		
1783 2022-05-03 16:20		20.50.201.200	172.18.0.3	GTP <tlsv1.2></tlsv1.2>		ot captured] , Ignored Unknow	wn Record
1801 2022-05-03 16:20		172.18.0.3	65.55.44.109	GTP <tlsv1.2></tlsv1.2>		ange Cipher Spec, Encrypted I	
1803 2022-05-03 16:20		55.55.44.109	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	145 Change Cipher Spec, Enc		
1804 2022-05-03 16:20	:50.848864132	L72.18.0.3	20.50.201.200	GTP <tlsv1.2></tlsv1.2>	491 Application Data		
1807 2022-05-03 16:20	:50.969075649	20.50.201.200	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	523 Application Data		
1814 2022-05-03 16:20		55.55.44.109	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	530 Application Data		
1820 2022-05-03 16:20		172.18.0.3	65.55.44.109	GTP <tlsv1.2></tlsv1.2>	526 Application Data		
1825 2022-05-03 16:20		172.18.0.3	65.55.44.109	GTP <tlsv1.2></tlsv1.2>	919 Application Data		
1828 2022-05-03 16:20	1:51.043865484	172.18.0.3	20.36.253.92	GTP <tlsv1.2></tlsv1.2>	180 Application Data		>
S 50000 1703, 1105 hitse							
> Frame 1783: 1126 bytes > Ethernet II, Src: 66:0	🚄 final_test_3a_tls_noi	psec_pluribus_050322.pd	apng				
> 802.1Q Virtual LAN, PR	File Edit View Go	Canture Analyze	Statistics Telephony	Wireless Tools Help			
> Internet Protocol Vers							
> User Datagram Protocol		📄 🗙 🎑 🍳	🦛 🏓 譬 🌪 🏓		₹ Ⅲ		
> GPRS Tunneling Protoco	tis						
	No. Time		Source	Destination	Protocol	Lengti Info	
> Internet Protocol Vers		16:19:47.801722	172.18.0.3	20,50,201,200	GTP <tlsv1.2></tlsv1.2>	657 Client Hello	
> Transmission Control P	4812 2022-05-03				GTP <tlsv1.2></tlsv1.2>	1172 [TCP Previous segmen	t not capt
 Transmission Control P Transport Laver Securi 		16:19:47.890201	20.50.201.200	172.18.0.3			
 Transmission Control P Transport Layer Securi Ignored Unknown Rec 	4826 2022-05-03		20.50.201.200 172.18.0.3	172.18.0.3 65.55.44.109	GTP <tlsv1.2></tlsv1.2>	233 Client Key Exchange,	Encrypted
 Transmission Control P Transport Layer Securi Ignored Unknown Red [Expert Info (W) 	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639	172.18.0.3 65.55.44.109	65.55.44.109 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec,	
 Transmission Control P Transport Layer Securi Ignored Unknown Red [Expert Info (W [Ignored Unknown]] 	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4869 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625	172.18.0.3 65.55.44.109 172.18.0.3	65.55.44.109 172.18.0.3 20.50.201.200	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data	
 Transmission Control P Transport Layer Securi Ignored Unknown Red [Expert Info (W) 	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4869 2022-05-03 4876 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data	
<pre>> Transmission Control P > Transport Layer Securi > Ignored Unknown Rec</pre>	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4869 2022-05-03 4876 2022-05-03 4888 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.144722	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data	
> Transmission Control P Transport Layer Securi	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4869 2022-05-03 4867 2022-05-03 4868 2022-05-03 4876 2022-05-03 4888 2022-05-03 4888 2022-05-03 4901 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.144722 16:19:48.170728	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 572 Application Data	
> Transmission Control P Transport Layer Securi Ignored Unknown Ret [Expert Info (W [Ignored Unh [Severity 1, [Group: Pro 0000 66 0e 94 bc 8	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4869 2022-05-03 4876 2022-05-03 4888 2022-05-03 4901 2022-05-03 4906 2022-05-03	16:19:47.830201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.144722 16:19:48.170728 16:19:48.170844	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109 65.55.44.109	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 572 Application Data 965 Application Data	
> Transmission Control P Transport Layer Securi Ignored Unknown Red [Expert Info (w [Ignored Unh [severity 1r [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 00 10 10 10 10 10 10 10 10 10 10 10 10	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4867 2022-05-03 4876 2022-05-03 4888 2022-05-03 4901 2022-05-03 4906 2022-05-03 4905 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.144722 16:19:48.170728 16:19:48.170844 16:19:48.170612	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 572 Application Data 965 Application Data 226 Application Data	
<pre>> Transmission Control P Transport Layer Securi</pre>	4826 2022-05-05 4863 2022-05-03 4867 2022-05-03 4867 2022-05-03 4876 2022-05-03 4876 2022-05-03 4901 2022-05-03 4906 2022-05-03 4915 2022-05-03 4917 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.144722 16:19:48.170728 16:19:48.170844 16:19:48.170612	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109 65.55.44.109 20.36.253.92	GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 572 Application Data 965 Application Data	
> Transmission Control P Transport Layer Securi Y Ignored Unknown Red (Expert Info (k [Export Info (k [Expo	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4869 2022-05-03 4869 2022-05-03 4888 2022-05-03 4901 2022-05-03 4906 2022-05-03 4915 2022-05-03 4927 2022-05-03 4947 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.144722 16:19:48.170728 16:19:48.170844 16:19:48.177612 16:19:48.185841	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109 65.55.44.109 20.36.253.92 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 237 Application Data	
<pre>> Transmission Control P > Transport Layer Securi</pre>	4326 2022-05-02 4867 2022-05-02 4867 2022-05-03 4867 2022-05-03 4876 2022-05-03 4876 2022-05-03 4988 2022-05-03 4996 2022-05-03 4995 2022-05-03 4997 2022-05-03 4947 2022-05-03 4947 2022-05-03	16:19:47.890201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.14722 16:19:48.170728 16:19:48.170728 16:19:48.177612 16:19:48.185841 16:19:48.210631	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 266 Application Data 273 Application Data 657 Client Hello	t not capt
<pre>> Transmission Control P > Transport Layer Securi > Ignored Unknown Rei > [Expert Info (w [gnored unknown Rei > [Expert Info (w [gnored unknown Rei > [Expert Info (w) [group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0020 ff d2 c0 a8 0 0030 04 30 4c c8 0 0040 98 b2 14 32 c 0050 73 cf 6b 45 8 0060 e6 55 68 bb a </pre>	4326 2022-05-02 4867 2022-05-02 4867 2022-05-03 4867 2022-05-03 4876 2022-05-03 4876 2022-05-03 4988 2022-05-03 4996 2022-05-03 4995 2022-05-03 4997 2022-05-03 4947 2022-05-03 4947 2022-05-03	16:19:47.850201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.10870 16:19:48.10870 16:19:48.170728 16:19:48.170724 16:19:48.177612 16:19:48.17561 16:19:48.223176	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 65.55.44.109	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 21.38.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data	t not capt
<pre>> Transmission Control P > Transport Layer Securi > Ignored Unknown Rei > [Expert Info (w [severity li [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0020 ff d2 c0 a8 0 0030 04 30 4c c8 0 0040 98 b2 14 32 cc 0050 73 cf 6b 45 8 0060 e6 55 68 bb a 0070 04 03 02 07 8 0080 15 07 04 2f 3</pre>	4826 2022-05-02 4863 2022-05-02 4867 2022-05-03 4867 2022-05-03 4867 2022-05-03 4869 2022-05-03 4901 2022-05-03 4901 2022-05-03 4901 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03	16:19:47.830201 16:19:47.967596 16:19:47.976639 16:19:47.982625 16:19:48.102870 16:19:48.170728 16:19:48.170728 16:19:48.170728 16:19:48.177612 16:19:48.185841 16:19:48.223176 16:19:48.223070	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 65.55.44.109 65.55.44.109	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 172.18.0.3 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data	t not capt
 Transport Layer Securit Transport Layer Securit Tgnored Unknown Rei Expert Info (K) Ignored Unknown (Escerity 1) [Group: Prot (Group: Prot (Group: Prot (Group: Case (Cose)) (Group: C	4826 2022-05-02 4863 2022-05-02 4867 2022-05-03 4867 2022-05-03 4867 2022-05-03 4869 2022-05-03 4901 2022-05-03 4901 2022-05-03 4901 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03 4905 2022-05-03	16:19:47.850201 16:19:47.967563 16:19:47.967639 16:19:47.982625 16:19:48.108280 16:19:48.108280 16:19:48.124722 16:19:48.178728 16:19:48.178728 16:19:48.178844 16:19:48.178612 16:19:48.223176 16:19:48.223176 16:19:48.223076	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 65.55.44.109 65.55.44.109 128.8.46.80, bst	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data	t not capt
<pre>> Transmission Control P > Transport Layer Securi > Ignored Unknown Rei > [Expert Info (w [severity li [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0020 ff d2 c0 a8 0 0030 04 30 4c c8 0 0040 98 b2 14 32 cc 0050 73 cf 6b 45 8 0060 e6 55 68 bb a 0070 04 03 02 07 8 0080 15 07 04 2f 3</pre>	4826 2022-05-03 4863 2022-05-03 4867 2022-05-03 4867 2022-05-03 4867 2022-05-03 4901 2022-05-03 4901 2022-05-03 4901 2022-05-03 4901 2022-05-03 4902 202-05-03 4915 2022-05-03 4903 2022-05-03 4963 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03 4968 2022-05-03	16:19:47.850201 16:19:47.967563 16:19:47.967639 16:19:47.982625 16:19:48.108280 16:19:48.108280 16:19:48.124722 16:19:48.178728 16:19:48.178728 16:19:48.178844 16:19:48.178612 16:19:48.223176 16:19:48.223176 16:19:48.223076	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 20.36.253.92 172.18.0.3 25.55.44.109 65.55.44.109	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data	t not capt
Transmission Control P Transport Layer Securi ' Imansport Layer Securi ' Imansport Layer Securi ' Imansport Layer Security I [Severity I [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0010 08 00 45 28 0 0020 ff d2 c0 a8 0010 08 00 42 c8 0020 ff d2 c0 a8 0020 ff d2 c0 a8 0020 66 0e 94 bc 8 0020 ff d2 c0 a8 0020 66 05 68 bb a 0060 66 55 68 bb a 0060 68 87 bd d7 1	4326 2022-05-02 4867 2022-05-02 4867 2022-05-02 4867 2022-05-03 4867 2022-05-03 4876 2022-05-03 4901 2022-05-03 4901 2022-05-03 4901 2022-05-03 4915 2022-05-03 4915 2022-05-03 4963 202 4963 4963 202 4963 496 496 4963 496 496	16:19:47.850201 16:19:47.967596 16:19:47.967596 16:19:47.987639 16:19:48.108260 16:19:48.108260 16:19:48.12482 16:19:48.178728 16:19:48.178728 16:19:48.178612 16:19:48.223176 16:19:48.223176 16:19:48.223076 16:19:48.12307 16:19:	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 65.55.44.109 65.55.44.109 65.55.44.109 128.8.46.80, Dst 59324, Dst Port: work 44 (66:0e:94:bc:84	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 1	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data 593 [TCP Previous Segmen	t not capt
Transmission Control P Transport Layer Securi ' Imansport Layer Securi ' Imansport Layer Securi ' Imansport Layer Security I [Severity I [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0010 08 00 45 28 0 0020 ff d2 c0 a8 0010 08 00 42 c8 0020 ff d2 c0 a8 0020 ff d2 c0 a8 0020 66 0e 94 bc 8 0020 ff d2 c0 a8 0020 66 05 68 bb a 0060 66 55 68 bb a 0060 68 87 bd d7 1	4826 2022-05-03 4853 2022-05-03 4857 2022-05-03 4857 2022-05-03 4857 2022-05-03 4901 2022-05-03 4906 2022-05-03 4901 2022-05-03 4901 2022-05-03 4912 2022-05-03 4927 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 4963 2022-05-03 C Vartual extensis Ethernet II, So Internet Protoco > Internet Protoco Source	16:19:47.830201 16:19:47.967596 16:19:47.967599 16:19:47.976639 16:19:48.102870 16:19:48.102870 16:19:48.170728 16:19:48.170728 16:19:48.170728 16:19:48.170728 16:19:48.223176 16:19:48.22576 16:19:48.22576 17:19:19:19 17:19:19	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 20.36.253.92 172.18.0.3 25.55.44.109 65.55.44.109 128.8.46.80, Dst 59324, Dst Port: work 4a (66:0e:94:bc:86 192.168.255.210,	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 1	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data 593 [TCP Previous Segmen	t not capt
Transmission Control P Transport Layer Securi ' Imansport Layer Securi ' Imansport Layer Securi ' Imansport Layer Security I [Severity I [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0010 08 00 45 28 0 0020 ff d2 c0 a8 0010 08 00 42 c8 0020 ff d2 c0 a8 0020 ff d2 c0 a8 0020 66 0e 94 bc 8 0020 ff d2 c0 a8 0020 66 05 68 bb a 0060 66 55 68 bb a 0060 68 87 bd d7 1	4326 2022-05-02 4867 2022-05-02 4867 2022-05-03 4867 2022-05-03 4869 2022-05-03 4876 2022-05-03 4906 2022-05-03 4906 2022-05-03 4915 2022-05-03 4915 2022-05-03 4963 2022 495 49	16:19:47,39201 16:19:47,97639 16:19:47,97639 16:19:47,97639 16:19:44,92625 16:19:48,10870 16:19:48,10870 16:19:48,170728 16:19:48,177512 16:19:48,177512 16:19:48,120631 16:19:48,223076 16:19:48,223076 16:19:48,225070 10 Version 4, Src: rotacol, Src Port: rotacol, Src Port:	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 20.36.253.92 172.18.0.3 25.55.44.109 65.55.44.109 128.8.46.80, Dst 59324, Dst Port: work 4a (66:0e:94:bc:86 192.168.255.210,	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 1	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data 593 [TCP Previous Segmen	t not capt
Transmission Control P Transport Layer Securi ' Imansport Layer Securi ' Imansport Layer Securi ' Imansport Layer Security I [Severity I [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0010 08 00 45 28 0 0020 ff d2 c0 a8 0010 08 00 42 c8 0020 ff d2 c0 a8 0020 ff d2 c0 a8 0020 66 0e 94 bc 8 0020 ff d2 c0 a8 0020 66 05 68 bb a 0060 66 55 68 bb a 0060 68 87 bd d7 1	4326 2022-05-02 4653 2022-05-02 4857 2022-05-03 4857 2022-05-03 4857 2022-05-03 4858 2022-05-03 4901 2022-05-03 4901 2022-05-03 4905 202-05-03 4905 202-05-0	16:19:47.830201 16:19:47.967596 16:19:47.967596 16:19:47.987639 16:19:48.10876 16:19:48.10870 16:19:48.10870 16:19:48.178728 16:19:48.17824 16:19:48.17824 16:19:48.17824 16:19:48.22697 01 Version 4, Src: rotocol, Src Port: ble Local Area Net c: 66:0:9:94:bc:80: 01 Version 4, Src: rotocol, Src Port: Protocol	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 20.36.253.92 172.18.0.3 65.55.44.109 65.55.44.109 65.55.44.109 128.8.46.80, Dst 59324, Dst Port: work 40 (66:0e:94:bb:18 192.168.255.210, 2152, Dst Port:	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 172.18.0.3 172.18.	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data 593 [TCP Previous Segmen	t not capt
Transmission Control P Transport Layer Securi ' Imansport Layer Securi ' Imansport Layer Securi ' Imansport Layer Security I [Severity I [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0010 08 00 45 28 0 0020 ff d2 c0 a8 0010 08 00 42 c8 0020 ff d2 c0 a8 0020 ff d2 c0 a8 0020 66 0e 94 bc 8 0020 ff d2 c0 a8 0020 66 05 68 bb a 0060 66 55 68 bb a 0060 68 87 bd d7 1	4326 3022-05-03 4865 2022-05-02 4867 2022-05-03 4867 2022-05-03 4869 2022-05-03 4886 2022-05-03 4906 2022-05-03 4905 2022-05-03 4915 2022-05-03 4927 2022-05-03 4936 2022-05-03 4936 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 5 Unternet Protoc Visrtual extensi Ethernet II, 57 1 Internet Protoc 2 User Datagram P 9 GPRS Tunneling 9 GPRS Tunneling 1 Internet Protoc	16:19:47.367201 16:19:47.97659 16:19:47.97659 16:19:47.97659 16:19:44.1982625 16:19:48.102870 16:19:48.102870 16:19:48.102870 16:19:48.177612 16:19:48.17864 16:19:48.218651 16:19:48.223070 16:19:48.223070 16:19:48.223070 16:19:48.223070 16:19:48.223070 10:19:48.	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 20.36.253.92 172.18.0.3 26.55.44.109 65.55.44.109 65.55.44.109 128.8.46.80, Dst 59324, Dst Port: work 4a (66:0e:94:bc:86 192.168.255.210, 2152, Dst Port: 20.50.201.200, Ds	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 2:10.205.67.130 4789	GTP <tlsv1.2> GTP <tlsv1.2> GT</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data 593 [TCP Previous Segmen	t-not capt
Transmission Control P Transport Layer Securi ' Imansport Layer Securi ' Imansport Layer Securi ' Imansport Layer Security I [Severity I [Group: Pro 0000 66 0e 94 bc 8 0010 08 00 45 28 0 0010 08 00 45 28 0 0020 ff d2 c0 a8 0010 08 00 42 c8 0020 ff d2 c0 a8 0020 ff d2 c0 a8 0020 66 0e 94 bc 8 0020 ff d2 c0 a8 0020 66 05 68 bb a 0060 66 55 68 bb a 0060 68 87 bd d7 1	4326 3022-05-03 4865 2022-05-02 4867 2022-05-03 4867 2022-05-03 4869 2022-05-03 4886 2022-05-03 4906 2022-05-03 4905 2022-05-03 4915 2022-05-03 4927 2022-05-03 4936 2022-05-03 4936 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 49363 2022-05-03 5 Unternet Protoc Visrtual extensi Ethernet II, 57 1 Internet Protoc 2 User Datagram P 9 GPRS Tunneling 9 GPRS Tunneling 1 Internet Protoc	16:19:47.830201 16:19:47.967596 16:19:47.976639 16:19:47.976639 16:19:48.102870 16:19:48.102870 16:19:48.124722 16:19:48.124722 16:19:48.124722 16:19:48.124722 16:19:48.127612 16:19:48.128541 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.2253070 16:19:48.7255070 16:19:19:19:19:19:19:195	172.18.0.3 65.55.44.109 172.18.0.3 20.50.201.200 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 20.36.253.92 172.18.0.3 20.36.253.92 172.18.0.3 26.55.44.109 65.55.44.109 65.55.44.109 128.8.46.80, Dst 59324, Dst Port: work 4a (66:0e:94:bc:86 192.168.255.210, 2152, Dst Port: 20.50.201.200, Ds	65.55.44.109 172.18.0.3 20.50.201.200 172.18.0.3 172.18.0.3 172.18.0.3 65.55.44.109 20.36.253.92 172.18.0.3 65.55.44.109 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 172.18.0.3 2:10.205.67.130 4789	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	233 Client Key Exchange, 191 Change Cipher Spec, 537 Application Data 569 Application Data 576 Application Data 965 Application Data 226 Application Data 273 Application Data 657 Client Hello 294 Application Data 593 [TCP Previous Segmen	t net capt

Figure 19: Capture of TLS-Encrypted Packets at UE, Injected/Modified Packets on Untrusted Link, and Capture of Packets on Outgoing Link to Core without IPsec Tunnel on Untrusted Link

test3A-MITRE-r6k-noipsec-050322-1	619.pcap				- 0	\times
Edit View Go Capture Ar	alvze Statistics Telephony	Wireless Tools Help				
	। ९ 🗰 🔿 🖭 🚡 👲	= e e e	TT			
<u>.</u>					\bowtie	• +
Time	Source	Destination	Protocol	Lengti Info		^
2934 2022-05-03 16:19:46.	376961 172.18.0.3	20.50.201.200	GTP <tlsv1.2></tlsv1.2>	466 Application Data	-	
2948 2022-05-03 16:19:46.		20.50.201.200	GTP <tlsv1.2></tlsv1.2>	611 Client Hello		
2962 2022-05-03 16:19:46.		172.18.0.3	GTP <tlsv1.2></tlsv1.2>		not captured] , Ignored Unknown Record	
2998 2022-05-03 16:19:46. 3002 2022-05-03 16:19:46.		65.55.44.109 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	145 Change Cipher Spec, En	hange Cipher Spec, Encrypted Handshake Message	
3004 2022-05-03 16:19:46.		20.50.201.200	GTP <tlsv1.2></tlsv1.2>	491 Application Data		_
3010 2022-05-03 16:19:46.	797128 20.50.201.200	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	523 Application Data		
3024 2022-05-03 16:19:46.		172.18.0.3	GTP <tlsv1.2></tlsv1.2>	530 Application Data		
3035 2022-05-03 16:19:46.		65.55.44.109	GTP <tlsv1.2></tlsv1.2>	526 Application Data		
3048 2022-05-03 16:19:46. 3060 2022-05-03 16:19:46.		20.36.253.92 172.18.0.3	GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	180 Application Data 227 Application Data		
3079 2022-05-03 16:19:46.		65.55.44.109	GTP <tlsv1.2></tlsv1.2>	611 Client Hello		
3095 2022-05-03 16:19:46.	917369 65.55.44.109	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	248 Application Data		
3100 2022-05-03 16:19:46.		172.18.0.3	GTP <tlsv1.2></tlsv1.2>		not captured] , Ignored Unknown Record	
3139 2022-05-03 16:19:46.	963822 172.18.0.3	65.55.44.109	GTP <tlsv1.2></tlsv1.2>	438 Application Data		~
					>	
thernet II, Src: 66:0e:94:0		21), Dst: Ericsson_85	:91:d5 (98:7a:10:85:9	1:d5)		^
02.1Q Virtual LAN, PRI: 0,						
nternet Protocol Version 4 ser Datagram Protocol, Src						
PRS Tunneling Protocol	Port: 2152, DSt Port: 21	.52				
nternet Protocol Version 4	Sec. 20 50 201 200 Det	• 172 18 0 3				
ransmission Control Protoco						-
ransport Layer Security	File Edit View Go Ca	pture Analyze Statistics	Telephony Wireless Te	ools Help		
 ✓ Ignored Unknown Record ✓ [Expert Info (Warnin) 		🕅 🙆 🍳 👄 🍝		B. Q. Q. IT		
[Ignored Unknown				4 4 4 II		
[Severity level:	tis 📃					
[Group: Protocol]		Source	Destinatio		Lengti Info	
0 98 7a 10 85 91 d5	3468 2022-05-03 16:				496 Application Data [TCP segment of a	
Transport Layer Security: Protoco	3488 2022-05-03 16: 3503 2022-05-03 16:				321 Application Data, Application Data 466 Application Data	a
	3516 2022-05-03 16:				611 Client Hello	
	3530 2022-05-03 16:				1126 [TCP Previous segment not captured	d], Ig
	3566 2022-05-03 16:				187 Client Key Exchange, Change Cipher	
	3570 2022-05-03 16:				145 Change Cipher Spec, Encrypted Hand	dshake
		19:46.674412 172.18.	0.3 20.50.2	01.200 GTP <tlsv1.2></tlsv1.2>	491 Application Data	
	3572 2022-05-03 16:	10.46 704617 - 30 50 3	01 200 172 18	0.2 CTD (TLC)(1.2)		
	3578 2022-05-03 16:				523 Application Data	
×		19:46.836500 65.55.4	4.109 172.18	0.3 GTP <tlsv1.2></tlsv1.2>	530 Application Data	
×	3578 2022-05-03 16: 3592 2022-05-03 16:	19:46.836500 65.55.4 19:46.862573 172.18.	4.109 172.18 0.3 65.55.4	0.3 GTP <tlsv1.2> 44.109 GTP <tlsv1.2></tlsv1.2></tlsv1.2>		
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16:	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.877441 20.36.2	44.109 172.18 0.3 65.55.4 0.3 20.36.2 153.92 172.18	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 253.92 GTP <tlsv1.2> 0.3 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data	
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16:	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.877441 20.36.2 19:46.902437 172.18.	44.109 172.18 0.3 65.55.4 0.3 20.36.2 153.92 172.18 0.3 65.55.4	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 253.92 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello	
× +	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16: 3663 2022-05-03 16:	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.877441 20.36.2 19:46.902437 172.18. 19:46.914862 65.55.4	44.109 172.18. 0.3 65.55.4 0.3 20.36.2 153.92 172.18. 0.3 65.55.4 44.109 172.18.	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 253.92 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.4.109 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.3 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data	41 7.
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16: 3663 2022-05-03 16: 3663 2022-05-03 16: 3668 2022-05-03 16: 3678 2022-05-03 16: 3688 202000000000000000000000000000000000	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.877441 20.36.2 19:46.902437 172.18. 19:46.914862 65.55.4 19:46.914862 65.55.4	44.109 172.18. 0.3 65.55.4 0.3 20.36.2 153.92 172.18. 0.3 65.55.4 0.4.109 172.18.	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 53.92 GTP <tlsv1.2> 0.3 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 (TCP Previous segment not captured	d], Ig
*	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16: 3663 2022-05-03 16:	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.877441 20.36.2 19:46.902437 172.18. 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.916395 57.57.4	44.109 172.18. 0.3 65.55.4 0.3 20.36.4 0.3 20.36.5 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.41.09 172.18. 0.3 65.55.4 0.3 65.55.4	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 553.92 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 44.109 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data	d] , Ig
*	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3667 2022-05-03 16: 3663 2022-05-03 16: 3663 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3714 2022-05-03 16: 3714 2022-05-03 16: 3714 2022-05-03 16: 3716 2022-05-03 16: 3717 2022-05-03 16: 3716 2022-05-03 16: 3717 2022-05-03 16: 3716 2020000000000000000000000000000000000	19:46.836500 65.55.4 19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.902437 172.18. 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.916895 572.18. 19:46.970680 65.55.4	44.109 172.18. 0.3 65.55. 0.3 20.36. 55.92 172.18. 4.109 172.18. 44.109 172.18. 0.3 65.55.4 4.109 172.18. 4.109 172.18. 0.3 65.55.4	0.3 GTP <tlsv1.2> 44.109 GTP <tlsv1.2> 44.109 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 44.109 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.4109 GTP <tlsv1.2> 0.3 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data	d] , Ig
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16: 3663 2022-05-03 16: 3707 2022-05-03 16: 3714 2022-05-03 16: 3726 2022-05-03 16: 3727 2022-05-03 16: 3726 2022-05-03 16: 3726 2022-05-03 16: 3727 2022	19:46.836500 65.55.4 19:46.836570 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.803741 20.36.2 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.92080 65.55.4 19:46.970808 65.54.4 19:46.970808 65.54.4	44.109 172.18. 0.3 65.55.4 0.3 28.36.5 153.92 172.18. 0.3 65.55.4 0.4 109 172.18 0.3 0.3 65.55.4 0.4 109 172.18 0.3 0.3 65.55.4 0.3 65.55.5 0.3 65.55.5	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 15.9.22 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.41.09 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data	d] , Ig
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3707 2022-05-03 16: 3706 2022-05-03 16: 3706 2022-05-03 16: 5 7 76 2022-05-03 16: 7 76 2025 205 205 205 205 205 205 205 205 20	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.862573 172.18. 19:46.862573 172.18. 19:46.8627741 20.36.2 19:46.902437 172.18. 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.916805 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.970680 65.55.4 19:46.970680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 19:46.90680 65.55.4 <td>44.189 172.18. 0.3 65.55.4 0.3 28.36.5 153.92 172.18. 0.3 65.55.4 44.189 172.18. 0.3 65.55.4 44.189 172.18. 0.3 65.55.4 44.189 172.18. 0.3 65.55.4 44.199 172.18. 0.3 65.55.4 1.180 172.18. 0.3 65.55.4 1.126 bytes capture</td> <td>0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 63.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.4 GTP (TLSV1.2) 0.4 GTP (TLSV1.2) 0.4 GTP (TLSV1.2) 0.4 GTP (TLSV1.2)</td> <td>530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data 611 Client Hello</td> <td>d], Ig</td>	44.189 172.18. 0.3 65.55.4 0.3 28.36.5 153.92 172.18. 0.3 65.55.4 44.189 172.18. 0.3 65.55.4 44.189 172.18. 0.3 65.55.4 44.189 172.18. 0.3 65.55.4 44.199 172.18. 0.3 65.55.4 1.180 172.18. 0.3 65.55.4 1.126 bytes capture	0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 63.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.4 GTP (TLSV1.2) 0.4 GTP (TLSV1.2) 0.4 GTP (TLSV1.2) 0.4 GTP (TLSV1.2)	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data 611 Client Hello	d], Ig
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3627 2022-05-03 16: 3767 2022-05-03 16: 3774 2022-05-03 16: 3774 2022-05-03 16: 3774 2022-05-03 16: 3774 2022-05-03 16: 3776 2020-05-03 16: 3776 202	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.860364 172.18. 19:46.860364 172.18. 19:46.860374 120.36. 19:46.90374 20.36.2 19:46.904862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.901305 172.18. 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.987372 172<18	44.109 172.18 0.3 65.55.4 0.3 20.365.5 53.92 172.18 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.3 65.55.4 0.126 bytes capture asile:85:91:0%), Dst:	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 15.9.22 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.41.09 GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data 611 Client Hello	d], Ig
×	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3616 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3707 202	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.869364 172.18. 19:46.869364 172.18. 19:46.87741 20.36.2 19:46.90364 172.18. 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.916805 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:47.9717 18 19:48.97172 172 19:49.97172 172	4.109 172.18 0.3 65.55.4 0.3 28.36.5 153.92 172.18 0.3 65.55.4 4.109 172.18 0.3 65.55.4 4.109 172.18 0.3 65.55.4 4.109 172.18 0.3 65.55.4 1.102 bytes capture a:10:85:91:c9), Dst: 704	0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 41.109 GTP (TLSV1.2) 41.09 GTP (TLSV1.	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data 611 Client Hello	d] , Ig
× + ^	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3714 202	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.860364 172.18. 19:46.860364 172.18. 19:46.860374 120.36. 19:46.90374 20.36.2 19:46.904862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.901305 172.18. 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.987372 172<18	4.189 172.18 0.3 65.55.4 0.3 28.365. 153.92 172.18 0.3 65.55.4 4.189 172.18 0.3 65.55.4 4.189 172.18 0.3 65.55.4 4.189 172.18 0.3 65.55.4 1.126 bytes capture a:18:85:91:c9), Dst: 704 .255.210, Dst: 192.16	0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 41.109 GTP (TLSV1.2) 41.09 GTP (TLSV1.	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data 611 Client Hello	d], Ig
	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3714 202	19:46.836500 65.55.4 19:46.80573 172.18. 19:46.805364 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.912805 65.55.4 19:46.914862 65.55.4 19:46.912805 172.18. 19:46.970806 65.55.4 19:46.970808 65.57.4 19:46.970808 65.57.7 19:46.970808 65.57.7 19:46.970808 65.57.7 19:46.970808 65.57.4 19:46.970808 65.57.7 19:46.970808 65.57.7 19:46.970808 65.57.4 19:46.970808 65.57.4 19:46.970808 65.57.4 10:46.970808 65.57.4 10:46.970808 65.57.4 10:46.970808 65.57.4 10:46.970808 65.57.4 10:46.970808 65.57.4 10:47.9717 172 10:5717 192.18	4.189 172.18 0.3 65.55.4 0.3 28.365. 153.92 172.18 0.3 65.55.4 4.189 172.18 0.3 65.55.4 4.189 172.18 0.3 65.55.4 4.189 172.18 0.3 65.55.4 1.126 bytes capture a:18:85:91:c9), Dst: 704 .255.210, Dst: 192.16	0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 4.109 GTP (TLSV1.2) 4.109 GTP (TLSV1.2) 4.109 GTP (TLSV1.2) 4.109 GTP (TLSV1.2) 1.10	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 [TCP Previous segment not captured 438 Application Data 246 Application Data 611 Client Hello	d], Ig
× •	3578 2022-05-03 16: 3502 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3706 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3706 2022-05-03 16: 3707 202	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.860364 172.18. 19:46.860364 172.18. 19:46.860364 172.18. 19:46.90364 172.18. 19:46.90374 20.36.2 19:46.90367 172.18. 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.903080 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.970808 65.55.4 19:46.97072 172.18 tess on wire (9068 bits 15.9 cicsson_85:91:05 (9.87:192.152, D 15.3 cicl, Src Port: 1252, D 15.9	4.109 172.18. 0.3 65.55. 0.3 20.36: 153.92 172.18. 0.3 65.55. 0.3 172.18. 0.3 172.18.	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.4 100 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 15.105 GTP <tlsv1.2> 1</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 (TCP Previous segment not captured 438 Application Data 611 Client Hello a:b7:81)	d], Ig
× + 	3578 2022-05-03 16: 3592 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3663 2022-05-03 16: 3663 2022-05-03 16: 3707 2020-05-03 16: 3707 2020-05-03 16: 3707 2020-05-05-05-05-05-05-0	19:46.836500 65.55.4 19:46.836570 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.80364 172.18. 19:46.87741 20.36.2 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.914862 65.55.4 19:46.92080 65.55.4 19:46.93080 65.55.4 19:46.93080 65.55.7 19:46.93080 65.55.7 19:46.93080 65.55.7 19:46.93080 65.55.7 19:46.93080 65.55.7 19:46.93080 65.55.7 19:46.970808 65.55.7 19:46.970808 65.55.4 19:46.970808 65.55.7 19:46.970808 65.55.7 19:46.970808 65.55.4 19:46.97070 172.18 tes on wire (9008) bits ticsson 85:91:09 981:09 tool 0, Src Port: 2152, D 0000 terotool, Src Port: 20.5	4.109 172.18. 0.3 65.55. 0.3 20.36: 153.92 172.18. 0.3 65.55. 0.3 172.18. 0.3 172.18.	0.3 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 44.109 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 0.3 GTP (TLSV1.2) 41.109 GTP (TLSV1.2) 41.09 GTP (TLSV1.2)	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 (TCP Previous segment not captured 438 Application Data 611 Client Hello a:b7:81)	d] , Ig
	3578 2022-05-03 16: 3502 2022-05-03 16: 3603 2022-05-03 16: 3616 2022-05-03 16: 3628 2022-05-03 16: 3647 2022-05-03 16: 3647 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3706 2022-05-03 16: 3707 2022-05-03 16: 3707 2022-05-03 16: 3706 2022-05-03 16: 3707 202	19:46.836500 65.55.4 19:46.862573 172.18. 19:46.862573 172.18. 19:46.863744 172.18. 19:46.963744 20.36.2 19:46.9014862 65.55.4 19:46.9014862 65.55.4 19:46.9014862 65.55.4 19:46.970808 65.55.	4.109 172.18. 0.3 65.55. 0.3 20.36: 153.92 172.18. 0.3 65.55. 0.3 172.18. 0.3 172.18.	0.3 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 0.3 GTP <tlsv1.2> 0.4 100 GTP <tlsv1.2> 14.109 GTP <tlsv1.2> 15.105 GTP <tlsv1.2> 1</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	530 Application Data 526 Application Data 180 Application Data 227 Application Data 611 Client Hello 248 Application Data 547 (TCP Previous segment not captured 438 Application Data 611 Client Hello a:b7:81)	d] , Ig

Figure 20: Capture of TLS-Encrypted Packets at Core-Side Router Interfaces without IPsec Tunnel on Untrusted Link

📕 fi	final_test_3a_tls_noipsec_R6K_050322.pcapng -										
File	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help										
	∡ II 2 @ I II II 2 Q + + + MI F F D II II Q Q Q Q II										
📕 tls											
No.	Time	Source	Destination	Protocol	Lengt Info						
_ 1	0 2022-05-03 16:19:45	172.18.0.3	20.49.99.108	GTP <tlsv1.2></tlsv1.2>	159 Application Da	ta					
2	1 2022-05-03 16:19:59	172.18.0.3	20.49.99.108	GTP <tlsv1.2></tlsv1.2>	159 Application Da	ta					
2	1 2022-05-03 16:19:59	20.49.99.108	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	159 Application Da	ita					
2	2 2022-05-03 16:20:30	172.18.0.3	20.49.99.108	GTP <tlsv1.2></tlsv1.2>	159 Application Da	ta					
<											
	· · · · · · · · · · · · · · · · · · ·					<pre>WPF_{B4103562-16FC-4781-8AF1-BA141D151C5B}, id</pre>					
	hernet II, Src: Ericssor)st: Ericsson_8b:a	a0:4a (98:7a:10:8b:a0:	:4a)					
	Destination: Ericsson_8										
>	Source: Ericsson_eb:3e:	0e (1c:90:be:eb:	3e:0e)								
	Type: IPv4 (0x0800)		055 006 D 1 40								
	ternet Protocol Version	· ·	· · · · · · · · · · · · · · · · · · ·	02.168.8.104							
	> User Datagram Protocol, Src Port: 2152, Dst Port: 2152										
	> GPRS Tunneling Protocol										
	> Internet Protocol Version 4, Src: 172.18.0.3, Dst: 20.49.99.108										
	> Transmission Control Protocol, Src Port: 60855, Dst Port: 443, Seq: 1, Ack: 1, Len: 69										
	Y Transport Layer Security										
~	TLSv1.2 Record Layer: Application Data Protocol: http-over-tls Context Environment Application Data (23)										
				/	Content Type: Application Data (23)						
1 9990	9000 98 7a 10 8b a0 4a 1c 90 be eb 3e 0e 08 00 45 28 · · z··· J·· · · >···E(
0010	00 91 21 00 00 00 ff 1	1 10 98 c0 a8 f	f e2 c0 a8 ···!								
0010 0020	00 91 21 00 <u>00 00</u> ff 1	1 10 98 c0 a8 f d a9 a7 30 ff 0	f e2 c0 a8 ···!			Packets: 2290 · Displayed: 4 (0.2%)					

Figure 21: Capture of TLS-encrypted Packets on RAN-side Router Ingress Showing the Only Traffic Generated/Received by the UE for this Test

As described above, for the tests with IPsec encryption of TLS packets, over 1,000 packets were generated in order to clearly distinguish that injected packets are dropped inside the tunnel. Figure 22 shows the modified and injected IPsec-encrypted packets as well as the corresponding capture of those packets on the outgoing link toward the LTE core. As with the prior tests with IPsec encryption, we only see that the packets are ESP packets with sources and destinations the endpoints of the IPsec tunnel. These captured packets include user traffic and control traffic, where some of the UP packets are TLS packets, although it is impossible to distinguish which are which. Further, the payloads of all packets are not decipherable. Approximately 4,500 modified ESP packets were injected into the transport network.

Figure 23 shows a capture of these packets, both on the RAN-facing interface of the core-side router (where traffic is IPsec encrypted) and on the egress interface of the core-side router, after decryption (both TP5). There is a notable difference in traffic volume. Specifically, approximately 4,600 ESP packets were received on the RAN-facing interface, whereas only 33 packets successfully exit (or enter) the tunnel. Only three of those packets are TLS packets. Figure 24 shows the same three TLS packets on the clear (unencrypted) interface of the RAN-side router (TP2).

	Source 9 192.168.255.254 7 192.168.255.254 7 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 2 101.168.255.254 2 101.168.255.254 2 101.154 bytes capt 0:21 (66:0e:194:d3:a0:21 : 0, ID: 1001	Destination 192.168.8.25 192	4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 5 994:bc:80:4a (66:0	138 E 234 E 234 E 170 E 234 E 154 E 202 F	SP (SPI=0xc2 SP (SPI=0xca SP (SPI=0xca SP (SPI=0xca	5bald8) 5bald8) 5bald8) c068a2) c068a2) 5bald8)	>
Apply a display filter <ctr> Time 1 2022-05-03 13:46:32.920029 2 2022-05-03 13:46:33.151827 3 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.290457 6 2022-05-03 13:46:33.290457 7 2022-05-03 13:46:33.290457 7 2022-05-03 13:46:33.290457 7 2022-05-03 13:46:33.290457 7 2022-05-03 13:46:33.290457 7 2022-05-03 13:46:33.257394 8 2022-05-03 13:46:33.257394 8 2022-05-03 13:46:33.257394 8 2022-05-03 13:46:33.257384 Frame 1: 154 bytes on wire (123: Ethernet II, Src: 66:0e:94:43:ad 802.1Q Virtual LAN, PRI: 0, DEI Internet Protocol Version 4, Srr, Encapsulating File Edt View (0) 000 66 0e 9 000 66 0e 9 000 66 0e 9</ctr>	<pre>9 192.168.255.254 7 192.168.255.254 5 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 2 bits), 154 bytes capt 2 c 192.168.255.254 3 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c</pre>	Destination 192.168.8.25 192	Protocol 4 ESP 4 ESP	154 E 138 E 234 E 234 E 170 E 234 E 154 E 234 C 154 E 202 F	SP (SPI=0xc2 SP (SPI=0xca SP (SPI=0xca SP (SPI=0xca SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xca	5bald8) 5bald8) 5bald8) c068a2) c068a2) 5bald8)	
Time 1 2022-05-03 13:46:32.920025 2 2022-05-03 13:46:33.151827 3 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.290771 6 2022-05-03 13:46:33.298771 7 2022-05-03 13:46:33.25758 Frame 1: 154 bytes on wire (123: Ethernet II, Src: 66:0e:94:43:ad 802.10 Virtual LAN, PRI: 0, DEI: Internet Protocol Version 4, Src Encapsulating final_test_3b_tts:p File Edit View (00 66 0e 9 1 00 08 00 0 1 00 08	<pre>9 192.168.255.254 7 192.168.255.254 5 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 2 bits), 154 bytes capt 2 c 192.168.255.254 3 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c</pre>	192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25	4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 5) 994:bc:80:4a (66:0	154 E 138 E 234 E 234 E 170 E 234 E 154 E 234 C 154 E 202 F	SP (SPI=0xc2 SP (SPI=0xca SP (SPI=0xca SP (SPI=0xca SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xca	5bald8) 5bald8) 5bald8) c068a2) c068a2) 5bald8)	
1 2022-05-03 13:46:32.920029 2 2022-05-03 13:46:33.151827 3 2022-05-03 13:46:33.290455 4 2022-05-03 13:46:33.290455 5 2022-05-03 13:46:33.290871 6 2022-05-03 13:46:33.290872 7 2022-05-03 13:46:33.290872 7 2022-05-03 13:46:33.295827 7 2022-05-03 13:46:33.25758 Frame 1: 154 bytes on wire (123: Ethernet II, Src: 66:0e:94:d3:ad 802.10 Virtual LAN, PRI: 0, DEI Internet Protocol Version 4, Src Encapsulating File Edit View (2000) 00 66 0e 9 00 06 0e 9 00 00 00 00 00 00 00 00 00 00 00 00 00	<pre>9 192.168.255.254 7 192.168.255.254 5 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 2 bits), 154 bytes capt 2 c 192.168.255.254 3 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c 2 c</pre>	192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25	4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 5) 994:bc:80:4a (66:0	154 E 138 E 234 E 234 E 170 E 234 E 154 E 234 C 154 E 202 F	SP (SPI=0xc2 SP (SPI=0xca SP (SPI=0xca SP (SPI=0xca SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xca	5bald8) 5bald8) 5bald8) c068a2) c068a2) 5bald8)	>
2 2022-05-03 13:46:33.151827 3 2022-05-03 13:46:33.290455 4 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.29877 6 2022-05-03 13:46:33.298827 7 2022-05-03 13:46:33.298827 7 2022-05-03 13:46:33.298827 7 2022-05-03 13:46:33.298827 7 2022-05-03 13:46:33.298734 8 2022-05-03 13:46:34.255758 Frame 1: 154 bytes on wire (123: Ethernet II, Src: 66:0e:94:d3:ed 302.10 Virtual LAN, PRI: 0, DEI: Internet Protocol Version 4, Src Encapsulating File Edit View (123: File Edit View	7 192.168.255.254 5 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 1 192.168.255.254 3 192.168.255.254 3 192.168.255.254 3 192.168.193.133.2621 2 bits), 154 bytes capt 0.21 (66:09.193.132.262 0.21 192.168.255.254, Dst psec_testlaptop_050322.pcapng Go Capture Analyze Stat	192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 ured (1232 bit)), Dst: 66:0e: : 192.168.8.25	4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 5 994:bc:80:4a (66:0	138 E 234 E 234 E 170 E 234 E 154 E 202 F	SP (SPI=0xca SP (SPI=0xca SP (SPI=0xca SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xca	5bald8) 5bald8) 5bald8) c068a2) c068a2) 5bald8)	>
3 2022-05-03 13:46:33.290455 4 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.298771 6 2022-05-03 13:46:33.298777 7 2022-05-03 13:46:33.357394 8 2022-05-03 13:46:36 255758 Frame 1: 154 bytes on wire (123) thernet II, Src: 66:08:04:03:40 802.10 Virtual LAN, PRI: 0, DEI: Internet Protocol Version 4, Src Incapsulating final_test_3b_tts_jp File Edit View (120) 00 66 0e 9	<pre>5 192.168.255.254 7 192.168.255.254 7 192.168.255.254 7 192.168.255.254 8 192.168.255.254 8 192.168.255.254 8 192.168.255.254 9 101.166:0e:94:d3:a0:21 1 0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapng Go Capture Analyze Stat</pre>	192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25	4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 4 ESP 5 994:bc:80:4a (66:6	234 E 234 E 170 E 234 E 154 E 202 F	SP (SPI=0xca SP (SPI=0xca SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xc2	5ba1d8) 5ba1d8) c0668a2) c0668a2) 5ba1d8)	>
4 2022-05-03 13:46:33.290457 5 2022-05-03 13:46:33.290871 6 2022-05-03 13:46:33.298872 7 2022-05-03 13:46:33.29872 7 2022-05-03 13:46:33.257394 8 2022-05-03 13:46:36 255758 internet II, Src: 66:08:94:43:43 internet Protocol Version 4, Src internet Version 4, Src internet Protocol Version 4, Src intern	7 192.168.255.254 1 192.168.255.254 7 192.168.255.254 3 192.168.255.254 3 192.168.255.254 2 bits), 154 bytes capt 0:21 (66:0e:94:d3:a0:21 : 0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapnog Go Capture Analyze Stat	192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 uured (1232 bit), Dst: 66:0e: : 192.168.8.25	4 ESP 4	234 E 170 E 234 E 154 E 202 F	SP (SPI=0xca SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xca	5ba1d8) c068a2) c068a2) 5ba1d8)	>
5 2022-05-03 13:46:33.29871 6 2022-05-03 13:46:33.298827 7 2022-05-03 13:46:33.357394 8 2022-05-03 13:46:36.255758 irame 1: 154 bytes on wire (123) thernet II, Src: 66:0e:94:d3:a6 W2.1Q Virtual LAN, PRI: 0, DEI internet Protocol Version 4, Src incapsulating inal_test_3b_t5.jp File Edit View (1) 0 66 0e 9 0 8 00 9 1 50 1 5	1 192.168.255.254 7 192.168.255.254 8 192.168.255.254 8 192.168.255.254 8 192.166.05:94:d3:a0:21 10:160:00:194:d3:a0:21 10:1001 10:1001 10:1001 10:1002 10:1000 10:100 10:100 10:100 10:100 10:1000 10:1000 100	192.168.8.25 192.168.8.25 192.168.8.25 192.168.8.25 ured (1232 bit), Dst: 66:0e: : 192.168.8.25	4 ESP 4 ESP 4 ESP 4 FSP 4 FSP 5) 994:bc:80:4a (66:0	170 E 234 E 154 E 202 F	SP (SPI=0xc2 SP (SPI=0xc2 SP (SPI=0xca	c068a2) c068a2) 5ba1d8)	>
6 2022-05-03 13:46:33.298827 7 2022-05-03 13:46:33.357394 8 2022-05-03 13:46:36 255758 rame 1: 154 bytes on wire (123: thernet II, Src: 66:08:94:d3:a6 102:1Q Virtual LAN, PRI: 0, DEI: internet Protocol Version 4, Src incapsulating final_test_3b_tls_ip File Edit View (123: 0 66 0e 9	7 192.168.255.254 3 192.168.255.254 3 192.168.255.254 2 bits), 154 bytes capt 0:21 (66:0e:94:d3:a0:21 :0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapnc Go Capture Analyze Stat	192.168.8.25 192.168.8.25 192.168.8.25 ured (1232 bit), Dst: 66:0e: : 192.168.8.25	4 ESP 4 ESP 4 FCP 55) 994:bc:80:4a (66:0	234 E 154 E 202 F	SP (SPI=0xc2 SP (SPI=0xca	c068a2) 5ba1d8)	>
7 2022-05-03 13:46:33.357394 R 2022-05-03 13:46:36 255758 rame 1: 154 bytes on wire (123: thernet II, Src: 66:08:94:43:ad 02.1Q Virtual LAN, PRI: 0, DEI: nternet Protocol Version 4, Src ncapsulating final_test_3b_tls.jp File Edit View (0) 0 66 0e 9 0 8 00 0	<pre>192.168.255.254 192.168.255.254 2 bits), 154 bytes capt 0:21 (66:0e:94:d3:a0:21 : 0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapng Go Capture Analyze Stat</pre>	192.168.8.25 192.168.8.25 ured (1232 bit), Dst: 66:0e: : 192.168.8.25	4 ESP 4 FCP ts) :94:bc:80:4a (66:0	154 E 202 F	SP (SPI=0xca	5ba1d8)	>
R 2022-05-03 13-46-36 25575R rame 1: 154 bytes on wire (123) thernet II, Src: 66:0e:94:03:ad 02.10 Virtual LAN, PRI: 0, DEI nternet Protocol Version 4, Src ncapsulating final_test_3b_tls.jp File Edit View (0 0 66 0e 9 0 0 0 0	<pre>1 192 168 255 254 2 bits), 154 bytes capt 0 21 (66:0e:94:d3:a0:21 : 0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapng Go Capture Analyze Stat</pre>	192 168 8 25 ured (1232 bit), Dst: 66:0e: : 192.168.8.25	4 FCP (5) 94:bc:80:4a (66:6	202 F			>
thernet II, Src: 66:0e:94:d3:ad 02.1Q Virtual LAN, PRI: 0, DET Internet Protocol Version 4, Src ncapsulating final_test_3b_tts_ip File Edit View (0 66 0e 9 0 8 00 1 so	0:21 (66:0e:94:d3:a0:21 : 0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapno Go Capture Analyze Stat), Dst: 66:0e: : 192.168.8.25	94:bc:80:4a (66:0	0e:94:bc:80:4a)			>
thernet II, Src: 66:0e:94:d3:at i00.1Q Virtual LAN, PRI: 0, DET internet Protocol Version 4, Src incapsulating final_test_3b_tts_ip File Edit View (0 66 0e 9 0 8 00 0	0:21 (66:0e:94:d3:a0:21 : 0, ID: 1001 c: 192.168.255.254, Dst psec_testlaptop_050322.pcapno Go Capture Analyze Stat), Dst: 66:0e: : 192.168.8.25	94:bc:80:4a (66:0	0e:94:bc:80:4a)			
File Edit View (Go Capture Analyze Sta						
		tistics Telephony					
0 66 0e 9	📕 🖹 🖹 🎑 🔍 👄	usues reception,	y Wireless Tools	Help			
0 08 00 / esp		ا 🕰 主 🔶					
0 08 00 4 sep			• • •				
U TT TE UNA Tara							
0 77 2b b		Source	Destinati				
0 10 ec d	03 16:31:58.913502144	192.168.25		68.8.254 ESP		(SPI=0xc2c068a2)	
0 79 f8 0 89 2022-05-	03 16:31:58.913507428	192.168.25		8.8.254 ESP		(SPI=0xc2c068a2)	
	03 16:31:58.913524003	192.168.25		68.8.254 ESP		(SPI=0xc2c068a2)	
	03 16:31:58.913527815	192.168.25		8.8.254 ESP		(SPI=0xc2c068a2)	
0.00	03 16:31:58.913531489	192.168.25		8.8.254 ESP		(SPI=0xc2c068a2)	
	03 16:31:58.913535118	192.168.25		8.8.254 ESP		(SPI=0xc2c068a2)	
	03 16:31:58.913538501	192.168.25		8.8.254 ESP		(SPI=0xca5ba1d8)	
	03 16:31:58.913543857	192.168.25		8.8.254 ESP		(SPI=0xc2c068a2)	
V	03 16:31:58.913547442	192.168.25		8.8.254 ESP		(SPI=0xc2c068a2)	
111 37 2022 03	-03 16:31:58.913551047 -03 16:31:58.913554605	192.168.25 192.168.25		8.8.254 ESP 8.8.254 ESP		(SPI=0xc2c068a2) (SPI=0xc2c068a2)	
<	05 10.51.50.515554005	172.100.25	5.254 152.1	0.0.254 256	210 1.51	(511-0x02000002)	
0000 66 0e 9 0010 08 0 0020 ff f	H L LAN. PRT: 1. DET: 0. 94 bc 80 4a 66 0e final_test_3b_tls_ipsec_pluributer 7a 6a 6a	94 d3 a0 2	21 81 00 23 e9				
0030 0a f 0040 be 9 Fil	e Edit View Go Captu	ire Analyze St	atistics Telephony	Wireless Tools Help			
0050 aa 9 0060 3a 9	(🔳 🖉 🛞 📙 🛅 🎽	रे 🙆 🤇 🔶	• 🔿 😫 春 👱	् 📃 🔍 🔍 🔍			
0060 3a 9 0070 9f 2	esp						
0080 da 9				Destination	Dest 1	1	
0090 d0 f No.	Time 987 2022-05-03 16:31		ource 92.168.255.254	Destination 192,168,8,254	Protocol ESP	Lengti Info	
00a0 e3 c	987 2022-05-03 16:31 988 2022-05-03 16:31			192.168.8.254 192.168.8.254	ESP	424 ESP (SPI=0xc2c068a2) 216 ESP (SPI=0xc2c068a2)	
00b0 1c 2 00c0 8c 4	988 2022-05-03 16:31 989 2022-05-03 16:31		92.168.255.254 92.168.255.254	192.168.8.254	ESP		
0.72	989 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	200 ESP (SPI=0xc2c068a2) 264 ESP (SPI=0xc2c068a2)	
🔵 🍸 Encapsı	990 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	1208 ESP (SPI=0xC2C068a2)	
	991 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	1208 ESP (SPI=0xc2c068a2) 1208 ESP (SPI=0xc2c068a2)	
	993 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	440 ESP (SPI=0xc2c068a2)	
	994 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	1208 ESP (SPI=0xc2c068a2)	
	995 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	440 ESP (SPI=0xc2c068a2)	
	996 2022-05-03 16:31		92.168.255.254	192.168.8.254	ESP	1208 ESP (SPI=0xc2c068a2)	
	997 2022-05-03 16:31				ESP	440 ESP (SPI=0xc2c068a2)	
	998 2022-05-03 16:31			192.168.8.254	ESP	168 ESP (SPI=0xc2c068a2)	
	999 2022-05-03 16:31			192.168.8.254	ESP	1208 ESP (SPI=0xc2c068a2)	
	1000 2022-05-03 16:31			192.168.8.254	ESP	440 ESP (SPI=0xc2c068a2)	
<						:	
> > > > > > > > > > > > > > > > > > >		0e:94:bc:80:4a 5ion 4, Src: 1 1, Src Port: 4 31 Area Netwo 0e:94:bc:80:4a 5ion 4, Src: 1	(66:0e:94:bc:80: 28.8.46.80, Dst: 6255, Dst Port: 4 rk (66:0e:94:bc:80:	4a), Dst: Cisco_ff:f0 10.205.67.130 789 4a), Dst: 66:0e:94:d:	:68 (00:08:6		CF-9956

Figure 22: Capture of Modified and Injected TLS-Encrypted Packets on Untrusted Link and Capture of Packets on Outgoing Link to Core with IPsec Tunnel on Untrusted Link

TLP:WHITE:5GSTB

	test3B-MITRE-r6k-ipsec-050322-1630.pcap					- 🗆 ×
File	Edit View Go Capture Analyze	Statistics Telephony	Wireless Tools Help			
	🔲 🖉 🛞 📕 🗋 🕱 🗳 🔍	← ⇒ 🖺 🛧 👱		**		
A	Apply a display filter <ctrl-></ctrl->					→ +
No.	Time	Source	Destination	Protocol	Lengtl Info	^
	31 2022-05-03 16:30:54.734866	192.168.255.254	192.168.8.254	ESP	1162 ESP (SPI=0xc2c068a2)	
	32 2022-05-03 16:30:54.734880	192.168.255.254	192.168.8.254	ESP	394 ESP (SPI=0xc2c068a2)	
	33 2022-05-03 16:30:54.734881	192.168.255.254	192.168.8.254	ESP	1162 ESP (SPI=0xc2c068a2)	
	34 2022-05-03 16:30:54.734883	192.168.255.254	192.168.8.254	ESP	394 ESP (SPI=0xc2c068a2)	
	35 2022-05-03 16:30:54.734912	192.168.255.254	192.168.8.254	ESP	1162 ESP (SPI=0xc2c068a2)	
	36 2022-05-03 16:30:54.734914	192.168.255.254	192.168.8.254	ESP	394 ESP (SPI=0xc2c068a2)	
	37 2022-05-03 16:30:54.734916	192.168.255.254	192.168.8.254	ESP	1162 ESP (SPI=0xc2c068a2)	
	38 2022-05-03 16:30:54.734935	192.168.255.254	192.168.8.254	ESP	394 ESP (SPI=0xc2c068a2)	
	39 2022-05-03 16:30:54.734936	192.168.255.254	192.168.8.254	ESP	1162 ESP (SPI=0xc2c068a2)	×
<						>
>	Frame 1: 122 bytes on wire (976 b	its), 122 bytes capt	ured (976 bits)			
	Ethernet II, Src: Ericsson_85:91:			3:a0:21 (66:0e:94:d3:a0:2	1)	
>	802.1Q Virtual LAN, PRI: 0, DEI:	0, ID: 31				
	Internet Protocol Version 4, Src:	192.168.8.254, Dst	192.168.255.254			
v	Encapsulating Security Payload					
	ESP SPI: 0xc311e47c (32727297)	24)				
	ESP Sequence: 32					
	d test3B-MITRE-r6k-clear-050322-1630.p	cap				- □ >
	File Edit View Go Capture Ana	lyze statistics lelepho				
00	/ I (O) I I X (I	🍳 🍋 🔿 🖭 🏹	🔸 📃 📃 🔍 Q			
		• • • = •				
	tis					
00 00		Source	Destination	Protocol	Lengti Info	
00	No. Time				Lengt Info 163 Application Data	X 🔿 🔹
00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805	718 172.18.0.3 806 172.18.0.3	Destination	Protocol GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data	
00 00 00 00	No. Time 4 2022-05-03 16:31:03.089	718 172.18.0.3 806 172.18.0.3	Destination 20.49.99.108	Protocol GTP <tlsv1.2></tlsv1.2>	163 Application Data	X 🗔 🔹
00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805	718 172.18.0.3 806 172.18.0.3	Destination 20.49.99.108 20.49.99.108	Protocol GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data	X 🗔 🔻
00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805	718 172.18.0.3 806 172.18.0.3	Destination 20.49.99.108 20.49.99.108	Protocol GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data	X 🗆 🔹
00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805	718 172.18.0.3 806 172.18.0.3	Destination 20.49.99.108 20.49.99.108	Protocol GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data	X 🗔 🔹
00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805	718 172.18.0.3 806 172.18.0.3	Destination 20.49.99.108 20.49.99.108	Protocol GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data	X 💷 +) .
00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 <	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108	Destination 20.49.99.108 20.49.99.108 172.18.0.3	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data	× • •
00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 > Frame 4: 163 bytes on wire (1)	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108	Destination 20.49.99.108 20.49.99.108 172.18.0.3	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> S)</tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data 163 Application Data	× • •
00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108	Destination 20.49.99.108 20.49.99.108 172.18.0.3	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> S)</tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data 163 Application Data	
00 00 00 00 00 20 20 20 20 20 20 20 20 2	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 > Frame 4: 163 bytes on wire (1) > Ethernet II, Src: Erisson_88 > > 802.1Q Virtual LAN, PRI: 0, C	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: :91:c9), Dst: fa:16:	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> s) 3e:7a:b7:81 (fa:16:3e:7a:</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data 163 Application Data	× • •
00 00 00 00 00 00 00 00 00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 4 2022-05-03 16:31:17.812 5 Prame 4: 163 bytes on wire (1) 5 Ethernet II, Src: Ericsson_85 802.1Q Virtual LAN, PRI: 0, C	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 304 bits), 163 byte: :91:c9 (98:7a:10:85 EEI: 0, ID: 3704 5rc: 192.168.255.211	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit; 91:c9), Dst: fa:16: 0, Dst: 192.168.8.10	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> s) 3e:7a:b7:81 (fa:16:3e:7a:</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data 163 Application Data	× • •
00 00 00 00 00 00 00 00 00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 > Frhemet II, Src: Ericsson 85 > 802.1Q Virtual LAN, PRI: 0, C > Internet Protocol Version 4,	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 304 bits), 163 byte: :91:c9 (98:7a:10:85 EEI: 0, ID: 3704 5rc: 192.168.255.211	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit; 91:c9), Dst: fa:16: 0, Dst: 192.168.8.10	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> s) 3e:7a:b7:81 (fa:16:3e:7a:</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data 163 Application Data	
00 00 00 00 00 00 00 00 00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 > Ethernet II, Src: Ericsson_85 802.10 Virtual LAN, PRI: 0, D > Internet Protocol Version 4, > User Datagram Protocol, Src F > GPRS Tunneling Protocol > Internet Protocol Version 4,	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 1304 bits), 163 byte: 5:91:c9 (98:7a:10:85 DEI: 0, ID: 3704 Src: 192.168.255.210 Port: 2152, Dst Port	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: 91:c9), Dst: fa:16:: 0, Dst: 192.168.8.104 : 2152	Protocol GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> GTP <tlsv1.2> s) 3e:7a:b7:81 (fa:16:3e:7a:</tlsv1.2></tlsv1.2></tlsv1.2></tlsv1.2>	163 Application Data 163 Application Data 163 Application Data	× • •
00 00 00 00 00 00 00 00 00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 Ethernet II, Src: Ericsson_85 8 802.1Q Virtual LAN, PRI: 0, D Internet Protocol Version 4, User Datagram Protocol, Src F 6 GPRS Tunneling Protocol Internet Protocol Version 4, Transmission Control Protocol	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 5:91:c9 (98:7a:10:85 5:17.0 JD: 3704 5rc: 192.168.255.210 ort: 2152, Dst Port 5rc: 172.18.0.3, Ds	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: :91:c9), Dst: fa:16: 3, Dst: 192.168.8.104 : 2152 :: 20.49.99.108	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	× • •
00 00 00 00 00 00 00 00 00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 × Frame 4: 163 bytes on wire (1 × Ethernet II, Src: Ericsson_85 > 802.1Q Virtual LAN, PRI: 0, D > Internet Protocol Version 4, > User Datagram Protocol, Src F > GPRS Tunneling Protocol > Internet Protocol Version 4, > Transpission Control Protocol Yransport Layer Security	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 315 20.49.99.108 315 20.49.99.108 515 20.49.99.108 515 20.49.99.108 515 20.49.91.08 515 20.49.51.08 515 20.49.55.21 515 20.55.21 515 20.55.21 515 20.55.21 515	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: 91:c9), Dst: fa:16: 3, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Dst Port: 443, Seq: :	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
00 00 00 00 00 00 00 00 00 00 00 00 00	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 315 20.49.99.108 315 20.49.99.108 315 20.49.99.108 511:09 (98:7a:10:85 511:09 (98:7a:10:85)	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: 91:c9), Dst: fa:16: 3, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Dst Port: 443, Seq: :	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
2 File 2 File	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 > Ethernet II, Src: Ericsson_85 802.10 Virtual LAN, PRI: 0, D > Internet Protocol Version 4, > User Datagram Protocol, Src F > GPRS Tunneling Protocol > Internet Protocol Version 4, > Transmission Control Protocol Y Tasport Layer Security Y TLSV1.2 Record Layer: App Content Type: Applicat	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 511:0, ID: 3704 5rc: 192.168.255.210 Port: 2152, Dst Port 5rc: 172.18.0.3, Ds ⁻ 1, Src Port: 60855, I 11cation Data Protoction Data (23)	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: 91:c9), Dst: fa:16: 3, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Dst Port: 443, Seq: :	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
00 00 00 00 00 00 00 00 00 00 00 00 00	<pre>No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 </pre> Frame 4: 163 bytes on wire (1 5 Ethernet II, Src: Ericsson_85 802.1Q Virtual LAN, PRI: 0, D Internet Protocol Version 4, User Datagram Protocol, Src F 6 GPRS Tunneling Protocol Internet Protocol Version 4, Transmission Control Protocol Transport Layer Security	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 511:0, ID: 3704 5rc: 192.168.255.210 Port: 2152, Dst Port 5rc: 172.18.0.3, Ds ⁻ 1, Src Port: 60855, I 11cation Data Protoction Data (23)	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: 91:c9), Dst: fa:16: 3, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Dst Port: 443, Seq: :	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
90 90 90 90 90 90 90 90 90 90 90 90 90 9	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812	718 172.18.0.3 806 172.18.0.3 315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 3315 20.49.99.108 511:0, ID: 3704 5rc: 192.168.255.210 Port: 2152, Dst Port 5rc: 172.18.0.3, Ds ⁻ 1, Src Port: 60855, I 11cation Data Protoction Data (23)	Destination 20.49.99.108 20.49.99.108 172.18.0.3 s captured (1304 bit: 91:c9), Dst: fa:16: 3, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Dst Port: 443, Seq: :	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
2 File 2 File	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812	718 172.18.0.3 806 172.18.0.3 815 20.49.99.108 1304 bits), 163 byte: 5:91:29 (98:7a:10:85 12: 0 (98:7a:10:85 12: 0 (98:7a:10:85 12: 0 (98:7a:10:85 12: 0 (98:7a:10:85), 12 12:	Destination 20.49.99.108 20.49.99.108 20.49.99.108 172.18.0.3 5 captured (1304 bit: :91:c9), Dst: fa:16: 3, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Jost Port: 443, Seq: : ol: http-over-tls c9 81 00 0e 78	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
2 File 2 File	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 > Ethernet II, Src: Ericsson.85 802.1Q Virtual LAN, PRI: 0, C > Internet Protocol Version 4, > User Datagram Protocol, Src F > GPRS Tunneling Protocol > Internet Protocol Version 4, > Transmission Control Protocol > TISV1.2 Record Layer: App Content Type: Applicat Version: TLS 1.2 (0x0) Length: 64 0000 fa 16 3e 7a b7 81 9 0010 08 00 45 38 00 91	718 172.18.0.3 806 172.18.0.3 806 172.18.0.3 315 20.49.99.108 1394 bits), 163 byte: 5:91:09 (98:7a:10:85 EI: 0, ID: 3704 Src: 192.168.255.210 Port: 2152, Dst Port Src: 172.18.0.3, Ds' 1, Src Port: 60855, I lication Data Protoc tion Data (23) 303) 208 7a 10 85 91 3e ae 00 00 fe	Destination 20.49.99.108 20.49.99.108 20.49.99.108 172.18.0.3 5 captured (1304 bit: :91:c9), Dst: fa:16: 0, Dst: 192.168.8.104 : 2152 1: 20.49.99.108 Dst Port: 443, Seq: 3 ol: http-over-tls c9 81 00 0e 78 11 f3 e9 c0 a8	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
2 File 2 File	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 > Ethernet II, Src: Ericsson_85 802.10 Virtual LAN, PRI: 0, D > Internet Protocol Version 4, Version 1, Sc > Bdagram Protocol, Src F 6PRS Tunneling Protocol Sc > Internet Protocol Version 4, Transmission Control Protocol > Internet Protocol Version 4, Transport Layer Security TLSV1.2 Record Layer: App Content Type: Applicat Version: TLS 1.2 (9x00) Length: 64 00000 fa 16 38 78 90 0010 02 04 45 38 80 91 0020 ff d2 20 8 8 68 68	718 172.18.0.3 806 172.18.0.3 806 172.18.0.3 815 20.49.99.108 8315 20.49.99.108 8315 20.49.99.108 8315 20.49.99.108 8315 20.49.99.108 8376 JU 3704 8376 JU 3704 8376 JU 3704 8376 JU 3704 8376 JU 3704 8376 JU 3704 8376 JU 375 JU 8376 JU 83	Destination 20.49.99.108 20.49.99.108 20.49.99.108 172.18.0.3 5 captured (1304 bit: 91:c9), Dst: fa:16: 9, Dst: 192.168.8.10 : 2152 :: 20.49.99.108 Jot Port: 443, Seq: : ol: http-over-tls c9 81 00 00 78 11 f3 e9 c0 a8 7d a9 b7 30 ff	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	
2 File 2 File	No. Time 4 2022-05-03 16:31:03.089 25 2022-05-03 16:31:17.805 26 2022-05-03 16:31:17.812 Frame 4: 163 bytes on wire (1 > Ethernet II, Src: Ericsson.85 802.1Q Virtual LAN, PRI: 0, C > Internet Protocol Version 4, > User Datagram Protocol, Src F > GPRS Tunneling Protocol > Internet Protocol Version 4, > Transmission Control Protocol > TISV1.2 Record Layer: App Content Type: Applicat Version: TLS 1.2 (0x0) Length: 64 0000 fa 16 3e 7a b7 81 9 0010 08 00 45 38 00 91	718 172.18.0.3 806 172.18.0.3 806 172.18.0.3 315 20.49.99.108 304 bits), 163 byte: 5:91:29 (98:7a:10:85 EI: 0, ID: 3704 Src: 192.168.255.21 Vort: 2152, Dst Port Src: 172.18.0.3, Ds 1, Src Port: 60855, I lication Data Protoc tion Data (23) 303) 28 7a 10 85 91 3e ae 00 00 fe 28 68 08 68 00 15 00 00 6d 5b	Destination 20.49.99.108 20.49.99.108 20.49.99.108 172.18.0.3 5 captured (1304 bit: :91:c9), Dst: fa:16: 0, Dst: 192.168.8.104 : 2152 1: 20.49.99.108 Dst Port: 443, Seq: 3 ol: http-over-tls c9 81 00 0e 78 11 f3 e9 c0 a8	Protocol GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> GTP <tl5v1.2> 3) 3e:7a:b7:81 (fa:16:3e:7a: 4</tl5v1.2></tl5v1.2></tl5v1.2></tl5v1.2>	163 Application Data 163 Application Data 163 Application Data	

Figure 23: Captures of TLS-Encrypted Packets on Core-Side Untrusted Link and On Trusted Router After Decryption of IPsec

			00100	/				
	inal_test_3b_tls_ipsec_R6K_050322.pcapng					-		\times
File	Edit View Go Capture Analyze Sta	atistics Telephony W	ireless Tools Help					
	I 🖉 🐵 📕 🗎 🕱 🙆 🗣 👄 🗄	🗵 😱 🗶 📃 📃 🛛						
tis							\times	+
No.	Time	Source	Destination	Protocol	Lengt Info			
	29 2022-05-03 16:31:06.064418	172.18.0.3	20.49.99.108	GTP <tlsv1.2></tlsv1.2>	159 Application Data			
	81 2022-05-03 16:31:20.779081	172.18.0.3	20.49.99.108	GTP <tlsv1.2></tlsv1.2>	159 Application Data			
	82 2022-05-03 16:31:20.789250	20.49.99.108	172.18.0.3	GTP <tlsv1.2></tlsv1.2>	159 Application Data			
<								
> U > G > I > T > T	<pre>nternet Protocol Version 4, Src: ser Datagram Protocol, Src Port: PRS Tunneling Protocol nternet Protocol Version 4, Src: ransport Layer Security / TLSV1.2 Record Layer: Applicat Content Type: Application D Version: TLS 1.2 (0x0303) Length: 64</pre>	: 2152, Dst Port: : 172.18.0.3, Dst: rc Port: 60855, Ds :ion Data Protocol	2152 20.49.99.108 t Port: 443, Seq:					
000 001 002	0 08 68 08 68 08 68 00 7d a9 b	9 c0 a8 ff d2 c0 7 30 ff 00 6d 54	a8≻ a5 -h-h-h-}0-	- mT -				
0					Packets: 105 · Displayed: 3 (2.9%)	Pi	ofile: STB I	Profile

Figure 24: Capture of TLS-Encrypted Packets on RAN-Side Router Ingress Showing the Only Traffic Generated/Received by the UE for This Test with IPsec Tunnel

Test Result

Success: TLS-encrypted traffic is unreadable with or without IPsec encryption; this includes all capture points, not just those on the untrusted link. Adding IPsec to the untrusted link further obscures the traffic, preventing an eavesdropper from reading the source and destination of the TLS messages, as well as knowing that the encapsulated packets are TLS encrypted. In addition, TLS encryption and IPsec encryption prevent injection or modification of packets. Whereas, without the IPsec tunnel, injected TLS packets pass out of the cellular network to be dropped by either the UE or the HTTPS server, when the IPsec tunnel is enabled, that injected traffic is dropped at the tunnel endpoints and not allowed to flow to other parts of the larger network.

Conclusions and Next Steps

For each of the three test cases described here, the tests successfully verified the efficacy of employing security procedures recommended by the CSRIC VII WG2 report, implementing commercial hardware in a commercially-relevant NSA configuration. This verification of the CSRIC NSA recommendations in a commercially-deployed environment is the first of its kind. Test Cases 1 and 2 focused on confidentiality and integrity on an untrusted backhaul link for user traffic and control traffic, respectively. Test Case 3 added end-to-end TLS encryption between an application on the UE and a server on the internet.

Test Case 1 demonstrated that implementation of an IPsec tunnel over the untrusted link prevents eavesdropping on user traffic as well as modification and injection of false traffic designed to appear as originating from or destined to a valid UE. All traffic on the untrusted link

appeared as encrypted ESP packets with no ability to read the contents. Modified and injected packets were observed at test points on the untrusted link, but were dropped inside the tunnel and did not reach either the UE or the internet. Furthermore, in absence of that IPsec tunnel, packet contents and headers were fully decipherable, and modified and injected UP packets were able to reach destinations outside the untrusted link, including the UE and the internet.

Test Case 2 demonstrated that implementation of an IPsec tunnel over the untrusted link prevents eavesdropping on control traffic as well as modification and injection of false traffic designed to appear as originating from the UE, RAN, or MME. As with Test Case 1, all traffic on the untrusted link appeared as encrypted ESP packets with no ability to read the contents. Modified and injected packets were observed at test points on the untrusted link, but were dropped inside the tunnel and did not reach either the UE, RAN, or the MME. Furthermore, in absence of that IPsec tunnel, packet contents and headers were fully decipherable. While modified and injected CP packets were able to reach destinations outside the untrusted link, including the RAN and the MME, that traffic also generated ABORT messages, suggesting that other protocols within the system identified the injected packets as problematic. The exact cause of those ABORT messages was not investigated.

Test Case 3 demonstrated that end-to-end TLS encryption further occludes user traffic between the UE and a server, or other endpoint. The TLS encryption prevented eavesdropping and modification and injection of packets, regardless of the implementation of an IPsec tunnel on the untrusted link, although that protection only exists for the user traffic that is sent between the addresses that set up the encrypted connection. The TLS encryption also protects the associated traffic at points outside the untrusted link, including what is transmitted over the air between the UE and the RAN.

The three successful test cases outlined above conclude the inaugural tests of the 5G Security Test Bed, an industry effort to improve 5G network security through collaboration with government agencies, policymakers, international standards bodies, thought leaders, and partners. While these tests focused on a 5G non-standalone network architecture, with the 5G network built over a 4G LTE core, future steps include implementation and testing of CSRIC VII WG2 recommendations for a 5G standalone configuration, utilizing an Ericsson Release 16 Dual Mode Core. The 5G STB is also in the process of developing test cases for network slicing and roaming security use cases. In addition, the method the 5G STB uses for IPsec tunneling will be modified to utilize PKI certificates.

The 5G STB members and administrator welcome engagement from stakeholders with an interest in the mission of the 5G Security, and we expect new participants and the diversity of test cases to grow in tandem.

Appendix: Acronyms

3GPP	3rd Generation Partnership Project
5G STB	5G Security Test Bed
BBU	Baseband Unit
СР	Control Plane
CPE	Customer Premise Equipment
CSRIC	Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
eNB/eNodeB	Evolved Node B
EN-DC	E-UTRA New Radio – Dual Connectivity
EPG	Evolved Packet Gateway
ESP	Encapsulating Security Payload
E-UTRA	Evolved Universal Mobile Telecommunications System (UMTS)
	Terrestrial Radio Access
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
gNB/gNodeB	Next Generation Node B
HSS	Home Subscriber Server
IKEv2	Internet Key Exchange Protocol Version 2
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol Security
LTE	Long Term Evolution
MACsec	Media Access Control Security
MME	Mobility Management Entity
NIST	National Institute of Standards and Technology
NMS	Network Management System
NR	New Radio
PGW	Packet Data Network Gateway
RAN	Radio Access Network
RAT	Radio Access Technology
SEG	Security Gateway
SGW	Serving Gateway
STB	Security Test Bed
TAS	Telecom Application Server
TDD	Time Division Duplex
TLS	Transport Layer Security
ТР	Test Point

UE	User Equipment	
UMD	University of Maryland	
UP	User Plane	
UPF	User Plane Function	
VPN	Virtual Private Network	
WG	Working Group	

References

Communications Security, Reliability, and Interoperability Council (CSRIC) VII Working Group 2 (WG2), Report on Review and Recommendations on Optional Security Features in 3GPP Standards Impacting 5G Non-Standalone Architecture (Dec. 2020), https://www.fcc.gov/file/20181/download.

CSRIC VII WG3, Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards (Sept. 16, 2020), https://www.fcc.gov/file/19297/download.

CSRIC V WG6, Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network, (Sept. 2016). https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG6_Final_091416.docx.

Jon Metzler, Security Implications of 5G Networks, UC Berkeley Center for Long-Term Cybersecurity at 7 (Sept. 2020), https://cltc.berkeley.edu/wpcontent/uploads/2020/09/Security_Implications_5G.pdf.

IETF Datatracker, Request for Comment (RFC) 4303 (Dec. 2005), https://datatracker.ietf.org/doc/html/rfc4303.

3GPP Portal, Technical Specification (TS) 33.210 (last updated Dec. 23, 2021), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationI d=2279.

3GPP Portal, TS 33.310 (last updated Mar. 24, 2022), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationI d=2293.

3GPP Portal, TS 33.401 (last updated Mar. 24, 2022), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationI d=2296.

3GPP Portal, TS 33.501 (last updated Mar. 24, 2022), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationI d=3169.