Betrieb: exceeding solutions GmbH

Betreuer: M. Eng. Niklas Rack

Semester: WS 2024/25

Prüfer: Prof. Dr. Uwe Heuert

Masterarbeit

Entwicklung eines automatisierten Testsystems für 5G-Sicherheitstestfälle, inklusive Aufbau und Erprobung eines 5G-Campusnetzes

Seyed Khashayar Valadi Someh Saraei

05.03.2025

Fachbereich: INW

Studiengang: Automatisierungstechnik und Informatik

Abstract

Diese Masterarbeit befasst sich mit der Entwicklung eines automatisierten Testsystems zur Überprüfung sicherheitsrelevanter Funktionen in 5G-Netzwerken. Ziel war es, eine realitätsnahe und flexible Testumgebung auf Basis eines privaten 5G-Netzes zu schaffen. Hierfür wurden Open-Source-Komponenten wie Open5GS und srsRAN sowie Hardware wie der USRP B210 verwendet. Das Testsystem ermöglicht sowohl generische Sicherheitsprüfungen als auch spezifische Tests für zentrale 5G-Netzfunktionen wie AMF und SMF. Durch die Integration von Robot Framework, Wireshark und weiteren Tools konnten Testfälle effizient automatisiert und ausgewertet werden. Die Ergebnisse zeigen, dass das System potenzielle Schwachstellen zuverlässig identifiziert und somit einen wertvollen Beitrag zur Verbesserung der Netzwerksicherheit in 5G-Umgebungen leistet.

Schlagwörter

5G, Netzwerksicherheit, Testautomatisierung, Robot Framework, Open5GS, srsRAN, AMF, SMF, USRP B210, private 5G-Netzwerke, 3GPP-Testfälle

Danksagung

Ich möchte an dieser Stelle allen danken, die mich während der Erstellung meiner Masterarbeit unterstützt haben, insbesondere exceeding solutions, die mir diese Möglichkeit gegeben und mich während der gesamten Arbeit begleitet haben.

Mein besonderer Dank gilt Herrn Professor Uwe Heuert für das entgegengebrachte Vertrauen, mir dieses spannende Thema als Masterarbeit zu ermöglichen. Ebenso danke ich meinem ersten Betreuer, Niklas Rack, und meinem zweiten Betreuer, Kevin Saalmann, für ihre wertvolle Unterstützung, ihr Fachwissen und ihre hilfreichen Ratschläge, die wesentlich zum Gelingen dieser Arbeit beigetragen haben.

Ein herzliches Dankeschön geht auch an meine Familie für ihre beständige Unterstützung und Ermutigung während meines gesamten Studiums. Besonders möchte ich meiner Freundin Sephora danken, die mir beim Formatieren der Arbeit mit so viel Geduld und Engagement geholfen hat.

Ohne euch alle wäre diese Arbeit in dieser Form nicht möglich gewesen.

Vielen Dank!

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Mit der Einführung des 5G-Mobilfunkstandards vollzieht die Telekommunikationsbranche einen tiefgreifenden Wandel, der weit über die bloße Erhöhung von Datenraten und Netzwerkkapazitäten hinausgeht. Die Entwicklung und Prüfung von 5G-Netzwerken erfordern innovative Testsysteme, die eine präzise und automatisierte Überprüfung von Sicherheits- und Funktionsanforderungen ermöglichen. Ziel dieser Arbeit ist es, ein umfassendes Testsystem zu entwickeln, das die Überprüfung der Netzwerksicherheit und -integrität effizient und wiederholbar gestaltet.

Im Rahmen dieses Testsystems wurde ein privates 5G-Netzwerk aufgebaut, das als integraler Bestandteil der Testumgebung dient. Dieses Netzwerk wurde im Rahmen eines gemeinsamen Projekts zwischen der exceeding solutions GmbH und TÜVIT entwickelt und ermöglicht es, die im Testsystem definierten Anforderungen realitätsnah zu testen. Open-Source-Lösungen wie Open5GS und srsRAN sowie Hardwarekomponenten wie das USRP B210 und eine maßgeschneiderte Antennenkonfiguration bilden die technische Basis des Netzwerks.

Das Testsystem basiert auf den Vorgaben des 3GPP-Testkatalogs und umfasst sowohl generische Sicherheitsprüfungen als auch spezifische Testfälle für zentrale Netzwerkfunktionen wie AMF (Access and Mobility Management Function) und SMF (Session Management Function). Diese Komponenten sind entscheidend für die Architektur eines 5G-Kernnetzes und werden durch das Testsystem auf ihre Sicherheit und Funktionalität geprüft. Die Automatisierung der Testfälle erfolgte mithilfe des Robot Framework, einer leistungsstarken Testautomatisierungsplattform, die speziell für systematische und nachvollziehbare Testprozeduren entwickelt wurde.

Durch die Integration des privaten 5G-Netzwerks in das Testsystem wird sichergestellt, dass die entwickelten Testfälle in einer kontrollierten und flexiblen Umgebung durchgeführt werden können. Das Netzwerk unterstützt die Simulation realer 5G-Anwendungsfälle, ohne von den Einschränkungen öffentlicher Netzbetreiber abhängig zu sein, und bietet so optimale Voraussetzungen für die erfolgreiche Durchführung der Tests.

Im Verlauf der Arbeit wird zunächst auf die theoretischen Grundlagen von 5G eingegangen, einschließlich der Technologiekomponenten und der relevanten Standards. Anschließend wird der Aufbau des privaten 5G-Netzwerks beschrieben, gefolgt von der detaillierten Implementierung der Testautomatisierung. Der Schwerpunkt liegt auf der Entwicklung von automatisierten Testfällen für sicherheitskritische Szenarien sowie für die Überprüfung der ordnungsgemäßen Funktion der AMF und SMF-Komponenten. Die abschließende Analyse der Testergebnisse zeigt, inwieweit das entwickelte System den Anforderungen der Projektpartner gerecht wird und welche Verbesserungsmöglichkeiten sich für zukünftige Projekte ergeben.

Durch diese Arbeit wird nicht nur ein funktionierendes privates 5G-Netzwerk als Teil des Testsystems implementiert, sondern auch eine Testumgebung geschaffen, die es ermöglicht, die Netzwerksicherheit und Leistung kontinuierlich zu überwachen und zu optimieren. Dabei wird besonderer Wert auf die Einhaltung eines einheitlichen Standards für 5G-Software- und Hardwarekomponenten gelegt, um Interoperabilität und Zuverlässigkeit sicherzustellen. Die Automatisierung der Testfälle trägt wesentlich dazu bei, den Testprozess effizienter zu gestalten und gleichzeitig die Qualität und Konsistenz der Testergebnisse zu gewährleisten. Die gewonnenen Erkenntnisse und Ergebnisse bieten wertvolle Einblicke in die Herausforderungen und Potenziale bei der Implementierung privater 5G-Netzwerke und der Testautomatisierung im industriellen Kontext.

2. Grundlagen und Stand der Technik
2.1 Überblick über 5G-Technologien
2.1.1 Entwicklung von Mobilfunkgenerationen

Die erste Generation der Mobilfunktechnologie, auch bekannt als 1G, bezieht sich auf die frühen analogen Mobilfunkstandards. Das erste kommerzielle 1G-Netz wurde 1979 in Japan von NTT eingeführt. In Europa und den USA folgte die Einführung in den Jahren 1981/1982 mit Systemen wie dem Nordic Mobile Telephone (NMT) und dem Advanced Mobile Phone System (AMPS). Diese Systeme waren bis zur Ablösung durch die digitale Mobilfunktechnologie der zweiten Generation (2G) in Betrieb. Der wesentliche Unterschied zwischen 1G und 2G besteht darin, dass bei 1G-Netzen die Audiosignale in Form von analogen Funksignalen übertragen wurden, während 2G-Netzwerke eine vollständige Digitalisierung der Sprachübertragung sowie der Kommunikation innerhalb des Netzwerks ermöglichten.

Die Mobilfunktechnologie der zweiten Generation (2G) bietet im Vergleich zu ihren Vorgängern drei wesentliche Vorteile. Erstens werden Telefongespräche digital verschlüsselt, was eine höhere Sicherheit gewährleistet. Zweitens nutzen 2G-Systeme das Frequenzspektrum deutlich effizienter, was zu einer wesentlich höheren Verbreitung von Mobiltelefonen führte. Drittens ermöglichte 2G die Einführung von Datendiensten für Mobilgeräte, beginnend mit dem Kurzmitteilungsdienst (SMS) für textbasierte Nachrichten. Diese Technologie schuf die Grundlage für weitere Dienste wie Bildnachrichten und den Multimedia Messaging Service (MMS). Zu den drei Hauptdiensten von 2G gehört der Trägerdienst, auch bekannt als Datendienst, der die Grundlage für die mobile Kommunikation darstellt.[1]

Die Mobilfunktechnologie der dritten Generation (3G) bietet eine Datenübertragungsrate von mindestens 144 kbit/s. Spätere Versionen von 3G, die häufig als 3.5G und 3.75G bezeichnet werden, ermöglichen zudem mobilen Breitbandzugang mit mehreren Mbits für Smartphones und mobile Modems in Laptops. Dadurch eignet sich 3G für drahtlose Sprachtelefonie, mobilen Internetzugang, festen drahtlosen Internetzugang, Videoanrufe und mobile TV-Dienste. Seit der Einführung der 1G-Systeme ab 1979 erscheint etwa alle zehn Jahre eine neue Mobilfunkgeneration. Jede dieser Generationen zeichnet sich durch neue Frequenzbänder, höhere Datenraten und nicht abwärtskompatible

Übertragungstechnologien aus. Die ersten 3G-Netze wurden im Jahr 1998 eingeführt.[2]

Die Mobilfunktechnologie der vierten Generation (4G) erweitert die Möglichkeiten der 3G-Technologie um mobilen Breitbandzugang, der Laptops mit drahtlosen Modems, Smartphones und andere mobile Geräte unterstützt. Zu den potenziellen und bereits genutzten Anwendungen gehören erweiterter mobiler Webzugang, IP-Telefonie, Gaming-Dienste, hochauflösendes mobiles Fernsehen, Videokonferenzen, 3D-Fernsehen und Cloud-Computing.
LTE (Long Term Evolution), das häufig als 4G LTE vermarktet wird, erfüllte anfangs nicht vollständig die technischen Anforderungen eines 4G-Dienstes, wie sie in den 3GPP-Dokumenten der Releases 8 und 9 für LTE Advanced festgelegt sind. Aufgrund des Wettbewerbsdrucks durch WiMAX und dessen Weiterentwicklung mit neuen Advanced-Versionen hat sich LTE jedoch als Synonym für 4G etabliert. Die erste kommerzielle Einführung von LTE erfolgte 2009 in Norwegen und Stockholm, während Verizon 2011 in den USA LTE im neu erworbenen 700-MHz-Frequenzband einführte.

5G stellt eine bedeutende Weiterentwicklung der Mobilfunkstandards dar und geht weit über die 4G/IMT (international Mobile Telecommunications) -Advanced-Standards hinaus. Es basiert auf drei zentralen Eckpfeilern. eMBB (Enhanced Mobile Broadband), URLLC (Ultra-Reliable Low Latency Communication) und mMTC (Massive Machine-Type Communication). Diese Säulen bilden die Grundlage für die vielfältigen Einsatzmöglichkeiten und die technischen Fortschritte von 5G-Netzwerken.
Die Next Generation Mobile Networks Alliance (NGMN) hat spezifische Anforderungen an 5G-Netzwerke definiert. Diese beinhalten die Unterstützung von Datenraten im Bereich von mehreren zehn Megabit pro Sekunde (Mbit/s) für zehntausende Nutzer sowie die Bereitstellung von 1 Gbit/s für gleichzeitig mehrere Dutzend Arbeiter auf derselben Bürofläche. Zudem sollen 5G-Netze Hunderttausende von Verbindungen gleichzeitig unterstützen können, um den Anforderungen massiver Sensornetze gerecht zu werden. Im Vergleich zu 4G soll die spektrale Effizienz erheblich gesteigert werden, die Netzabdeckung verbessert und die

Signalübertragung effizienter gestaltet werden. Darüber hinaus muss die Latenzzeit im Vergleich zu LTE deutlich verringert werden.

Die drei Eckpfeiler von 5G ermöglichen diese Fortschritte: eMBB sorgt für extrem hohe Datenraten und wird für Anwendungen wie hochauflösendes Video-Streaming oder Virtual Reality genutzt. URLLC gewährleistet extrem zuverlässige und latenzarme Verbindungen, die beispielsweise für autonome Fahrzeuge oder industrielle Automatisierung entscheidend sind. mMTC unterstützt die Verbindung einer enormen Anzahl von IoT-Geräten, wie Sensoren in intelligenten Städten oder Industrieanlagen. Die NGMN Alliance sieht die Einführung von 5G im Zeitraum 2021 bis 2023 als notwendig an, um die wachsenden Anforderungen von Unternehmen und Verbrauchern zu erfüllen. Neben höheren Übertragungsgeschwindigkeiten wird erwartet, dass 5G auch neue Anwendungsfälle wie das Internet der Dinge (IoT), Rundfunkdienste und lebenswichtige Kommunikationssysteme in Notfällen unterstützt. [2]

Generation	Vorteile	Nachteile
1G	Sprachkommunikation	Keine Datenfunktionen, begrenzte Netzabdeckung, schlechte Gesprächsqualität, anfällig für Störungen
2G	Verbesserte Sprachqualität, SMS-Nachrichten, Datenübertragungsraten bis zu 64 kbit/s, internationales Roaming, bessere Netzabdeckung	Eingeschränkte Datenfunktionen im Vergleich zu späteren Generationen
3G	Datenübertragungsraten von bis zu 2 Mbit/s, Zugang zum Internet und Streaming auf mobilen Geräten, bessere Gesprächsqualität, geringere Latenzzeiten	Ursprünglich für Sprache und SMS konzipiert, aber nicht für die Datenübertragung optimiert
4G	Datenübertragungsraten von bis zu 100 Mbit/s, verbesserte Anrufqualität, bessere Netzabdeckung, optimiert für Hochgeschwindigkeitsdatenübertragung	Eingeschränkte Verfügbarkeit in einigen Gebieten, erfordert neuere Geräte
5G	Datenübertragungsraten von bis zu 20 Gbit/s, geringere Latenzzeiten, bessere Netzabdeckung, verbesserte Anrufqualität, ermöglicht neue Technologien wie autonome Fahrzeuge und intelligente Städte	Eingeschränkte Verfügbarkeit in einigen Gebieten, erfordert neuere Geräte

Tabelle 1: Schlüsselkonzepte jeder Mobilfunkgeneration[2]

2.1.2 Architekturen und Kernkomponenten von 5G

Das mobile Kernnetz übernimmt wichtige Aufgaben wie Sitzungsmanagement, Mobilitätsverwaltung, Authentifizierung und Sicherheit. Diese Funktionen sind entscheidend für die Bereitstellung von Diensten. Die 5G-Systemarchitektur, die im Rahmen der 3GPP-Spezifikation TS 23.501 entwickelt wird, definiert zwei unterschiedliche Architekturen für das 5G-Kernnetz: eine servicebasierte und eine Punkt-zu-Punkt-basierte. Im ersten Fall kommunizieren servicebasierte Schnittstellen mit Steuerungsebenen, während bei der Punkt-zu-Punkt-Architektur die Benutzerebene über direkte Verbindungen angebunden wird.

Die Punkt-zu-Punkt-Architektur wurde bereits in 2G, 3G, 4G und jetzt auch in 5G eingesetzt. In diesem Modell sind die Netzwerkfunktionen über standardisierte Schnittstellen verbunden, was eine Integration von Komponenten unterschiedlicher Anbieter ermöglicht. Dieses Konzept hat sich über Jahrzehnte hinweg bewährt und wurde in der Praxis erfolgreich umgesetzt.

Mit dem Übergang zur Cloud-Infrastruktur und dem wachsenden Bedarf an höherer „Service-Agilität“ wird das Punkt-zu-Punkt-Modell jedoch nicht mehr als die optimale Lösung betrachtet. Für Betreiber, die 5G als eine Gelegenheit für transformative Veränderungen in Bezug auf Funktionalität und Kosten pro Datenbit sehen, erscheint die servicebasierte Architektur (SBA) weitaus attraktiver.

Die größte Herausforderung der P2P-Architektur besteht darin, dass sie zahlreiche einzigartige oder nahezu einzigartige Schnittstellen zwischen funktionalen Elementen erfordert, die miteinander verbunden sind. Diese komplexe Struktur von Verbindungen schafft Abhängigkeiten, die es erschweren, Änderungen in der Architektur vorzunehmen. Wenn eine neue Funktion eingeführt oder eine bestehende Funktion erweitert wird, müssen die Betreiber mehrere angrenzende Funktionen neu konfigurieren und die Konfiguration testen, bevor das System in Betrieb genommen werden kann. Diese Komplexität führt zu einer höheren Schwelle für Innovationen und erschwert die Einführung neuer Dienste.

Dieser Zustand wird oft als „Netzwerkversteifung“ bezeichnet. Dadurch wird der Markt, auf den die Betreiber zugreifen können, künstlich begrenzt, und die Netzwerkdienste bleiben statisch. Solche Einschränkungen mögen in einem einfachen Dienstangebot

(z. B. Sprachdienste oder Breitband) akzeptabel sein. Im 5G-Zeitalter, in dem Betreiber eine Vielzahl von Diensten anbieten und sich schnell ändernde Anforderungen bedienen müssen, ist jedoch eine flexiblere und dynamischere Architektur erforderlich.

Die SBA entkoppelt die Endnutzerdienste von der darunter liegenden Netzwerk- und Plattformstruktur. Dies ermöglicht sowohl funktionale als auch servicebezogene Flexibilität. Durch den Einsatz der SBA, die für den Betrieb in Cloud-Umgebungen ausgelegt ist, können die verschiedenen Funktionen zu einem End-to-End-Service über standardisierte Programmierschnittstellen (APIs) kombiniert werden. Auf diese Weise wird es für Netzbetreiber einfacher, virtuelle Netzwerkfunktionen (VNFs) hinzuzufügen, zu entfernen oder anzupassen, um auf die Anforderungen zu reagieren und auf Abruf neue servicespezifische Wege (Service-Agilität) zu erstellen.

In dieser Masterarbeit liegt der Fokus auf der servicebasierten Architektur (SBA), die speziell für das 5G-Kernnetz entwickelt wurde. Diese Architektur zeichnet sich durch ihre besondere Eignung für den Einsatz in Cloud-Umgebungen aus. Aufgrund ihrer cloudnativen Struktur wird die SBA als besser geeignet angesehen, um den aktuellen und zukünftigen Anforderungen moderner Netzwerkinfrastrukturen gerecht zu werden, die von führenden Netzbetreibern angestrebt werden. Angesichts dieser Eigenschaften stellt die SBA eine bevorzugte Lösung für den Aufbau und Betrieb von 5G-Kernnetzen dar.

Die Architektur von 5G-Netzwerken unterscheidet sich wesentlich von früheren Generationen. Sie basiert auf einer Service-orientierten Architektur, die eine flexible Bereitstellung von Diensten ermöglicht. Die Hauptkomponenten eines 5G-Netzwerks umfassen das Radio Access Network (RAN), das Core Network (CN) und die Edge-Computing-Infrastruktur. Das RAN besteht aus verschiedenen Basisstationen, die mit neuen Technologien wie Massive MIMO und Beamforming ausgestattet sind, um eine höhere Kapazität und Effizienz zu erreichen. Das Core Network wurde virtualisiert und nutzt Network Funktion Virtualization (NFV) und Software-Defined Networking (SDN), um eine flexible und skalierbare Netzwerkinfrastruktur zu gewährleisten. Edge-Computing ermöglicht die Verarbeitung von Daten näher am Endnutzer, was zu niedrigeren Latenzzeiten und einer besseren Leistung führt.[3]

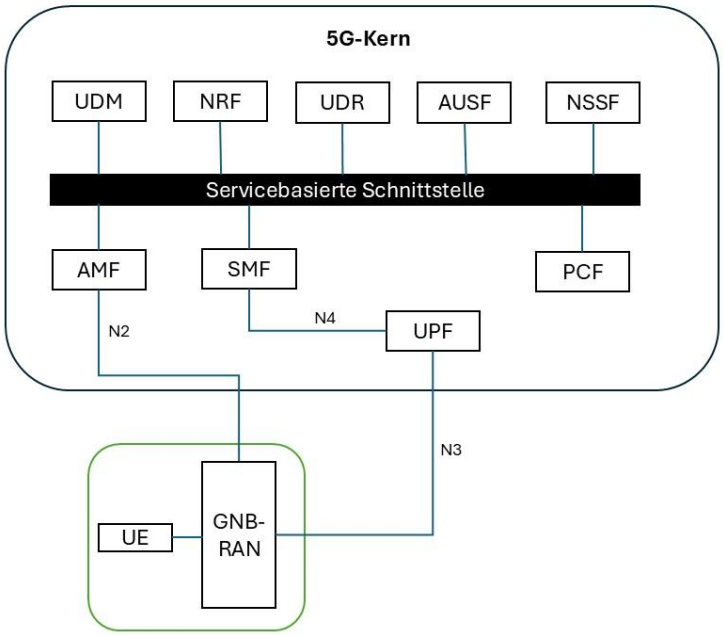

Abbildung 1: 5G-Kern und Netzwerkfunktionen[4]

2.1.3 Netzwerkfunktionen

Diese Abbildung 1 zeigt die Architektur des 5G-Kernnetzes (5GC) und dessen Hauptkomponenten sowie deren Interaktionen untereinander. Es stellt die wichtigsten Netzwerkfunktionen (NF) dar, die in der 5G-Architektur über eine servicebasierte Schnittstelle (Service based Interface) miteinander kommunizieren.

- **AMF (Access and Mobility Management Function)**

Die AMF (Access and Mobility Management Function) ist eine zentrale Komponente in der 5G-Netzarchitektur, die für die Verwaltung des Zugangs und der Mobilität der Geräte im Netzwerk verantwortlich ist. Sie authentifiziert die Endgeräte, überwacht den Handover-Prozess zwischen verschiedenen Funkzellen und stellt sicher, dass die Verbindungen stabil bleiben, auch wenn sich die Nutzer durch das Netzwerk bewegen. Dabei spielt sie eine Schlüsselrolle in der Sicherstellung einer nahtlosen Netzwerkabdeckung und eines stabilen Nutzererlebnisses.

Ebenso ist die AMF für die Verschlüsselung (NAS ciphering) und die Integritätssicherung (NAS integrity protection) der NAS-Nachrichten verantwortlich, die die Vertraulichkeit und Authentizität der übertragenen Informationen gewährleisten. Diese Funktionen sind entscheidend, um die Sicherheit der Daten während der Übertragung und die Integrität der Kommunikation im gesamten Netzwerk sicherzustellen.[5]

- **UPF (User Plane Function)**

Die UPF ist für die Verwaltung des Datenverkehrs im 5G-Netz zuständig. Sie leitet Datenpakete zwischen dem Endgerät und externen Netzwerken weiter, verwaltet den Datenfluss und gewährleistet die Einhaltung der Qualitätssicherungsstandards (QoS).

- **SMF (Session Management Function)**

Die SMF ist verantwortlich für die Verwaltung von Sitzungen im 5G-Netzwerk. Sie steuert die Einrichtung, Pflege und Beendigung von Netzwerksitzungen und konfiguriert die UPF, um die Datenübertragung während einer Sitzung zu ermöglichen.

- **PCF (Policy Control Function)**

Die PCF steuert die Datenverkehrsrichtlinien im Netzwerk. Sie sorgt dafür, dass der Datenverkehr nicht die zulässigen Kapazitäten überschreitet und verwaltet die Richtlinien für die Qualität und Priorisierung der Datendienste.

- **UDM (Unified Data Management)**

Die UDM fungiert als zentrale Datenbank für Nutzerinformationen. Sie ist für die Speicherung und Verwaltung von Abonnentendaten, wie z.B. Authentifizierungsinformationen, zuständig und unterstützt die Netzwerkfunktionen bei der Bereitstellung von Diensten für die Endnutzer.

- **NRF (Network Repository Function)**

Die NRF verwaltet das Register der Netzwerkfunktionen. Sie ermöglicht es den verschiedenen NF, sich zu registrieren, zu finden und miteinander zu kommunizieren, wodurch die Interaktion und Koordination zwischen den Funktionen erleichtert wird.[5]

- **NSSF (Network Slice Selection Function)**

Die NSSF ist für die Auswahl und Verwaltung von Netzwerkslices verantwortlich. Sie hilft dabei, Geräte den richtigen Netzwerkslices zuzuweisen, um spezifische Dienste oder Anforderungen zu erfüllen.

- **AUSF (Authentication Server Function)**

Die AUSF ist für die Authentifizierung der Geräte und Nutzer im 5G-Netz verantwortlich. Sie arbeitet mit anderen Funktionen, wie der AMF, zusammen, um sicherzustellen, dass nur autorisierte Geräte auf das Netzwerk zugreifen können.

- **UDR (Unified Data Repository)**

Die UDR ist eine zentrale Datenbank im 5G-Kernnetz, die verschiedenen Arten von Netzwerkdaten speichert und verwaltet. Dazu gehören Abonnentendaten, Policy-Daten, Sitzungsinformationen und Anwendungsdaten. Die UDR stellt sicher, dass alle relevanten Netzwerkfunktionen (z. B. UDM, PCF) auf diese Informationen zugreifen können, um ihre Aufgaben effizient zu erfüllen.[6]

2.2 (3GPP) und seine Rolle bei 5G

Das 3rd Generation Partnership Project (3GPP) ist eine globale Kooperationsplattform, die sich der Entwicklung von technischen Spezifikationen für Mobilfunktechnologien widmet. Gegründet im Jahr 1998, besteht 3GPP aus mehreren regionalen Telekommunikationsstandardisierungsorganisationen (SSOs), darunter ETSI (Europa), ARIB und TTC (Japan), ATIS (USA), CCSA (China), und TTA (Südkorea). Diese Partnerorganisationen arbeiten gemeinsam an der Erarbeitung von globalen Standards für mobile Telekommunikationssysteme.
Um den wachsenden Anforderungen neuer Dienste gerecht zu werden, die eine breite Palette an Industrien betreffen und unterschiedlichste Leistungsanforderungen haben, entwickelt die 3GPP eine innovative 5G-Systemarchitektur (5GS). Diese umfasst sowohl 5G New Radio (NR) als auch ein komplett neues 5G-Kernnetz (5GC). Dieses Kernnetz ist von zentraler Bedeutung für den Erfolg der 5G-Technologie, da es neue Dienste ermöglicht und gleichzeitig von den Effizienzvorteilen der Cloud-Technologie profitiert. [7]

2.2.1 Organisation und Aufgaben von 3GPP

Entwicklung globaler Mobilfunkstandards: Die Hauptaufgabe von 3GPP besteht darin, technische Spezifikationen zu entwickeln, die den Betrieb von Mobilfunknetzwerken weltweit standardisieren. Zu den bedeutendsten von 3GPP entwickelten Standards gehören GSM (2G), UMTS (3G), LTE (4G) und 5G NR (New Radio), die die Grundlage für mobile Netzwerke in nahezu allen Ländern der Welt bilden.

Förderung der Interoperabilität: Eine zentrale Aufgabe von 3GPP ist die Sicherstellung der Interoperabilität zwischen verschiedenen Netzwerken und Geräten. Durch die Erstellung einheitlicher Standards wird garantiert, dass Endgeräte und Netzinfrastrukturen verschiedener Hersteller nahtlos miteinander funktionieren. Dies hat entscheidend dazu beigetragen, dass Mobilfunkdienste weltweit verfügbar und miteinander kompatibel sind.

Technische Weiterentwicklung von Mobilfunktechnologien: 3GPP verfolgt kontinuierlich das Ziel, die Leistungsfähigkeit von Mobilfunknetzen zu verbessern. Mit jeder neuen Generation der Mobilfunkstandards werden höhere Datenraten, geringere Latenzzeiten und verbesserte Effizienz in der Nutzung des Spektrums angestrebt. So war 3GPP maßgeblich an der Entwicklung von 5G beteiligt, das nicht nur höhere Geschwindigkeiten ermöglicht, sondern auch die Grundlage für neue Technologien wie das Internet der Dinge (IoT) und autonome Fahrzeuge schafft.

Spezifikation von Netzwerkarchitekturen: Neben den Mobilfunktechnologien an sich entwickelt 3GPP auch Spezifikationen für die zugrunde liegenden Netzwerkinfrastrukturen. Diese umfassen sowohl die Radio Access Network (RAN)-Schnittstellen als auch die Core-Network-Architektur (CN). Insbesondere die Arbeit an der servicebasierten Architektur (SBA) im 5G-Kernnetz stellt eine der jüngsten Innovationen dar, die auf Flexibilität und Skalierbarkeit in modernen Netzwerken abzielt.

Koordination der globalen Standardisierung: 3GPP übernimmt die Rolle eines Koordinators zwischen verschiedenen regionalen Standardisierungsorganisationen und sorgt dafür, dass die entwickelten Spezifikationen weltweit einheitlich übernommen und implementiert werden. Dies umfasst auch die enge Zusammenarbeit mit internationalen Regulierungsbehörden wie der ITU (International Telekommunikation Union).

Veröffentlichung von Releases: 3GPP arbeitet in einem kontinuierlichen Zyklus, in dem neue technische Spezifikationen und Standards in sogenannten "Releases" veröffentlicht werden. Jede Veröffentlichung repräsentiert eine neue Phase in der Entwicklung der Mobilfunktechnologien. Zum Beispiel wurde mit Release 15 die erste Standardisierung für 5G eingeführt, während spätere Releases kontinuierliche Verbesserungen und Erweiterungen von 5G beinhalten.[8]

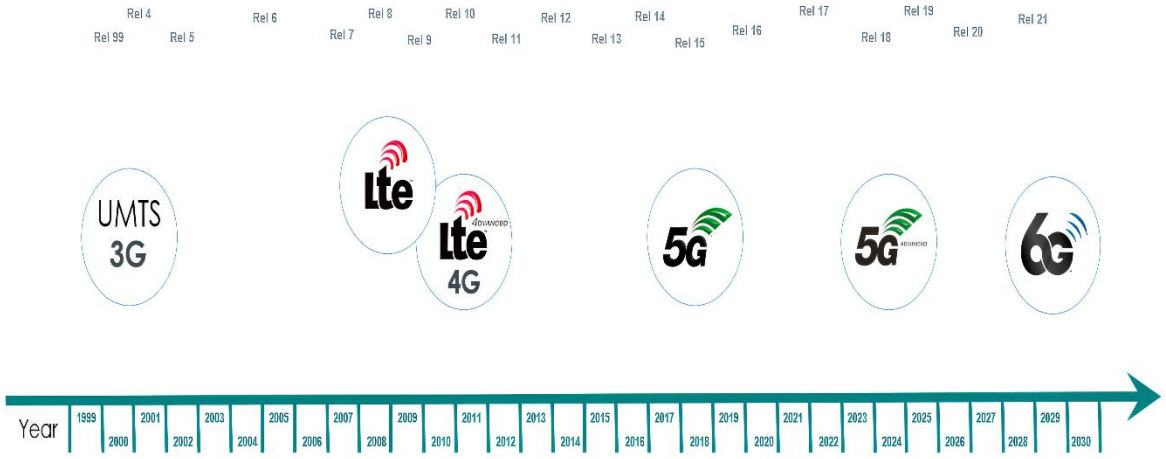

Abbildung 2: 3GPP Releases und Generations [7]

2.3 Private 5G-Netzwerke

2.3.1 Definition und Anwendungsfälle

Ein privates 5G-Netzwerk ist ein auf 3GPP-Standards basierendes Mobilfunknetz, das speziell für eine bestimmte Unternehmenskundengruppe oder für industrielle Anwendungen eingerichtet wird. Es ermöglicht exklusiven Zugang zu privaten Ressourcen und kann dedizierte Frequenzspektren sowie maßgeschneiderte Hardware- und Software-Infrastrukturen umfassen. Diese Netzwerke sind in der Lage, eine Vielzahl von Anwendungsfällen zu unterstützen, darunter drahtloser Festnetzanschluss, mobiles Breitband, IoT-Endpunkte und extrem zuverlässige, latenzarme Anwendungen, die insbesondere in Industrieumgebungen von entscheidender Bedeutung sind.[9]

2.3.2 Vergleich zu öffentlichen 5G-Netzen

Öffentliche 5G-Netze sind von Mobilfunkanbietern bereitgestellte Netzwerke, die für die breite Öffentlichkeit zugänglich sind. Sie bieten die typischen Vorteile von 5G, wie höhere Datenraten, geringere Latenzzeiten und eine verbesserte Netzabdeckung. Allerdings haben Unternehmen, die sich für die Nutzung öffentlicher 5G-Netze entscheiden, keine Kontrolle über die Netzwerkeinstellungen oder deren

Konfiguration. Die Infrastruktur wird vollständig von den Netzbetreibern verwaltet, was für den allgemeinen Einsatz in den meisten Anwendungen ausreicht, aber nicht immer den spezifischen Anforderungen von Unternehmen gerecht wird.

Private 5G-Netze hingegen bieten Unternehmen eine exklusive, maßgeschneiderte Infrastruktur, die speziell auf ihre Bedürfnisse zugeschnitten ist. Im Gegensatz zu öffentlichen Netzen haben Unternehmen bei privaten Netzwerken die volle Kontrolle über die Netzwerkkonfiguration, was höhere Flexibilität und Sicherheit ermöglicht. Dies ist besonders wichtig für Industrien, in denen Datenschutz und eine stabile Netzwerkperformance von entscheidender Bedeutung sind, wie etwa in der Fertigung, im Gesundheitswesen oder bei IoT-Anwendungen.[10]

Ein zentraler Vorteil privater 5G-Netze besteht in der vollständigen Netzwerkkontrolle, die sie Unternehmen bieten. Diese Netzwerke ermöglichen es den Betreibern, sämtliche Netzwerkeinstellungen individuell anzupassen, einschließlich der Priorisierung von Diensten und der Zuordnung von Bandbreiten. In öffentlichen Netzen hingegen fehlt den Unternehmen diese Flexibilität, da die Netzwerkkonfiguration und -verwaltung ausschließlich dem Mobilfunkanbieter unterliegt.

Ein weiterer entscheidender Vorteil ist die Sicherheit. Private 5G-Netze sind nur für autorisierte Nutzer zugänglich und bieten dadurch ein höheres Maß an Sicherheit, verglichen mit öffentlichen Netzen, die für eine Vielzahl von Nutzern geöffnet sind. Diese Eigenschaft macht private Netze besonders attraktiv für Branchen, in denen der Datenschutz und die Netzwerksicherheit eine hohe Priorität haben.

Auch die Anpassbarkeit privater 5G-Netze ist ein großer Pluspunkt. Unternehmen können die Netzwerke speziell an ihre eigenen Bedürfnisse anpassen, etwa zur Unterstützung von IoT-Geräten, für Anwendungen mit niedriger Latenz oder für Szenarien, in denen hohe Datendurchsätze erforderlich sind. Öffentliche Netze bieten hingegen standardisierte Dienste, die weniger Flexibilität in Bezug auf spezifische Unternehmensanforderungen erlauben.

Die Zuverlässigkeit privater 5G-Netze ist ebenfalls ein wesentlicher Vorteil. Da es in einem privaten Netz keine Konkurrenz mit anderen Nutzern um die Nutzung der Ressourcen gibt, bleibt die Netzwerkleistung stabil und vorhersehbar. Im Gegensatz

dazu können öffentliche Netze bei hoher Auslastung durch viele Nutzer überlastet werden, was zu einer Verschlechterung der Netzwerkqualität führen kann.

Zusätzlich können private 5G-Netze bei der Frequenznutzung exklusive Frequenzbänder verwenden. Dies ermöglicht es, Interferenzen mit anderen Netzwerken zu vermeiden. In öffentlichen Netzen hingegen wird das Frequenzspektrum unter vielen Nutzern geteilt, was potenziell zu Überlastungen führen kann.

Nachteile privater 5G-Netze:

Trotz ihrer vielen Vorteile sind private 5G-Netze auch mit Kosten verbunden. Der Aufbau eines unabhängigen privaten Netzwerks erfordert hohe Investitionen, insbesondere wenn es um den Erwerb von eigener Infrastruktur und Spektrum geht. Diese hohen Investitionskosten können für kleinere Unternehmen eine Herausforderung darstellen.

Darüber hinaus ist die Komplexität ein weiterer Nachteil privater Netze. Die Verwaltung und der Betrieb eines privaten 5G-Netzes erfordern technisches Fachwissen und spezifisches Know-how. Dies betrifft insbesondere die Wartung und den reibungslosen Betrieb der Netzwerkinfrastruktur. Im Gegensatz dazu werden öffentliche Netzwerke vollständig von den Netzbetreibern verwaltet, was den Unternehmen den Aufwand und die Verantwortung für den Betrieb des Netzes abnimmt.

Feature	Release 15 — Dec 2018	Release 16 — July 2020	Release 17 — July 2022	Release 18:
Datenrate/Bereichsverkehrskapazität(20 Gbit/s)	Komplett	Komplett	Komplett	Komplett
Spektrumeffizienz (3x LTE)	Komplett	Komplett	Komplett	Komplett
Netzwerk-Energieeffizienz	Komplett	Komplett	Komplett	Komplett
Verbindungsdichte (1.000.000/km2)	teilweise	teilweise	Komplett	Komplett
Latenz (<10 ms)	None	teilweise	Komplett	Komplett
Zuverlässigkeit (99,999 % unter 10 ms)	None	teilweise	Komplett	Komplett
Mobilität (Roaming mit 500 km/h)	Komplett	Komplett	Komplett	Komplett
Nicht öffentliche Netzwerke (private Netzwerke)	None	teilweise	Komplett	Komplett
Industrielles IoT (TSN-Unterstützung)	None	teilweise	teilweise	Komplett
Network Slicing	Komplett	Komplett	Komplett	Komplett
Sidelink (direkte Kommunikation zwischen Endgeräten)	None	teilweise	teilweise	Komplett

Tabelle 2: 3GPP Releases 16, 17, and 18[9]

Die Tabelle 2 stellt die Entwicklung der wichtigsten 5G-Funktionen über die verschiedenen 3GPP-Releases dar, beginnend mit Release 15 (Dezember 2018) bis Release 18. Dabei werden zentrale 5G-Funktionen wie Datenrate, Spektrumseffizienz, Latenz, Zuverlässigkeit, Mobilität und Network Slicing aufgeführt und bewertet, inwieweit sie in den jeweiligen Releases implementiert wurden.

In Release 15 wurden grundlegende 5G-Funktionen wie hohe Datenraten, Spektrumseffizienz und Mobilität vollständig umgesetzt. Release 16 brachte teilweise Verbesserungen in Bereichen wie Verbindungsdichte, Latenz und nicht-öffentliche Netzwerke (private Netzwerke). Mit Release 17 wurden viele der zuvor teilweise umgesetzten Funktionen, wie Verbindungsdichte, Latenz und Sidelink-Kommunikation, vollständig realisiert. Release 18 stellt den nächsten Schritt dar, in dem alle Funktionen, einschließlich industrielles IoT, Network Slicing und Sidelink-Kommunikation, komplettiert werden.

Die Tabelle verdeutlicht den kontinuierlichen Fortschritt von 5G durch die 3GPP-Standardisierung, wobei jede Version zusätzliche Funktionalitäten und Optimierungen bringt, um den wachsenden Anforderungen der 5G-Technologie gerecht zu werden.

3. Sicherheitsaspekte von 5G

Die Sicherheit im Kontext von 5G spielt eine entscheidende Rolle und gewinnt zunehmend an Bedeutung. Dies wird insbesondere deutlich, wenn man betrachtet, dass 5G der erste große Schritt hin zu einer vollständig vernetzten Gesellschaft ist. Die Anwendungsfelder dieser Technologie sind vielfältig: Wirtschaftlich gesehen, insbesondere im Rahmen von Industrie 4.0, ermöglichen vernetzte Fabriken automatisierte Prozesse, in denen Fahrzeuge und Maschinen miteinander kommunizieren, um beispielweise Materialien zu transportieren.
Im Gesundheitsbereich eröffnet 5G die Möglichkeit zu Anwendungen wie der Fernüberwachung von Patienten und zur telemedizinischen Diagnose. Auch in der Mobilität spielen 5G-Netze eine wichtige Rolle – vernetzte Fahrzeuge, seien es autonome Autos oder solche mit Fahrerassistenzsystemen, werden über das Netzwerk sowohl untereinander als auch mit anderen Verkehrsinfrastrukturen kommunizieren. Weiterhin können vernetzte Sensoren für Umweltanwendungen wie Temperatur- oder Schadstoffmessungen in Städten eingesetzt werden.

Die Anwendungsfälle stellen unterschiedliche Anforderungen an die Leistungsfähigkeit des Netzes (KPI), etwa durch niedrige Latenzzeiten, hohe Zuverlässigkeit und Verfügbarkeit. Besonders in kritischen Bereichen, wie dem Gesundheitssektor oder im Straßenverkehr, kann die Erfüllung dieser KPIs über Leben und Tod entscheiden. Beispielsweise wurde 2019 ein Krankenhaus in Rouen, Frankreich, Opfer eines Cyberangriffs, der die medizinische Versorgung zeitweise komplett zum Erliegen brachte. Solche Angriffe unterstreichen die wachsende Gefahr durch Cyberattacken, die die Sicherheit und Gesundheit der Menschen gefährden.[13]

3.1 Bedrohungslandschaft und Sicherheitsanforderungen

Die Infrastruktur von 5G-Netzen ist erheblich komplexer als die der Vorgängergeneration 4G, was neue Angriffsrisiken mit sich bringt. Diese gesteigerte Komplexität resultiert in einer größeren Angriffsfläche, da die Kommunikation über vielfältige Protokolle und ihre Implementierung mehr mögliche Schwachstellen bietet. Zudem ist das 5G-Netz „offener“ gestaltet. Drittanbieter können eigene Anwendungen und Dienste basierend auf der 5G-Infrastruktur entwickeln. Diese Offenheit führt dazu,

dass die Angriffsfläche im Vergleich zu früheren Mobilfunkgenerationen deutlich ausgeweitet ist.
Darüber hinaus sind 5G-Netze durch ihre Flexibilität anfälliger für Angriffe. Dies zeigt sich etwa in der Aufteilung von Netzwerkfunktionen wie der SMF (Session Management Function) und UPF (User Plane Function). Technologien wie Software-defined Networking (SDN) und Network Function Virtualization (NFV) bieten zwar eine verbesserte Skalierbarkeit, eröffnen jedoch auch neue Möglichkeiten für Angreifer. Erlangen sie beispielsweise Kontrolle über die Steuerungsebene des Netzwerks, können sie erhebliche Schäden anrichten. Wenn etwa Zugriff auf die Network Repository Function (NRF) erlangt wird, könnten Angreifer gefälschte Netzwerkfunktionen einführen oder aktive Dienste manipulieren.
Im Vergleich zu früheren Mobilfunkgenerationen liegt der Fokus bei 5G deutlich stärker auf der Sicherheit. Die Spezifikationen von 5G wurden entwickelt, um aus den Erfahrungen früherer Generationen zu lernen und gleichzeitig neue Sicherheitsprotokolle zu integrieren. Bestehende Sicherheitsmaßnahmen aus 4G wurden übernommen und gezielt gestärkt, Schwachstellen wurden identifiziert und behoben.
Insgesamt spielt die Sicherheit im 5G-Netz eine weitaus größere Rolle als in früheren Generationen. Die Vielzahl möglicher Angriffsvektoren und die potenziellen Auswirkungen von Angriffen, die bis zur Gefährdung von Menschenleben reichen können, machen Sicherheitsaspekte zu einem zentralen Anliegen im Zeitalter von 5G. Daher markiert 5G nicht nur eine technologische Weiterentwicklung, sondern auch eine deutliche Verschiebung des Sicherheitsparadigmas in Mobilfunknetzwerken.

3.2 Sicherheitsarchitektur von 5G

Basierend auf den Sicherheitsanforderungen des industriellen Internets und einer Analyse der traditionellen Netzwerkarchitektur zeigt sich, dass herkömmliche Netzwerke die Anforderungen des industriellen Internets nicht ausreichend erfüllen können. Daher ist es notwendig, die Sicherheitsarchitektur zu verbessern und eine 5G-Netzsicherheitsarchitektur zu entwickeln, die den spezifischen Sicherheitsanforderungen des industriellen Internets gerecht wird. [11]

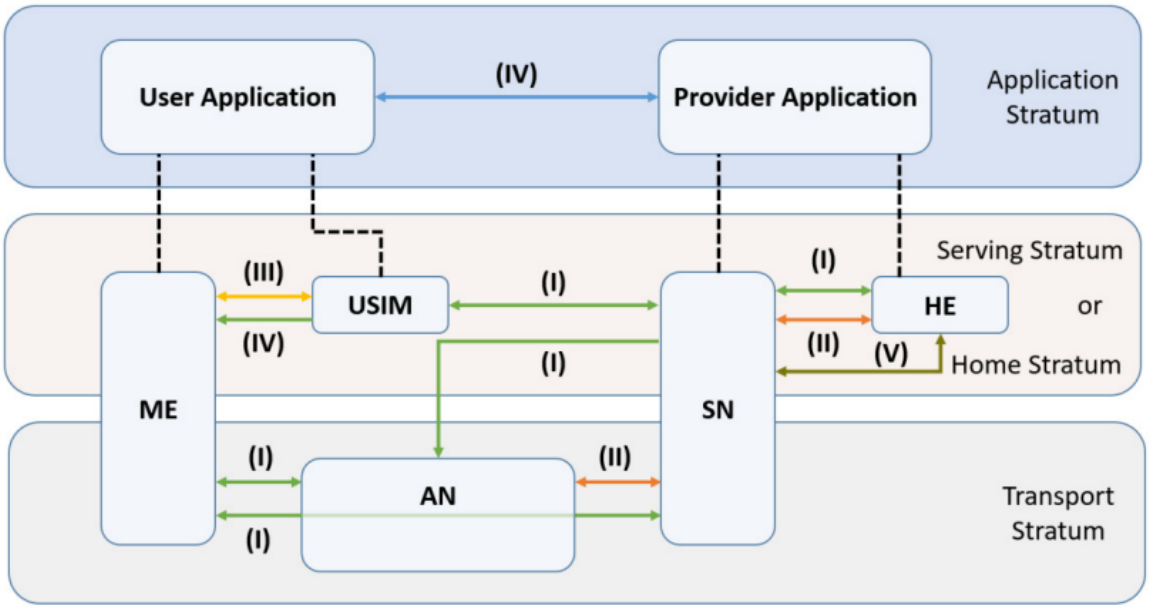

Abbildung 3: Sicherheitsarchitektur von 5G[11]

Die Abbildung 3 zeigt die Sicherheitsarchitektur eines 5G-Netzwerks und veranschaulicht die verschiedenen Schichten und Verbindungen, die für die Sicherheit und Kommunikation in 5G-Systemen relevant sind. Die Darstellung ist in drei Schichten unterteilt: Transport Stratum, Serving/Home Stratum und Application Stratum. Jede Schicht spielt eine wichtige Rolle in der Kommunikation und Sicherheit des 5G-Netzwerks.

1. Transport Stratum

Dies ist die unterste Ebene der Abbildung. Sie enthält die Komponenten, die für die Übertragung der Nutzerdaten im 5G-Netz verantwortlich sind:

- **AN (Access Network)**: Das Zugangsnetzwerk, das die Verbindung zwischen dem Endgerät (ME) und dem Netzwerk herstellt. Hier findet die eigentliche Übertragung der Datenpakete statt.
- **ME (Mobile Equipment)**: Das Endgerät des Nutzers (z.B. Smartphone, IoT-Gerät), das über das Zugangsnetzwerk mit dem Kernnetz (SN) kommuniziert.
- Die Verbindungen zwischen dem AN und ME (Pfeil I) sind sicherheitskritisch, da sie den initialen Datenverkehr abdecken.

2. Serving/Home Stratum

Diese mittlere Ebene repräsentiert den „Kern“ des 5G-Netzwerks, der sowohl den Serving Network (SN) als auch das Home Network (HE) beinhaltet.

- **USIM (Universal Subscriber Identity Module)**: Eine Sicherheitskomponente, die sich typischerweise auf der SIM-Karte des Nutzers befindet und für die Authentifizierung und Autorisierung verantwortlich ist. Sie sichert die Identität des Nutzers ab.
- **SN (Serving Network)**: Das Netzwerk, das dem Nutzer Dienste bereitstellt und für die Authentifizierung sowie die Verwaltung der Verbindung zuständig ist.
- **HE (Home Environment)**: Das Heimatnetzwerk des Nutzers, das zusätzliche Sicherheitsmechanismen bereitstellt und für die Verwaltung der Benutzerprofile und Authentifizierungsdaten verantwortlich ist.

3. Application Stratum

Diese Ebene umfasst die Anwendungsschicht, in der die Nutzer- und Anbieteranwendungen interagieren.

- **User Application**: Die Anwendung, die auf dem Endgerät (ME) ausgeführt wird, beispielsweise eine mobile App oder ein IoT-Service.
- **Provider Application**: Die korrespondierende Anwendung, die von einem Dienstanbieter bereitgestellt wird.

Diese Netzsicherheitsarchitektur umfasst sechs definierte Sicherheitsbereiche:[12]

- **Sicherheit des Netzwerkzugangsdomain (I)**: Diese Domäne umfasst verschiedene Sicherheitsfunktionen, die sicherstellen, dass sich Endgeräte (UE, User Equipment) sicher authentifizieren und auf Dienste zugreifen können, sowohl über 3GPP- als auch über nicht-3GPP-Zugänge. Diese Mechanismen schützen die (drahtlosen) Schnittstellen vor Angriffen. Zudem wird der Sicherheitskontext vom Servicenetzwerk an das Endgerät übermittelt, um den sicheren Zugang zu gewährleisten.[11]
- **Sicherheit der Netzwerkdomain (II)**: Diese Domäne garantiert den sicheren Austausch von Signalisierungsdaten und Nutzerdaten zwischen den

Netzwerkkomponenten, um die Integrität und Vertraulichkeit der Übertragung sicherzustellen.

- **Sicherheit der Benutzerdomain (III)**: Diese Sicherheitsmaßnahmen ermöglichen es, dass Nutzer sicher auf ihre mobilen Endgeräte zugreifen können. Hier steht die Sicherung der Benutzeridentität und des Gerätezugangs im Vordergrund.
- **Sicherheit der Applikationsdomain (IV)**: Diese Domäne gewährleistet, dass Anwendungen im Benutzerdomain sicher mit Anwendungen in der Domäne des Dienstanbieters kommunizieren können. So wird die sichere Interaktion von Anwendungen auf verschiedenen Ebenen sichergestellt.
- **Transparente und konfigurierbare Sicherheit (V)**: Diese Domäne umfasst Sicherheitsmechanismen, die gewährleisten, dass Nutzer die implementierten Sicherheitsfunktionen wahrnehmen und verstehen können. So wird sichergestellt, dass die Konfiguration der Sicherheitsfunktionen für den Endnutzer transparent ist.[11]

3.2.1 Authentifizierung und Verschlüsselung

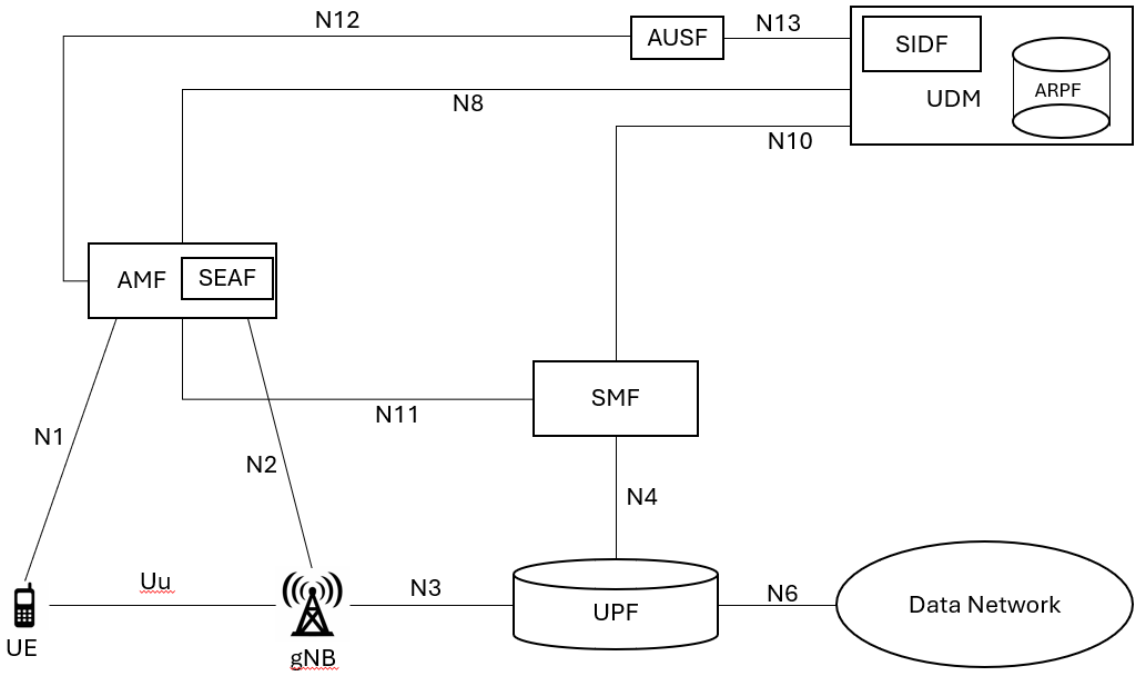

Abbildung 4: Beteiligte Komponenten bei der 5G-Sicherheitsfunktion[13]

Die Sicherheit im 5G-Netzwerk basiert auf mehreren Schlüsselkomponenten und Mechanismen, die gemeinsam sicherstellen, dass der Zugriff auf das Netzwerk sowie die Datenübertragung geschützt sind. Eine Vielzahl von Funktionen ist speziell darauf ausgelegt, sowohl die Identität der Benutzer zu schützen als auch die Integrität und Vertraulichkeit der übertragenen Informationen zu gewährleisten. Diese Funktionen sind in verschiedenen Netzwerkkomponenten implementiert und arbeiten eng zusammen, um eine umfassende Sicherheitsarchitektur bereitzustellen. Im Folgenden werden die wichtigsten Entitäten und ihre jeweiligen Sicherheitsaufgaben im 5G-Netzwerk näher erläutert.

Im UDM (Unified Data Management) befindet sich die erste Sicherheitsfunktion, bekannt als "Authentication Credential Repository and Processing Function" (ARPF). Um die Bedeutung der Sicherheit im 5G-Kontext zu betonen, wurden die Sicherheitsfunktionen mit spezifischen Namen versehen. Das ARPF speichert die permanenten Schlüssel der Abonnenten, die niemals das ARPF verlassen. Außerdem generiert es Authentifizierungsvektoren, die unter anderem dazu dienen, die

Authentifizierung zu überprüfen sowie die Hauptschlüssel für die Integrität und Verschlüsselung zu erstellen. Diese Funktion ist fest im UDM integriert.

Eine weitere wichtige Funktion im UDM ist die zur Verschleierung der Identität. Im 5G-Netz wird die dauerhafte Identität eines Nutzers als "Subscription Permanent Identifier" (SUPI) bezeichnet. Allerdings wird die SUPI nicht direkt über den Funkkanal übertragen. Stattdessen wird eine verschlüsselte Form dieser Identität verwendet, der sogenannte "Subscription Concealed Identifier" (SUCI). Der SUCI ist eine verschlüsselte Version des SUPI und schützt die Identität des Nutzers vor Manipulation durch Angreifer. Die "Subscription Identifier De-concealing Function" (SIDF) übernimmt die Aufgabe, den SUCI zu entschlüsseln und den ursprünglichen SUPI wiederherzustellen. Diese Funktion ist standardmäßig im UDM integriert, kann jedoch auch als eigenständige Funktion außerhalb des UDM existieren.

Die AUSF (Authentication Server Function) ist der Authentifizierungsserver im 5G-Netzwerk. Ihre Aufgabe besteht darin, Authentifizierungsvektoren für die Netzwerke bereitzustellen, die sie anfordern. Dabei wird immer nur ein Vektor pro Anfrage übermittelt. Die AUSF validiert die Authentifizierung des Teilnehmers und ist stets im Heimnetzwerk des Abonnenten angesiedelt.

In AMF gibt es ein Element, das die Rolle eines „Voraus-Authentifikators“ übernimmt, die sogenannte SEAF (SEcurity Anchor Function). Diese Funktion führt eine Vorprüfung der Authentifizierung durch und berechnet aus dem vom AUSF gesendeten Elternschlüssel den "Child Key". Dieser Schlüssel wird für die Integritätsprüfung und Verschlüsselung genutzt. Die SEAF ist in der AMF (Access and Mobility Management Function) integriert.

Aus praktischer Sicht ist die SEAF also ein Teil der AMF, wobei diese auch sicherheitsrelevante Aufgaben als AMF übernimmt. Die AMF verschlüsselt und gewährleistet die Integrität der sogenannten Non Access Stratum (NAS)-Nachrichten, die zwischen dem Endgerät (UE) und der AMF ausgetauscht werden und über die gNB (Next Generation Node B) übertragen werden. Die gNB selbst ist für die Verschlüsselung aller Daten und Nachrichten zuständig, die über den Funkkanal gesendet werden. Dabei berechnen sowohl die gNB als auch die AMF die Verschlüsselungs- und Integritätsschlüssel, die stets aus den übergeordneten Schlüsseln abgeleitet werden. Für jeden übertragenen Datenblock wird die Integrität

durch Berechnung und Prüfung des Message Authentication Codes (MAC) sichergestellt. Zusätzlich werden die Daten bei der Übertragung verschlüsselt und entschlüsselt.

Zusammenfassend lässt sich sagen, dass die Netzwerkfunktionen, die die Sicherheit in 5G gewährleisten, die UDM mit den Funktionen ARPF (Langzeitschlüsselspeicherung) und SIDF (Identitätsentschlüsselung) sind. Weiterhin spielt die AUSF als Authentifizierungsserver im Heimnetzwerk eine zentrale Rolle. Die AMF fungiert als SEAF und sorgt als Sicherheitsanker für den Schutz der NAS-Nachrichten. Schließlich übernimmt die gNB alle Aufgaben im Zusammenhang mit der Funkübertragung und deren Sicherheit.[14]

4. Aufbau eines privates 5G-Netzwerks

Der Aufbau eines privaten 5G-Netzwerks bietet eine flexible und kontrollierbare Infrastruktur, die speziell für spezifische Anwendungsfälle und Testumgebungen optimiert werden kann. Im Gegensatz zu öffentlichen Netzwerken ermöglicht ein privates 5G-Netzwerk eine vollständige Kontrolle über Sicherheitsmaßnahmen, Netzwerkeinstellungen und die Nutzung dedizierter Ressourcen. In diesem Abschnitt wird die Planung, Implementierung und Sicherheit eines privaten 5G-Netzwerks detailliert beschrieben, wobei der Fokus auf der Verwendung von Open-Source-Tools und spezifischen Hardwarekomponenten liegt.

4.1 Planungs- und Designphasen

4.1.1 Anforderungen und Zielsetzungen

Das primäre Ziel des Aufbaus eines privaten 5G-Netzwerks besteht darin, eine vollständig kontrollierbare und flexible Infrastruktur bereitzustellen, die speziell für die Entwicklung und Durchführung von Testfällen konzipiert ist. Dieses Netzwerk wird insbesondere für die Validierung und Prüfung spezifischer 5G-Komponenten wie der AMF (Access and Mobility Management Function), SMF (Session Management Function) und zukünftig auch der UPF (User Plane Function) eingesetzt.

Gründe für die Wahl eines privaten 5G-Netzwerks

Flexibilität:

Ein privates 5G-Netzwerk ermöglicht eine vollständige Kontrolle über die Netzwerkeinstellungen, einschließlich Sicherheitsprotokollen und Ressourcenmanagement. Dies erlaubt es, ohne Einschränkungen durch öffentliche Netzbetreiber spezifische Konfigurationen umzusetzen, die den Anforderungen der Testfälle entsprechen.

Kostenkontrolle:

Im Vergleich zu öffentlichen Netzwerken besteht keine Abhängigkeit von Mobilfunkbetreibern hinsichtlich der Nutzung von Spektrum oder Infrastrukturressourcen. Dies ermöglicht eine kosteneffiziente Implementierung und langfristige Unabhängigkeit.

Anpassbarkeit:

Durch die Verwendung von Open-Source-Software wie Open5GS und srsRAN kann das Netzwerk flexibel und präzise auf die Anforderungen der Testumgebung abgestimmt werden. Die Möglichkeit, individuelle Konfigurationen vorzunehmen, stellt sicher, dass das Netzwerk optimal für spezifische Testszenarien angepasst ist.

4.2 Technische Spezifikationen

Das private 5G-Netzwerk basiert auf einer Kombination von Software und Hardware, die folgende Komponenten umfasst.

Software:

- **Open5GS:** Eine Open-Source-Implementierung des 5G-Kernnetzes, die wichtigen Funktionen (NFs) wie AMF, SMF, UPF und UDM bereitstellt.
- **srsRAN:** Ein Open-Source-Projekt zur Simulation von gNB und UE für eine vollständige 5G-Umgebung.

Hardware:

- **USRP B210 SDR Kit – Dual Channel Transceiver (70 MHz – 6 GHz):** Software-Defined Radio (SDR) für die Implementierung von gNB und UE.
- **GPSDO (GPS Disciplined Oscillator):** Für genaue Zeit und Frequenzsynchronisation.
- **Aktive 5-Volt-GPS-Antenne:** Zur Synchronisation des Netzwerks mit globalen Zeitquellen.
- **5G-Antenne:** Zur Übertragung und Empfang von 5G-Signalen.
- **SIM-Karten (sysmoISIM von Sysmocom):** Zur Authentifizierung und Verbindung des UE mit dem Kernnetz.

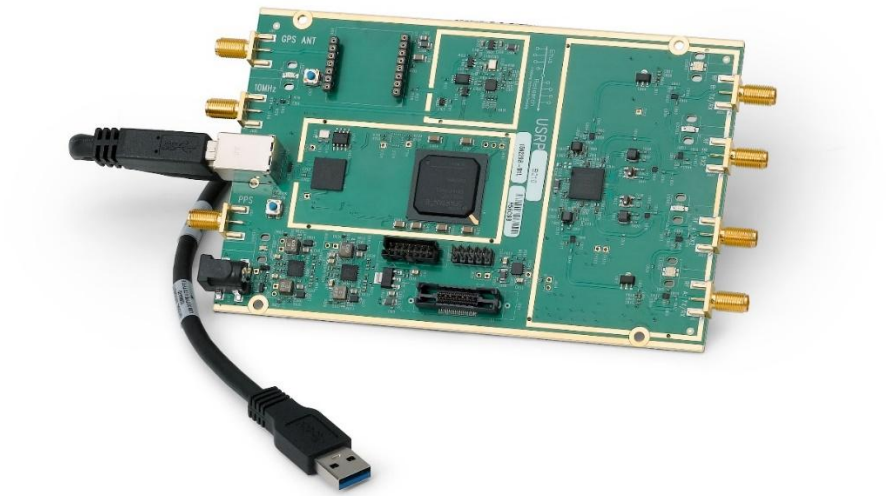

Abbildung 5: USRP B210 SDR Kit von Ettus[15]

Das USRP B210 von Ettus Research ist eine vollständig integrierte Software-Defined Radio (SDR)-Plattform, die auf einer einzigen Platine realisiert ist und eine durchgehende Frequenzabdeckung von 70 MHz bis 6 GHz bietet. Diese Plattform eignet sich hervorragend für kosteneffiziente Experimente und ist speziell für Forschung und Entwicklung im Bereich drahtloser Kommunikation konzipiert.

Das USRP B210 unterstützt duale Kanäle und ermöglicht sowohl Sende- als auch Empfangsvorgänge. Diese Flexibilität macht es ideal für den Einsatz in privaten 5G-Netzwerken, da es die Simulation und Analyse verschiedener Frequenzbänder und Kommunikationsszenarien erlaubt. Die Hardware ist kompatibel mit verschiedenen Open-Source-Softwareplattformen wie srsRAN, was eine nahtlose Integration in Testumgebungen und die Konfiguration von 5G-Komponenten ermöglicht.

Mit seiner breiten Frequenzabdeckung und den flexiblen Einsatzmöglichkeiten ist das USRP B210 eine Schlüsselkomponente für die Implementierung und das Testen von 5G-Netzwerklösungen. Es ermöglicht umfassende Experimentiermöglichkeiten bei vergleichsweise niedrigen Kosten, was es zu einem wertvollen Werkzeug für die Erforschung moderner Kommunikationssysteme macht.[15]

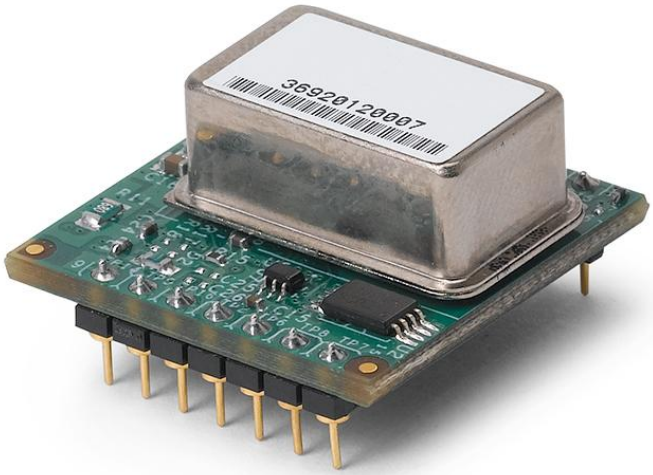

Abbildung 6: BOARD-MOUNTED GPSDO KIT [16]

Das Board-Mounted GPSDO Kit ist ein GPS-gesteuerter, temperaturgeregelter Quarzoszillator (GPSDO), der speziell für den Einsatz mit den USRP-Modellen B200 und B210 empfohlen wird. Dieses Kit stellt ein hochpräzises 10-MHz-Referenzsignal sowie ein 1-PPS-Signal (Pulse Per Second) zur Verfügung und ist ideal für Anwendungen, die eine erhöhte Frequenzgenauigkeit oder globale Zeitabstimmung erfordern.

Mit einer Frequenzgenauigkeit von 75 ppb (parts per billion) im nicht gesperrten Zustand und einer zeitlichen Präzision von 50 ns (Nanosekunden) im gesperrten Zustand bietet der GPSDO eine außergewöhnliche Leistung. Dies ermöglicht die Entwicklung von Systemen, die besonders präzise Frequenzreferenzen und zeitliche Synchronisation benötigen, wie es bei der Implementierung und dem Testen von 5G-Netzwerken erforderlich ist.

Durch die Integration dieses GPSDO-Kits in ein USRP B210 können Entwickler sicherstellen, dass ihre Systeme auch unter anspruchsvollen Bedingungen stabil und präzise arbeiten. Es ist somit eine entscheidende Komponente für die Erstellung robuster und synchronisierter drahtloser Kommunikationslösungen, insbesondere im Bereich privater 5G-Netzwerke.[16]

4.3 O-RAN gNB-Übersicht und Split 7.2x Architektur

4.3.1 Einführung in O-RAN und die funktionale Aufteilung

Mit der Einführung des gNodeB (gNB), das den eNodeB aus den LTE-Netzen ablöst, wurde eine neue Netzwerkarchitektur etabliert. Diese Architektur, die in der 3GPP Release 15 definiert wurde, ermöglicht ein modulares und flexibles Design, indem das gNB in drei Hauptkomponenten unterteilt wird. Die Centralized Unit (CU), die Distributed Unit (DU) und die Radio Unit (RU). Diese Komponenten kommunizieren über standardisierte Schnittstellen, um die Interoperabilität zu verbessern und die Netzwerkeffizienz zu steigern.

Die Einführung der funktionalen Aufteilung spielt eine zentrale Rolle bei der Optimierung der Netzwerkressourcen. Insbesondere der Split 7.2x, wie er von der Open RAN (O-RAN) Alliance definiert wurde, ermöglicht Ultra-Reliable Low Latency Communication (URLLC) und Edge-Deployments. Diese Aufteilung trennt zeitkritische Echtzeit-Aufgaben (die von der DU verwaltet werden) von nicht zeitkritischen Aufgaben (die von der CU bearbeitet werden). Dies verbessert die Skalierbarkeit des Netzwerks und ermöglicht Multi-Vendor-Netzwerkimplementierungen, was wiederum die Flexibilität und Effizienz bei der Bereitstellung von 5G-Netzen erhöht.

4.3.2 Funktionale Komponenten und ihre Rollen

1. Radio Unit (RU):
    - Die RU befindet sich am Rand des Netzwerks und ist für die Verarbeitung der Funkfrequenzen (RF) zuständig, einschließlich des Sendens und Empfangens von Signalen über die Luftschnittstelle. Sie ist über die Fronthaul-Schnittstelle mit der DU verbunden.
    - Durch ihre Nähe zu den Antennen wird eine optimale Signalverarbeitung gewährleistet.
2. Distributed Unit (DU):
    - Die DU übernimmt zeitkritische Aufgaben wie die Medium Access Control (MAC) und die Radio Link Control (RLC)-Schichten. Sie verarbeitet Benutzerdaten und verwaltet die Kommunikation mit der RU

(über die Fronthaul-Schnittstelle) und der CU (über die Midhaul-Schnittstelle).

3. Centralized Unit (CU):
    - Die CU kümmert sich um nicht zeitkritische Aufgaben, darunter die Radio Resource Control (RRC) und die Packet Data Convergence Protocol (PDCP)-Schichten. Sie verbindet das RAN über die NG-Schnittstelle mit dem Kernnetzwerk.

Vorteile der Split 7.2x Architektur:

Die Split 7.2x Architektur erlaubt es, verschiedene Teile der gNB-Funktionalität effizient zu verteilen. Dies führt zu:

- Flexibilität: Modularität ermöglicht die einfache Integration neuer Technologien und Anpassung an verschiedene Netzwerkarchitekturen.
- Kostenersparnis: Multi-Vendor-Ansätze fördern Wettbewerb und senken die Implementierungskosten.
- Leistungsfähigkeit: Die Aufteilung ermöglicht eine optimierte Verarbeitung von Echtzeit- und nicht-Echtzeit-Daten, was die Netzwerkqualität steigert.

Durch die Nutzung dieser Architektur mit Tools wie Open5GS und srsRAN lassen sich leistungsstarke private 5G-Netzwerke implementieren, die sowohl für Tests als auch für betriebliche Anwendungen geeignet sind.[17]

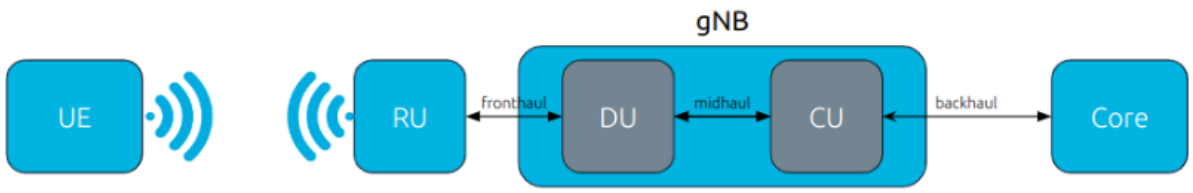

Abbildung 7: 5G Split 7.2x gNB Architektur mit RU und Core[18]

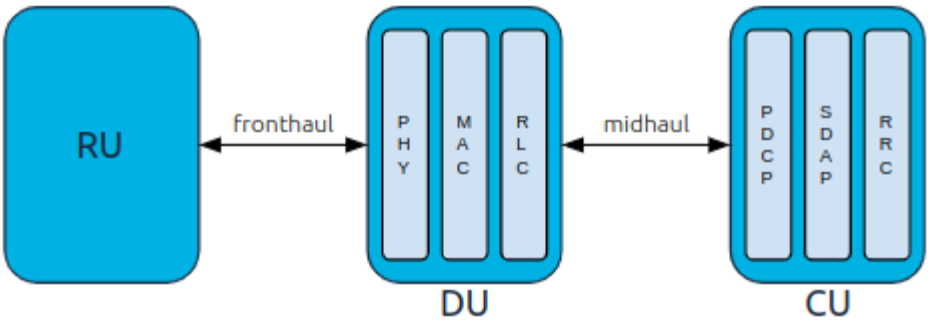

Abbildung 8: CU und DU in der O-RAN gNB-Architektur

Abbildung 9 zeigt die funktionale Split-Architektur in einem privaten 5G-Netzwerk mit srsRAN und Open5GS. Die srsDU (Distributed Unit) übernimmt zeitkritische Aufgaben wie MAC- und RLC-Verarbeitung, während die srsCU (Centralized Unit) nicht-zeitkritische Prozesse wie RRC und PDCP verwaltet. Die DU und CU kommunizieren über die F1-Schnittstelle, um eine effiziente Koordination sicherzustellen. Die CU verbindet sich über die N2-Schnittstelle (Signalisierung) und die N3-Schnittstelle (Daten) mit den 5G-Kernfunktionen in Open5GS. Der 5G-Kern umfasst zentrale Komponenten wie die AMF (Access and Mobility Management Function) und die UPF (User Plane Function) für die Netzwerkkontrolle und den Datenverkehr.[17]

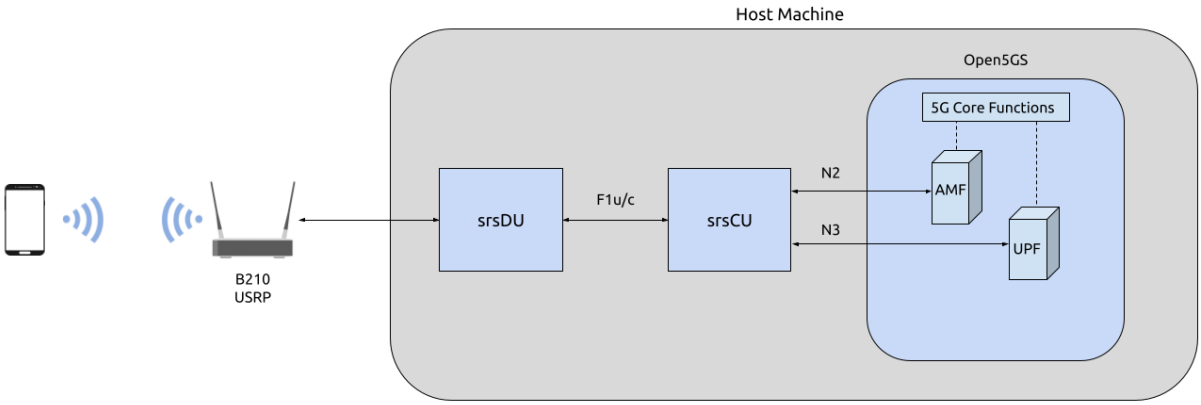

Abbildung 9: Kommunikation zwischen srsRANs DU und CU sowie Open5GS.

4.4 Authentifizierungsprozess in einem privaten 5G-Netzwerk

In einem privaten 5G-Netzwerk ist die Authentifizierung des User Equipment (UE) ein zentraler Prozess, der sicherstellt, dass nur autorisierte Geräte Zugriff auf die Netzwerkinfrastruktur erhalten. Der folgende Abschnitt beschreibt den Authentifizierungsablauf basierend auf der Kommunikation zwischen den Kernnetzwerkfunktionen wie AMF (Access and Mobility Management Function), AUSF (Authentication Server Function), UDM (Unified Data Management), und dem UE. Die Implementierung erfolgt mit Open5GS und SRSRAN.

4.4.1 Ablauf und Interaktionen

Anfrage und Weiterleitung:

- Das gNB (Next Generation Node B) empfängt die Authentifizierungsantwort vom UE und leitet diese an die AMF weiter.

Anfrage an den Authentifizierungsserver:

- Die AMF sendet eine Anfrage an die AUSF, um die Authentifizierung des UE zu bestätigen.

Authentifizierungsbestätigung:

- Die AUSF überprüft die Anfrage, bestätigt die Authentifizierung und übermittelt den Authentifizierungserfolg an die UDM. Die UDM gibt die Bestätigung an die UDR weiter.

Rückmeldung an die AMF:

- Die AUSF sendet den Authentifizierungserfolg zurück an die AMF.

Auswahl von Sicherheitsalgorithmen:

- Basierend auf den in der Registrierungsanfrage gesendeten UE-Fähigkeiten wählt die AMF die Integritäts- und Verschlüsselungsalgorithmen aus.

Security Mode Command:

- Die AMF sendet das "Security Mode Command" an das UE, um die Konfiguration der Sicherheitsparameter zu initiieren.

Schlüsselgenerierung und Überprüfung:

- Das UE führt die Schlüsselgenerierung für Verschlüsselung und Integritätsschutz durch. Es überprüft die Integrität des erhaltenen "Security Mode Command".

Abschluss der Sicherheitskonfiguration:

- Das UE sendet eine Nachricht „Sicherheitsmodus abgeschlossen“ zurück an das gNB, wodurch die Authentifizierung erfolgreich abgeschlossen wird.

Die obige Beschreibung wird in der folgenden Abbildung verdeutlicht, die den Kommunikationsfluss zwischen den Netzwerkkomponenten (gNB, AMF, AUSF, UDM und UE) darstellt.

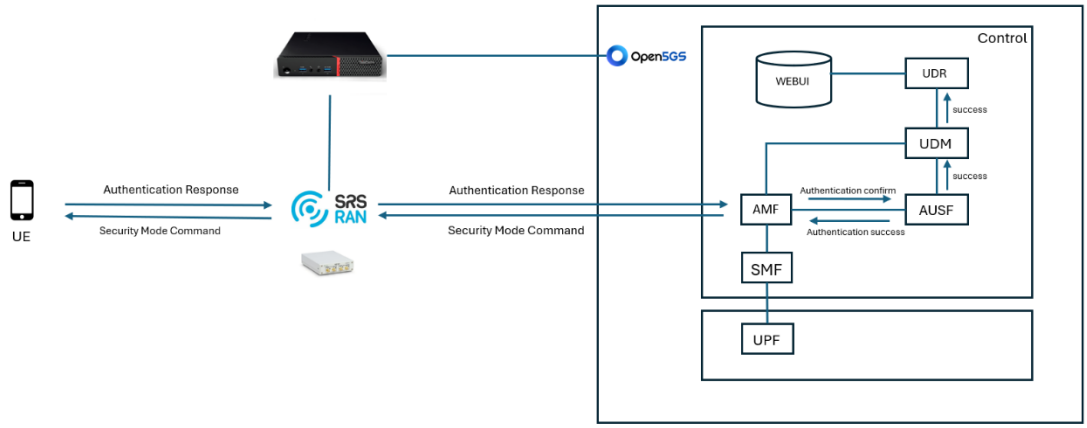

Abbildung 10: Kommunikationsfluss zwischen den Netzwerkkomponenten

5. Testen von 5G-Sicherheitsfunktionen

Die Sicherheitsfunktionen im 5G-Netzwerk spielen eine zentrale Rolle bei der Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie der Authentifizierung von Nutzern. Um sicherzustellen, dass diese Funktionen ordnungsgemäß implementiert und vor potenziellen Bedrohungen geschützt sind, ist das Testen der Sicherheitsmechanismen unerlässlich. In diesem Kapitel werden die Strategien und Methoden zur Entwicklung eines umfassenden Testsystems für die Sicherheitsüberprüfung in 5G-Netzwerken erläutert.

5.1 Überblick über Testmethoden und Strategien

Das Testen von 5G-Sicherheitsfunktionen erfordert einen strukturierten und umfassenden Ansatz, der sowohl generische Sicherheitsanforderungen als auch spezifische Testanforderungen für die verschiedenen Netzwerkfunktionen (NFs) im 5G-System abdeckt. Diese Tests basieren auf den von 3GPP entwickelten Testkatalogen, die detaillierte Sicherheitsanforderungen festlegen. Generische Testfälle konzentrieren sich auf allgemeine Sicherheitsaspekte, wie die Verschlüsselung von Daten, die Authentifizierung und den Schutz vor bekannten Angriffen, beispielsweise Denial-of-Service (DoS). Auf der anderen Seite betreffen spezifische Testfälle einzelne Netzwerkfunktionen wie die AMF (Access and Mobility Management Function) und SMF (Session Management Function), die eine wesentliche Rolle in der 5G-Netzarchitektur spielen.

Die Security Assurance Specification (SCAS) ist eine zentrale Komponente dieser Teststrategie und auch für 5G relevant. Der SCAS-Testkatalog für 5G enthält eine umfassende Sammlung von allgemeinen Sicherheitsanforderungen, die auf verschiedene Komponenten des 5G-Netzwerks angewendet werden. Diese Anforderungen stellen sicher, dass Sicherheitsfunktionen korrekt implementiert und getestet werden. TS 33.117 ist der Katalog, der generische Sicherheitsanforderungen für Netzwerke festlegt, während SCAS eine detaillierte Anleitung dazu bietet, wie diese Anforderungen spezifisch auf Netzwerkprodukte wie die AMF und SMF in 5G angewendet werden können.

Das Ziel bei der Entwicklung und Durchführung der Testfälle war es, festzustellen, ob die Testfälle automatisierbar sind und ob sie regelmäßig und schnell durchgeführt werden können. Automatisierte Testfälle bieten den großen Vorteil, dass sie wiederholt und konsistent ausgeführt werden können, was besonders in einem komplexen und dynamischen Umfeld wie 5G von entscheidender Bedeutung ist. Durch die Automatisierung der Testfälle können wir die Effizienz steigern und sicherstellen, dass Änderungen im Netzwerk zeitnah und zuverlässig auf Sicherheitsanforderungen überprüft werden.

5.2 Entwicklung von Testfällen nach 3GPP

5.2.1 Identifikation relevanter Testfälle

Die Identifikation relevanter Testfälle basiert auf den Anforderungen und Spezifikationen aus den 3GPP-Testkatalogen. Die Testfälle in unserem Testsystem decken sowohl generische Sicherheitstestfälle als auch spezifische Testfälle für die Netzwerkfunktionen AMF und SMF ab. In Zusammenarbeit mit TÜVIT haben wir eine Tabelle erstellt, die die Testfälle nach ihrer Automatisierbarkeit kategorisiert. Die untenstehende Tabelle 3 gibt einen Überblick über die bisher entwickelten und im Testsystem implementierten Testfälle.

Die Tabelle enthält sowohl spezifische Testfälle für die AMF (33.512) und SMF (33.515) als auch eine Vielzahl generischer Testfälle aus dem 3GPP TS 33.117-Katalog, die sicherstellen, dass das gesamte 5G-Netzwerk umfassend auf Sicherheitslücken geprüft wird.

Testfälle	Testkatalog
TC_NAS_INT_SELECTION_USE_AMF	AMF(33.512)
TC_UP_POLICY_PRECEDENCE_SMF	SMF(33.515)
TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFIKATION	TS 33.117
TC_IP_FWD_DISABLING	TS 33.117
TC_PROXY_ARP_DISABLING	TS 33.117
TC_BROADCAST_ICMP_HANDLING	TS 33.117
TC_SYN_FLOOD_PREVENTION	TS 33.117
TC_RESTRICTED_DATA_INFO_TRANSFER	TS 33.117
TC_BVT_PORT_SCANNING	TS 33.117
TC_BVT_VULNERABILITY_SCANNING	TS 33.117
TC_NO_UNUSED_HTTP_METHODS	TS 33.117

Tabelle 3: Übersicht der 5G-Sicherheits-Testfälle gemäß 3GPP-Katalog

Die Testfälle wurden so ausgewählt, dass sie die wichtigsten Sicherheitsaspekte abdecken. Dazu gehören der Schutz vor Angriffen auf die Authentifizierungsprotokolle, die Verwaltung der Netzwerkressourcen und die Absicherung der Datenübertragung. Ein besonderes Augenmerk wurde auf die Testfälle gelegt, die sich mit der Sicherheit der Kernnetzwerkfunktionen AMF und SMF befassen, da diese in der 5G-Netzarchitektur eine entscheidende Rolle spielen.

Zusätzlich haben wir die 3GPP-Tests danach kategorisiert, ob sie automatisierbar sind oder nicht. Dies ermöglicht es uns, diejenigen Tests hervorzuheben, die regelmäßig und effizient im Rahmen eines automatisierten Testsystems durchgeführt werden können. Um den ersten Teil unseres Projekts vorzustellen, haben wir 11 Testfälle ausgewählt, die in Tabelle 3 aufgeführt sind. Diese Testfälle sind im Testsystem implementiert und dienen als Grundlage für die laufende Sicherheitsüberprüfung des 5G-Netzwerks.

Durch diese Identifikation relevanter Testfälle wird sichergestellt, dass alle kritischen Sicherheitsanforderungen des 5G-Netzwerks abgedeckt sind. Die regelmäßige

Durchführung und Automatisierung dieser Testfälle ermöglicht es, potenzielle Schwachstellen frühzeitig zu identifizieren und Sicherheitsrisiken zu minimieren.

Für die generischen Testfälle haben wir die Amarisoft Call Box Mini verwendet, die ein vollständiges 5G-Netzwerk bereitstellt. Dies ermöglichte es uns, verschiedene grundlegende Sicherheitsfunktionen zu testen, einschließlich der Überprüfung der Datenintegrität, Authentifizierung und Verschlüsselung in einem simulierten 5G-Umfeld.

Für die spezifischen Testfälle, die sich auf die Network Functions (NFs) wie AMF (Access and Mobility Management Function) und SMF (Session Management Function) beziehen, haben wir auf Open5GS, ein Open-Source-5G-Core-Netzwerk, zurückgegriffen. Diese Lösung bietet eine flexible und anpassbare Umgebung, in der alle wesentlichen 5G-Kernnetzfunktionen wie AMF, SMF, UPF, UDM und andere Komponenten konfiguriert und getestet werden können.

Um den gNB (gNodeB) und die UE (User Equipment) zu simulieren, wurde UERANSIM eingesetzt, das uns erlaubt, die Interaktionen zwischen den Funkzugangskomponenten und dem Kernnetzwerk zu testen. Die Wahl von Open5GS und UERANSIM bietet mehr Flexibilität und Anpassungsmöglichkeiten als die Verwendung der Amarisoft Call Box Mini, insbesondere für die spezifischen Testfälle, da hier eine vollständige Simulation und Konfiguration der Kernkomponenten möglich ist.

5.3 Implementierung und Durchführung von Sicherheitstests

5.3.1 Testumgebungen und Tools

Für die Durchführung der Sicherheitstests wurde eine umfassende Testumgebung entwickelt, die auf einer Automatisierung mit Python basiert. Zur Automatisierung der Testfälle wird das leistungsstarke und vielseitige Robot Framework verwendet, das speziell für Testautomatisierung und Robotic Process Automation (RPA) entwickelt wurde.[19]

Robot Framework ist ein Open-Source-Framework, das sich durch folgende Eigenschaften auszeichnet:

- **Benutzerfreundliche Syntax:** Die schlüsselwortbasierte Syntax ist leicht lesbar und bietet eine klare Struktur, was die Erstellung und Wartung von Testfällen vereinfacht.
- **Erweiterbarkeit:** Das Framework unterstützt die Integration von Bibliotheken, die in Python, Java oder anderen Programmiersprachen entwickelt werden können. Dadurch kann es flexibel an verschiedene Testanforderungen angepasst werden.
- **Nahtlose Integration:** Es lässt sich mit einer Vielzahl von Tools und Technologien kombinieren, ohne dass Lizenzkosten anfallen.
- **Starke Community:** Eine aktive Entwickler-Community und zahlreiche Drittanbieter-Bibliotheken erweitern die Funktionalitäten des Frameworks erheblich und ermöglichen den Einsatz in unterschiedlichsten Projekten.

In der entwickelten Testumgebung wurden insgesamt 11 automatisierte Testfälle implementiert, die sowohl generische Sicherheitstestfälle als auch spezifische Testfälle für 5G-Netzwerkfunktionen wie AMF und SMF abdecken. In letzten Abschnitt werden einige der wichtigsten Testfälle beschrieben, um die Umsetzung und Zielsetzung des Testsystems zu verdeutlichen.

Zusätzlich wurde eine grafische Benutzeroberfläche (GUI) entwickelt, um das Testsystem benutzerfreundlich zu gestalten. Die Anwendung wurde mit Python, Tkinter und der modernen Designbibliothek ttkbootstrap entwickelt, wodurch ein ansprechendes und intuitives Interface gewährleistet wird.

Die erste Version der Anwendung bietet den Nutzern folgende Funktionen:

- Auswahl zwischen spezifischen Testfällen und generischen Testfällen.
- Anzeige von Logs und Berichten, die vom Robot Framework nach dem Ausführen der Testfälle automatisch erstellt werden.
- Direkte Anzeige der Testergebnisse in Form von Pass oder Fail, um den Erfolg oder das Scheitern eines Tests schnell nachvollziehen zu können.

Diese flexible und skalierbare Umgebung erlaubt eine effiziente und zuverlässige Validierung der Sicherheitstests gemäß den Anforderungen aus den 3GPP-Testkatalogen.

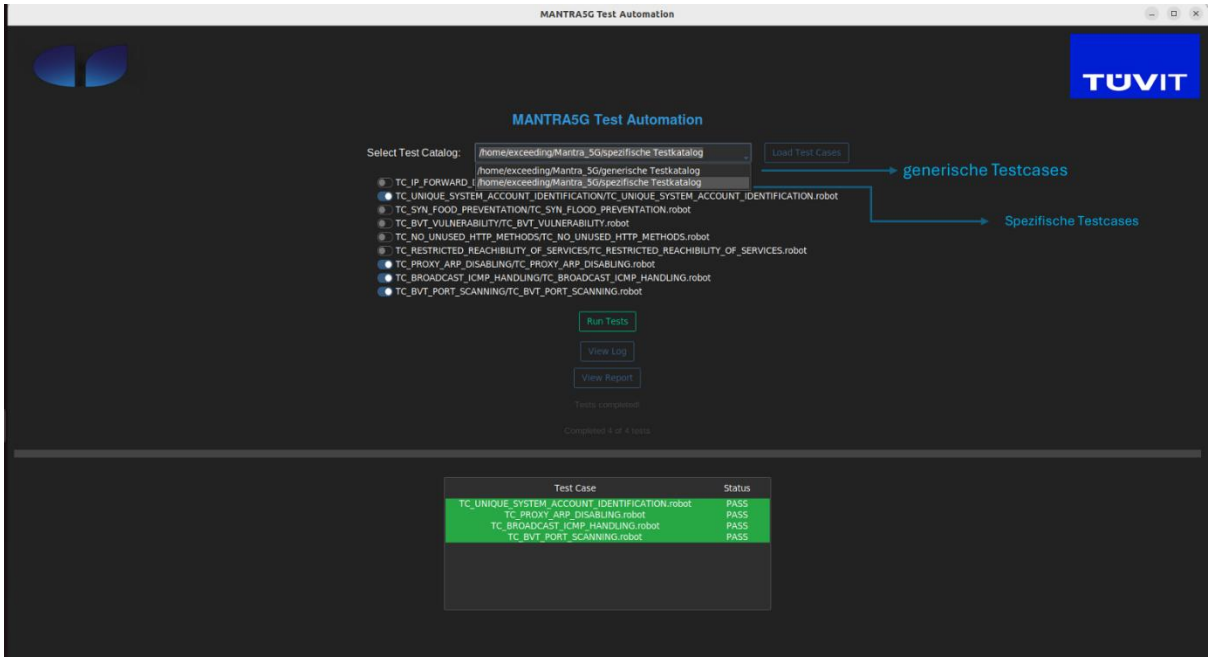

Abbildung 11: Auswahl und Ausführung generischer 5G-Testfälle.

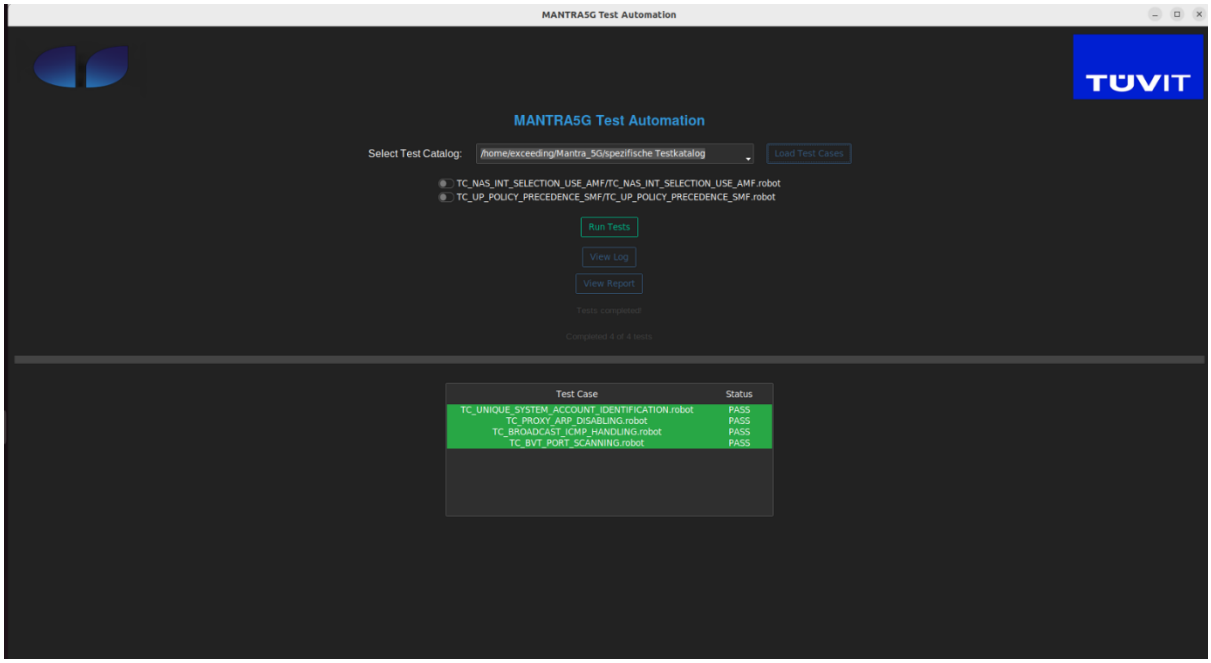

Abbildung 12: Spezifische 5G-Testfälle für AMF und SMF.

5.3.2 Auswertung und Analyse der Testergebnisse

Nach der Durchführung der Tests erfolgt eine gründliche Auswertung und Analyse der Testergebnisse. Die Automatisierung mit Robot Framework ermöglicht die Erstellung detaillierter Berichte, die folgende Informationen enthalten:

- Erfolgs- oder Fehlerstatus (Pass/Fail) für jeden Testfall.
- Log-Dateien, die den genauen Ablauf der Testfälle dokumentieren.
- Reports oder andere Zusatzinformationen, die bei einem Fehlschlag zur Fehleranalyse beitragen.

Die Testergebnisse werden strukturiert dargestellt, um Schwachstellen oder Probleme im System frühzeitig zu erkennen. Insbesondere bei fehlerhaften Testfällen kann der Tester die Berichte nutzen, um genaue Einblicke in den Fehler zu erhalten und gezielt Verbesserungen vorzunehmen.

Durch die Integration der Testergebnisse in das Testsystem wird sichergestellt, dass potenzielle Sicherheitslücken frühzeitig identifiziert und behoben werden können. Die automatische Protokollierung und das Reporting bieten eine hohe Transparenz und Nachvollziehbarkeit, was insbesondere bei umfangreichen Tests und kontinuierlicher Integration von großer Bedeutung ist.

Dieser strukturierte Ansatz zur Testimplementierung und Durchführung gewährleistet nicht nur eine effiziente Validierung der Sicherheitsanforderungen, sondern ermöglicht auch eine einfache Skalierung und Wartung des Testsystems.

5.3.3 Testfallbeschreibung und Design

1. **TC_NAS_INT_SELECTION_USE_AMF**

Der Zweck dieses Tests besteht darin, sicherzustellen, dass die AMF (Access and Mobility Management Function) in der Lage ist, den geeigneten NAS-Integritätsalgorithmus für die Kommunikation mit dem UE (User Equipment) korrekt auszuwählen. Dieser Test ist besonders wichtig, da die Auswahl des richtigen Integritätsalgorithmus eine entscheidende Rolle bei der Sicherstellung der

Datensicherheit in 5G-Netzwerken spielt. Der NAS-Integritätsalgorithmus dient dazu, die Integrität der NAS-Nachrichten zu gewährleisten, die zwischen dem UE und der AMF ausgetauscht werden. Er verhindert, dass diese Nachrichten während der Übertragung modifiziert oder manipuliert werden, was ein wesentlicher Schutzmechanismus gegen Man in the Middle Angriffe (MITM) darstellt. Bei einem MITM-Angriff könnte ein Angreifer versuchen, sich unbemerkt zwischen die Kommunikation zu schalten und Nachrichten zu verändern. Der NAS-Integritätsalgorithmus erkennt solche Manipulationen und sorgt dafür, dass manipulierte Nachrichten als ungültig verworfen werden.[20]

Der Test zielt darauf ab, zu überprüfen, ob die AMF den NAS-Integritätsalgorithmus mit der höchsten Priorität wählt, basierend auf einer vordefinierten Liste von unterstützten Algorithmen. Diese Liste der Integritätsalgorithmen wird sowohl auf der AMF als auch auf dem UE konfiguriert. In einem sicheren 5G-Netzwerk ist es entscheidend, dass die AMF den Algorithmus wählt, der sowohl vom UE als auch von der Netzwerkinfrastruktur unterstützt wird und die höchste Priorität aufweist, um die bestmögliche Sicherheitsstufe zu gewährleisten. Nur so kann sichergestellt werden, dass die Kommunikation vor Angriffen geschützt ist.

Darüber hinaus überprüft der Test, ob der von der AMF ausgewählte NAS-Integritätsalgorithmus tatsächlich während der Kommunikation verwendet wird. Dies bedeutet, dass die Integrität der Nachrichten durch den gewählten Algorithmus gesichert ist und die Nachrichten auf der Empfängerseite ordnungsgemäß validiert werden. Falls ein Angreifer versuchen sollte, Nachrichten während der Übertragung zu manipulieren, sorgt der Integritätsalgorithmus dafür, dass diese Manipulation erkannt und die Nachrichten als ungültig verworfen werden. Dies verhindert nicht nur MITM-Angriffe, sondern stellt auch sicher, dass die Datenintegrität zu jedem Zeitpunkt aufrechterhalten bleibt.

Ein weiteres Ziel dieses Tests besteht darin, die Flexibilität der AMF bei der Verwaltung der Liste der NAS-Integritätsalgorithmen zu überprüfen. Der Tester hat die Möglichkeit, die Reihenfolge der Integritätsalgorithmen auf der AMF zu ändern und zu beobachten, ob die AMF weiterhin in der Lage ist, den richtigen Algorithmus auszuwählen und zu verwenden, selbst wenn sich die Prioritäten in der Liste ändern. Dies stellt sicher, dass die AMF auch in unterschiedlichen Netzwerkszenarien

konsistent arbeitet, was für die Aufrechterhaltung der Netzwerksicherheit von wesentlicher Bedeutung ist.

Insgesamt soll dieser Test sicherstellen, dass die AMF in einem realen 5G-Netzwerkumfeld die NAS-Integritätsalgorithmen korrekt verwaltet und verwendet, um die Sicherheitsziele der Datenintegrität und des Manipulationsschutzes zu erreichen. Da die Integrität der Kommunikation im NAS-Protokoll entscheidend ist, trägt dieser Test maßgeblich dazu bei, die Robustheit und Sicherheit des 5G-Kernnetzes zu validieren und die Infrastruktur vor Man-in-the-Middle-Angriffen zu schützen.

- **5G Verschlüsselungsalgorithmen:**

NEA0: Kennung 0000. Dieser Algorithmus bietet keine Verschlüsselung, da der Schlüsselstrom nur aus Nullen besteht. Im Wesentlichen wird der Klartext nicht verschlüsselt, sodass NEA0 keinerlei Sicherheit bietet.

128-NEA1: Kennung 0001. Ein auf 128-bit SNOW 3G basierender Algorithmus, der als wortorientierter Stromchiffre arbeitet. Nach der Initialisierung des Schlüssels wird ein Schlüsselstrom aus 32-Bit-Wörtern erzeugt.

128-NEA2: Kennung 0010. Ein auf 128-bit AES basierender Algorithmus, der im CTR-Modus (Counter Mode) arbeitet. Obwohl AES ein Blockchiffre ist, macht der CTR-Modus daraus effektiv einen Stromchiffre. Dieser Modus ermöglicht eine parallele Verarbeitung und Vorberechnung des Schlüsselstroms. Wenn der Eingabetext kürzer ist, werden die zusätzlichen Bits des letzten Schlüsselstromblocks verworfen. Eine Auffüllung des Eingabetextes ist nicht erforderlich.

128-NEA3: Kennung 0011. Ein auf 128-bit ZUC basierender Algorithmus, der als Stromchiffre arbeitet.[21]

- **5G Integritätsalgorithmen:**

NIA0: Kennung 0000. Dieser Algorithmus bietet keine Integritätsschutz. Der generierte MAC (Message Authentication Code) besteht ausschließlich aus Nullen,

und der Empfänger überprüft diesen nicht. Es besteht kein Schutz vor Wiederholungsangriffen.

128-NIA1: Kennung 0001. Ein auf 128-bit SNOW 3G basierender Algorithmus.

128-NIA2: Kennung 0010. Ein auf 128-bit AES basierender Algorithmus, der im CMAC-Modus (Cipher based Message Authentication Code) arbeitet.

128-NIA3: Kennung 0011. Ein auf 128-bit ZUC basierender Algorithmus.

Diese Algorithmen gewährleisten die Vertraulichkeit und Integrität der Kommunikationsdaten im 5G-Netzwerk, indem sie sowohl die Verschlüsselung als auch den Schutz vor Manipulationen sicherstellen.[21]

Testverfahren und Ausführungsschritte:

Dieser Testfall wird innerhalb unserer 5G-Testumgebung mit der Open5GS-Core Implementierung und srsRAN als gNB und UE-Simulator durchgeführt. Ziel ist es, zu überprüfen, ob die AMF (Access and Mobility Management Function) den höchst priorisierten NAS-Integritätsalgorithmus entsprechend der Konfiguration auswählt.

Vorbereitungen:

Die AMF.yaml Datei wird entsprechend konfiguriert, um die Reihenfolge der Ciphering und Integritätsalgorithmen festzulegen. Dies gewährleistet, dass die AMF die richtigen Prioritäten kennt.

Eine PDU-Session wird aufgebaut, um die N1 und N2 Schnittstellen zwischen UE, gNB und der AMF zu initialisieren.

Für die Paketanalyse wird Wireshark oder tshark verwendet, um die Nachrichten zwischen den Komponenten aufzuzeichnen und auszuwerten.

Durchführungsschritte:

- **Registrierungsanforderung senden:**

Das UE sendet eine Registrierungsanfrage an die AMF, um den Verbindungsaufbau zu initialisieren.

- **Nachricht aufzeichnen:**

Die Security Mode Command Complete-Nachricht, die während des Authentifizierungsprozesses von der AMF zurückgesendet wird, wird mit Wireshark/tshark aufgezeichnet und gespeichert.

- **Analyse der Algorithmen:**

Aus der Nachricht werden der von der AMF gewählte NAS-Integritätsalgorithmus und die UE Security Capabilities ausgelesen. Die Auswahl des Algorithmus erfolgt gemäß der in der AMF.yaml-Datei definierten Reihenfolge und den unterstützten Sicherheitsfunktionen des UE.

Erwartetes Ergebnis:

Der von der AMF gewählte Algorithmus entspricht dem am höchsten priorisierten NAS-Integritätsalgorithmus in der Konfiguration und den UE Security Capabilities.

Die UE Security Capabilities sind korrekt in der Nachricht enthalten und validiert.

Dieser Test validiert, dass die Sicherheitsmechanismen der AMF wie erwartet funktionieren und die Sicherheit der NAS-Nachrichten gemäß den Konfigurationen gewährleistet ist.

Open

amf.yaml [Read-Only]
/etc/open5gs

```
logger:
  file:
    path: /var/log/open5gs/amf.log
#  level: info   # fatal|error|warn|info(default)|debug|trace

global:
  max:
    ue: 1024  # The number of UE can be increased depending on memory size.
#    peer: 64

amf:
  sbi:
    server:
      - address: 127.0.0.5
        port: 7777
    client:
#      nrf:
#        - uri: http://127.0.0.10:7777
      scp:
        - uri: http://127.0.0.200:7777
  ngap:
    server:
      - address: 127.0.0.5
  metrics:
    server:
      - address: 127.0.0.5
        port: 9090
  guami:
    - plmn_id:
        mcc: 999
        mnc: 70
      amf_id:
        region: 2
        set: 1
  tai:
    - plmn_id:
        mcc: 999
        mnc: 70
      tac: 1
  plmn_support:
    - plmn_id:
        mcc: 999
        mnc: 70
      s_nssai:
        - sst: 1
  security:
    integrity_order : [ NIA2, NIA1, NIA0 ]
    ciphering_order : [ NEA0, NEA1, NEA2 ]
  network_name:
    full: Open5GS
    short: Next
  amf_name: open5gs-amf0
  time:
#    t3502:
#      value: 720   # 12 minutes * 60 = 720 seconds
    t3512:
      value: 540    # 9 minutes * 60 = 540 seconds

###########################################################################
# SBI Server
###########################################################################
```

AMF.yaml in open5gs

Abbildung 13: Konfiguration der AMF.yaml-Datei in Open5GS

Die Datei legt die Einstellungen für die AMF (Access and Mobility Management Function) fest, einschließlich der Priorisierung von Integritätsalgorithmen (integrity_order) und Verschlüsselungsalgorithmen (ciphering_order). Diese Parameter bestimmen die Sicherheitsmechanismen für die NAS-Nachrichten im 5G-Netzwerk.

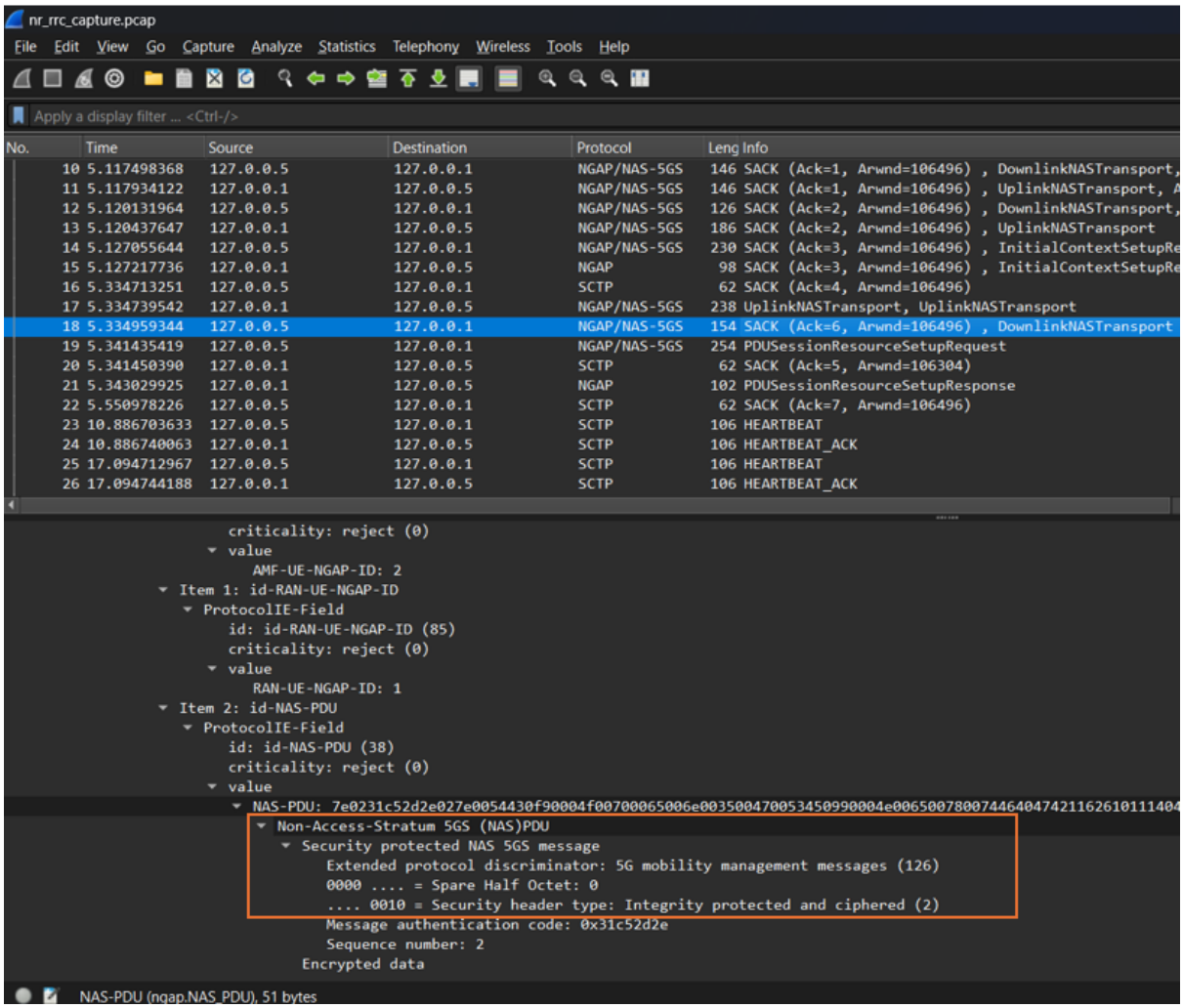

Abbildung 14: Wireshark-Analyse eines NAS-PDU-Sicherheitsheaders

Die Abbildung 12 zeigt, dass der NIA2 Algorithmus (Kennung 0010) im Sicherheitsheader für die Integritätsprüfung der NAS-Nachricht verwendet wird. Dieser auf 128-bit AES basierende Algorithmus, der im CMAC-Modus arbeitet, stellt sicher, dass die Nachricht während der Übertragung nicht manipuliert wurde. Zusätzlich zeigt der Header an, dass die Nachricht verschlüsselt ist, wodurch der Inhalt vor unbefugtem Zugriff geschützt wird. Diese Mechanismen gewährleisten ein hohes Maß an Sicherheit für die Kommunikation im 5G-Netzwerk.

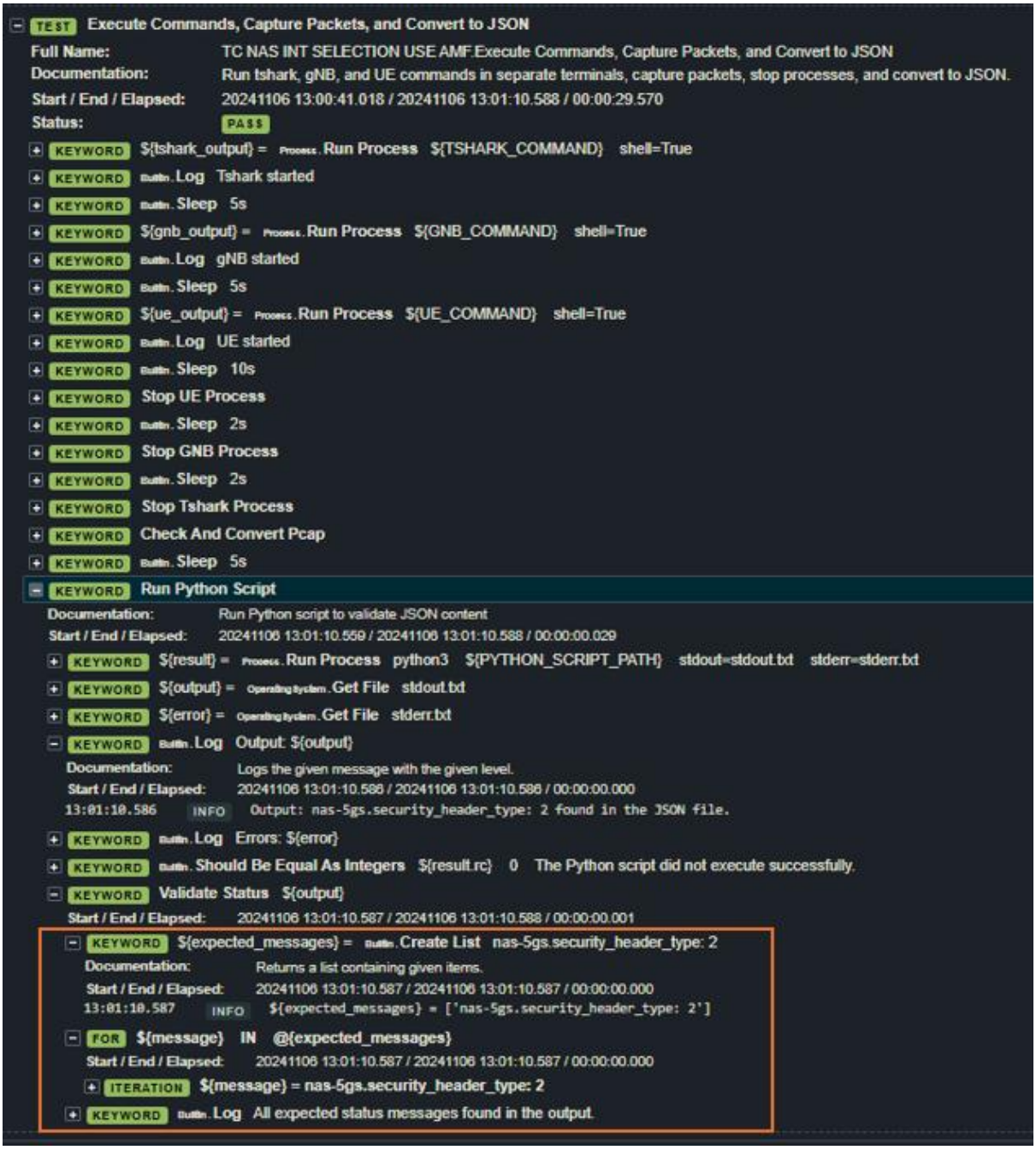

Abbildung 15: Log-Datei des Robot Framework

Der Test automatisiert die Erstellung einer PDU-Session, verbindet das UE mit dem gNB, und etabliert die N1 und N2 Schnittstellen. Die erfassten Netzwerkpakete werden in JSON umgewandelt, und ein Python-Skript analysiert den JSON-Output, um die verwendeten Sicherheitsalgorithmen zu identifizieren. Der Test überprüft, ob die Sicherheitsheader die Algorithmen 128-NIA2 für Integrität und 128-NEA2 für Verschlüsselung verwenden.

2. TC_UP_POLICY_PRECEDENCE_SMF

Der Testfall TC_UP_POLICY_PRECEDENCE_SMF hat zum Ziel, sicherzustellen, dass die User Plane (UP) Sicherheitsrichtlinien, die im UDM (Unified Data Management) gespeichert sind, in der SMF (Session Management Function) Vorrang gegenüber lokal konfigurierten Richtlinien haben. Da die User Plane für die Übertragung von Nutzerdaten zuständig ist, ist es wichtig, dass die Sicherheitsrichtlinien korrekt angewendet werden, um die Integrität und Vertraulichkeit der Daten zu gewährleisten.

Die SMF verwaltet die Sitzungen und die User Plane, während das UDM die zentralen Netzwerkkonfigurationen und Sicherheitsrichtlinien bereitstellt. Dieser Test stellt sicher, dass die SMF die vom UDM bereitgestellten Sicherheitsrichtlinien korrekt abruft und anwendet, und dass diese zentralen Vorgaben Vorrang vor lokal konfigurierten Richtlinien haben. Andernfalls könnten unsichere oder veraltete Richtlinien die Sicherheit des Netzwerks gefährden.[22]

Die User Plane Security Policy legt fest, ob die Nutzerdaten der User Plane innerhalb der PDU-Sitzung geschützt übertragen werden sollen. Diese Richtlinien steuern den Vertraulichkeitsschutz und den Integritätsschutz der übertragenen Daten:

Vertraulichkeitsschutz (UP confidentiality protection) kann wie folgt festgelegt werden:

- **required:** Vertraulichkeitsschutz ist zwingend erforderlich.
- **preferred:** Vertraulichkeitsschutz wird empfohlen.
- **not needed:** Vertraulichkeitsschutz ist nicht erforderlich.

Integritätsschutz (UP integrity protection) kann ebenso konfiguriert werden:

- **required:** Integritätsschutz ist zwingend erforderlich.
- **preferred:** Integritätsschutz wird empfohlen.
- **not needed:** Integritätsschutz ist nicht erforderlich.

Die User Plane Security Policies können entweder lokal in der SMF über DNN (Data Network Name) und S-NSSAI (Single-Network Slice Selection Assistance Information) konfiguriert oder zentral vom UDM bereitgestellt werden. Es ist wichtig, dass die vom

UDM gelieferten Richtlinien Vorrang haben, um die Sicherheit des Netzwerks zu gewährleisten.

Auswirkungen der User Plane Security Policy

Die Auswahl der User Plane Security Policy wirkt sich direkt auf die PDU-Sitzung aus. Wenn die Basisstation eine PDU-Sitzung aufbaut, wendet sie die von der SMF bereitgestellte Security Policy an, um die Datenübertragung zu schützen. Diese Richtlinie wird der gNB (gNodeB) von der SMF zur Verfügung gestellt, die sicherstellt, dass die Übertragungen gemäß den festgelegten Sicherheitsvorgaben geschützt werden.

Schlüsselaspekte des Tests

Abrufen und Anwenden von Sicherheitsrichtlinien: Der Test prüft, ob die SMF die vom UDM bereitgestellten User Plane Sicherheitsrichtlinien abruft und korrekt anwendet, sodass die zentral definierten Richtlinien gegenüber lokal konfiguriertem Vorrang haben.

Durch diesen Test wird sichergestellt, dass keine veralteten oder unsicheren lokalen Richtlinien die zentralen Richtlinien überschreiben. Dies trägt wesentlich dazu bei, die User Plane vor Bedrohungen zu schützen und die Netzwerksicherheit aufrechtzuerhalten.

Fazit

Der Testfall TC_UP_POLICY_PRECEDENCE_SMF stellt sicher, dass die SMF die zentralen User Plane Sicherheitsrichtlinien des UDM korrekt priorisiert. Dies garantiert, dass die Vorgaben für den Vertraulichkeits- und Integritätsschutz in der User Plane einheitlich und zuverlässig angewendet werden und das 5G-Netzwerk vor potenziellen Sicherheitsrisiken geschützt ist.

Testschritte und Vorgehen:

Konfiguration der SMF.yaml-Datei:

In der Konfigurationsdatei der SMF (smf.yaml) werden die Sicherheitsparameter Security Protection Indication und Confidentiality Protection Indication konfiguriert.

Diese Parameter geben an, wie die Sicherheit der User Plane im 5G-Kernnetzwerk umgesetzt werden soll.

```
pfcp:
  server:
    - address: 127.0.0.4
  client:
    upf:
      - address: 127.0.0.7
gtpc:
  server:
    - address: 127.0.0.4
gtpu:
  server:
    - address: 127.0.0.4
metrics:
  server:
    - address: 127.0.0.4
      port: 9090
session:
  - subnet: 10.45.0.0/16
    gateway: 10.45.0.1
  - subnet: 2001:db8:cafe::/48
    gateway: 2001:db8:cafe::1
dns:
  - 8.8.8.8
  - 8.8.4.4
  - 2001:4860:4860::8888
  - 2001:4860:4860::8844
mtu: 1400
#  p-cscf:
#    - 127.0.0.1
#    - ::1
#  ctf:
#    enabled: auto    # auto(default)|yes|no
freeDiameter: /etc/freeDiameter/smf.conf
security_indication:
  integrity_protection_indication: required
  confidentiality_protection_indication: required
  maximum_integrity_protected_data_rate_uplink: maximum-UE-rate
  maximum_integrity_protected_data_rate_downlink: maximum-UE-rate
########################################################################
# SMF Info
########################################################################
```

Abbildung 16: Konfiguration der SMF.yaml-Datei in Open5GS

Mithilfe eines Robot Framework-Skripts wird zunächst eine PDU-Session aufgebaut, bei der die N1- und N2-Schnittstellen zwischen dem UE (User Equipment) und dem gNB (Next Generation Node B) aktiviert werden. Während dieser PDU-Session werden die ausgetauschten Pakete erfasst und im PCAP-Format gespeichert, um die

Kommunikation zwischen den Netzwerkfunktionen abzubilden. Anschließend werden diese PCAP-Dateien durch das Robot Framework in das JSON-Format umgewandelt, um die Daten einfacher analysieren zu können. Für die Analyse wird ein Python-Skript namens Json.py verwendet, das die JSON-Daten auf die konfigurierten Parameter überprüft. Dabei wird sichergestellt, dass die in der SMF-Konfigurationsdatei angegebenen Werte für Security Protection Indication und Confidentiality Protection Indication korrekt implementiert wurden.

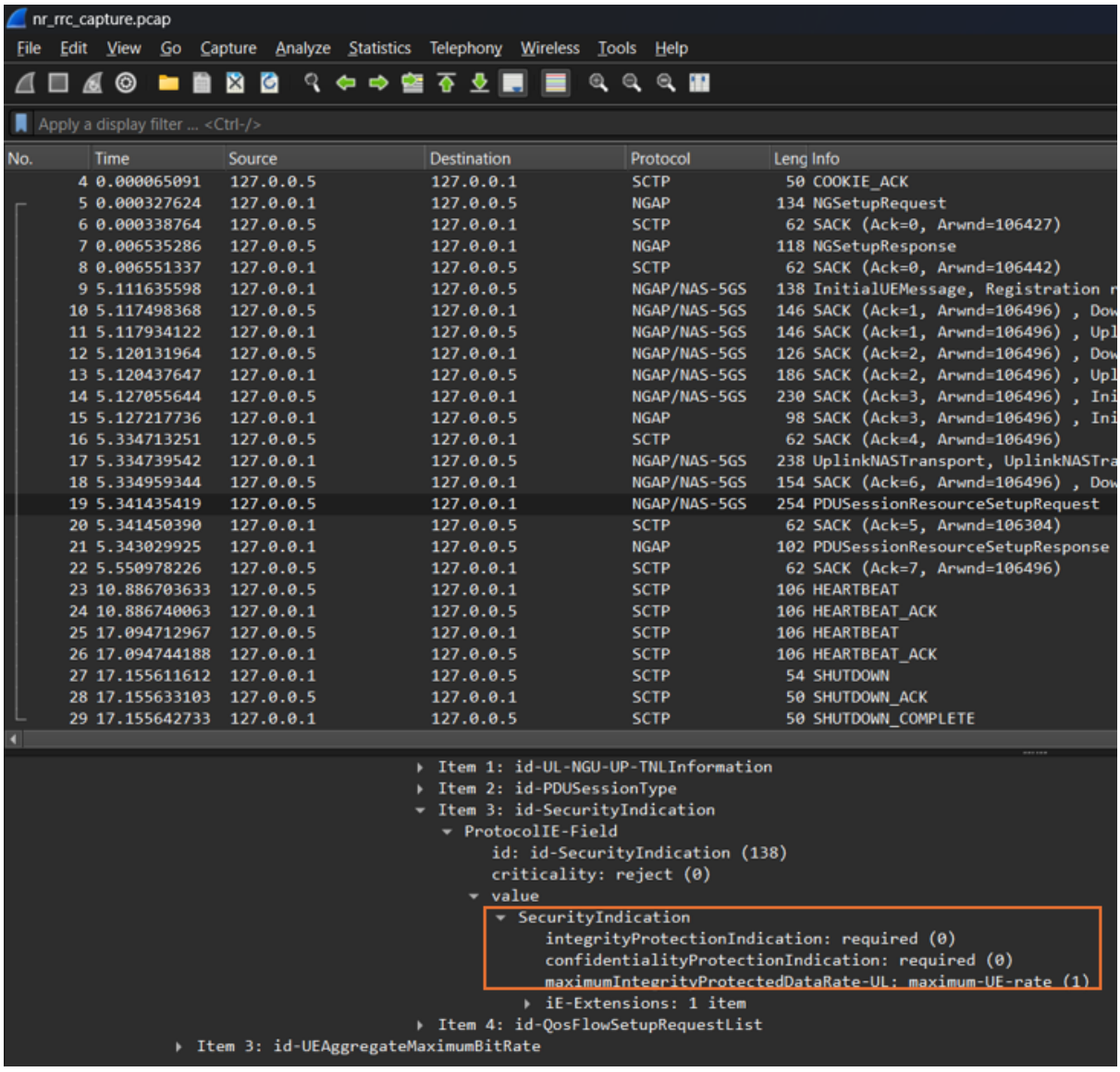

Abbildung 17: Wireshark-Analyse zur Überprüfung der Sicherheitsparameter

Validierung:

Der Test besteht, wenn die erfassten Sicherheitsparameter in den JSON-Daten mit den Anforderungen übereinstimmen. Falls die Parameter nicht korrekt oder unvollständig sind, schlägt der Test fehl.

Wichtige Validierungspunkte:

Security Protection Indication: Überprüft, ob die Sicherheitsmechanismen (z. B. Verschlüsselung) korrekt angewendet wurden.

Confidentiality Protection Indication: Validiert, ob die Vertraulichkeit der Daten sichergestellt ist.

Erwartetes Ergebnis:

Der Testfall wird bestanden, wenn die SMF die Sicherheitsparameter wie konfiguriert implementiert. Andernfalls zeigt der Test einen Fehler an, der auf eine Fehlkonfiguration oder eine fehlerhafte Implementierung hinweist.

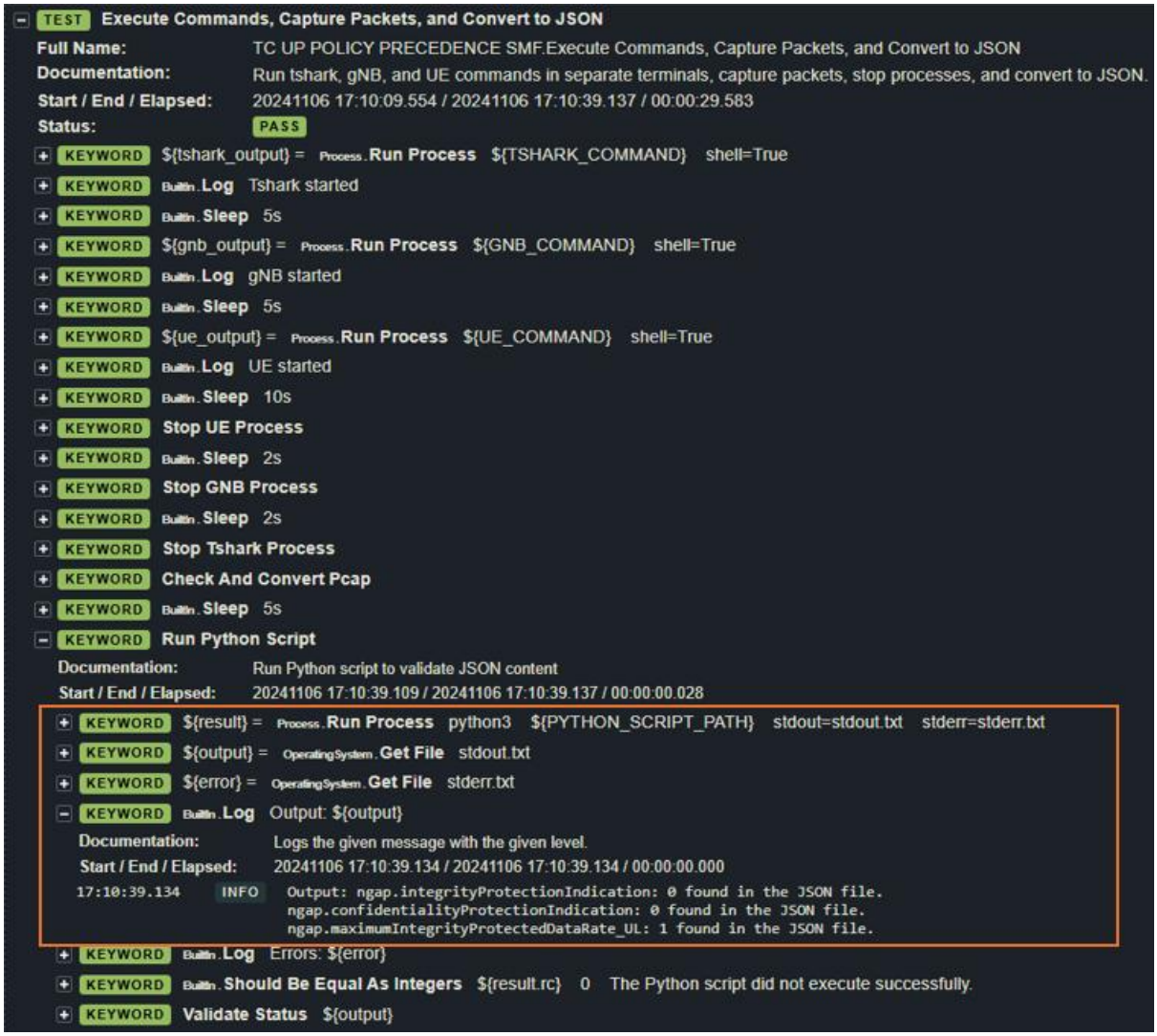

Abbildung 18: Log-Datei des Testfalls TC_UP_POLICY_PRECEDENCE_SMF.

Das Log-File zeigt die Ergebnisse des Testfalls TC_UP_POLICY_PRECEDENCE_SMF, der überprüft, ob die Sicherheitsparameter für Security Protection Indication und Confidentiality Protection Indication korrekt angewendet wurden. Im Ergebnis wurde festgestellt, dass beide Parameter den Wert 0 aufweisen, was bedeutet, dass der Modus required gewählt wurde. Dies stellt sicher, dass sowohl Vertraulichkeitsschutz als auch Integritätsschutz zwingend aktiviert sind.

3. TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFICATION

Dieser Test überprüft, dass jedem UNIX- Benutzerkonto eine eindeutige User ID (UID) zugewiesen wird. Dies ist essenziell für die Sicherheits- und Zugriffsverwaltung in Linux- und UNIX- basierten Systemen. Es wird sichergestellt, dass keine doppelten UIDs vorhanden sind und insbesondere, dass nur das Root-Konto die UID 0 besitzt, da diese besondere Systemprivilegien verleiht.[23]

UID (User Identifier) ist eine numerische Kennung, die jedes Benutzerkonto eindeutig identifiziert. Sie wird verwendet, um Benutzer zu unterscheiden und deren Berechtigungen im System festzulegen. Die UID übernimmt mehrere wichtige Aufgaben:

- **Zugriffsverwaltung**: Sie definiert die Berechtigungen und den Zugriff auf Dateien und Systemressourcen.
- **Prozessmanagement**: Sie verknüpft laufende Prozesse mit dem Benutzer, der sie gestartet hat.
- **Benutzeridentifizierung**: Bei der Anmeldung überprüft das System die UID zur Authentifizierung.
- **Eigentum an Dateien**: Jede Datei und jedes Verzeichnis hat eine UID, die den Eigentümer festlegt.

Zusätzlich ist die UID mit der GID (Group Identifier) verknüpft, welche die Zugehörigkeit zu einer bestimmten Benutzergruppe festlegt. Durch die Kombination von UID und GID können Linux-Systeme Berechtigungen für Benutzer und Gruppen verwalten.[24]

Besonders relevant ist das Root-Konto:

- Der Benutzername ist "root".
- Das Zeichen "x" zeigt an, dass das Passwort in der Datei /etc/shadow gespeichert ist.
- UID und GID 0 sind beide exklusiv dem Root-Konto zugewiesen.
- Das Heimatverzeichnis des Root-Kontos befindet sich unter /root.

Testverfahren und Ausführungsschritte:

1. Erstellen von Benutzerkonten: Mehrere UNIX®-Benutzerkonten im System erstellen.
2. Überprüfen der UIDs: Die UIDs der erstellten Benutzer sowie die vorhandenen Systemkonten, insbesondere des Root-Kontos, überprüfen.

Erwartete Ergebnisse:

- Alle UIDs im System sind eindeutig.
- Nur das Root-Konto hat die UID 0.

TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFICATION.robot

```
*** Settings ***
Library  SSHLibrary
Resource    ../../resources/variables.robot


*** Test Cases ***
Verify TOE Configuration
    Open Connection  ${HOST}  port=${PORT}
    Login  ${USERNAME}  ${PASSWORD}
    ${passwd_content}  Execute Command  cat /etc/passwd
    Log Many  ${passwd_content}  # Display the contents of /etc/passwd for verification

    # Extract the line for the root user
    ${root_line}  Evaluate  [line for line in '''${passwd_content}'''.splitlines() if line.startswith("root:")][0]

    # Extract UID and GID for the root user
    ${uid}  Evaluate  '''${root_line}'''.split(':')[2]
    ${gid}  Evaluate  '''${root_line}'''.split(':')[3]

    # Verify that both UID and GID are 0
    Should Be Equal As Numbers  ${uid}  0
    Should Be Equal As Numbers  ${gid}  0

    # Add more steps for additional verification or interaction with TOE

    Close All Connections

```

Abbildung 19: Testfall TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFICATION

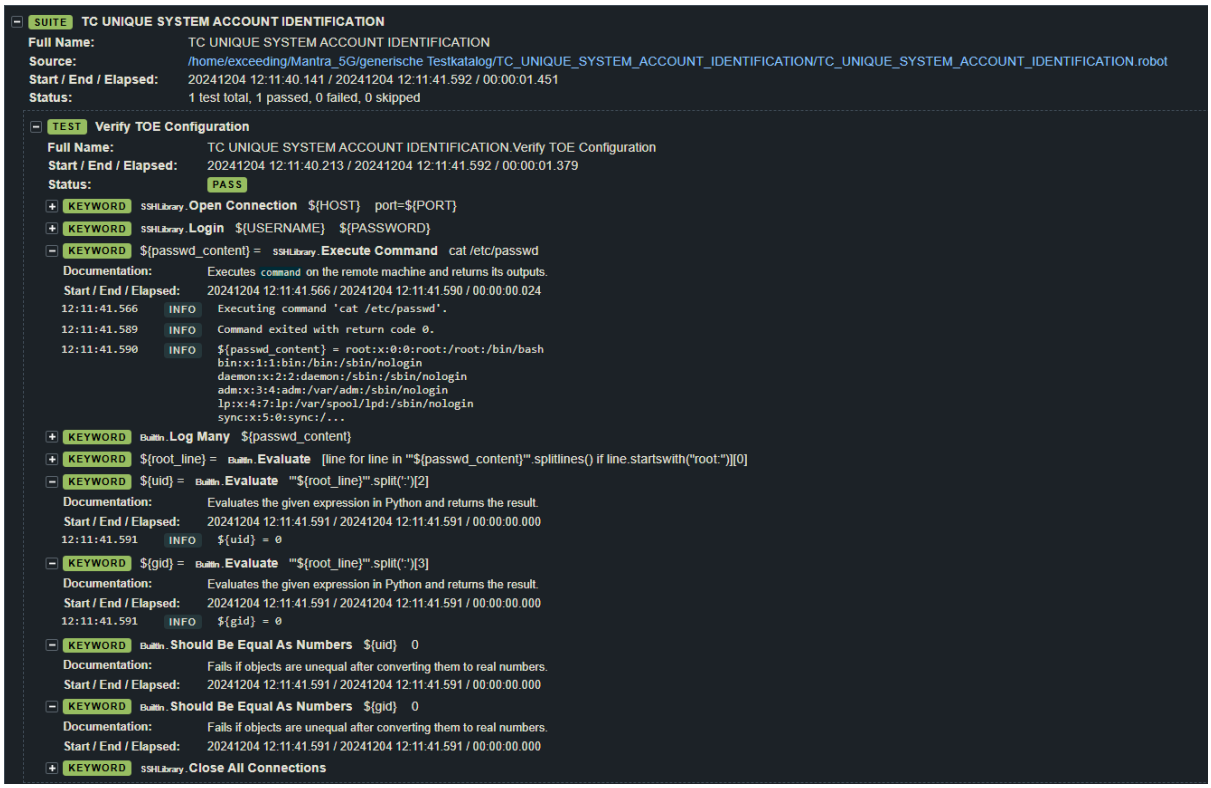

Abbildung 20: Log von TC_UNIQUE_SYSTEM_ACCOUNT_IDENTIFICATION.

4. TC_NO_UNUSED_HTTP_METHODS

HTTP-Methoden bieten verschiedene Funktionen, um Webserver und Webanwendungen anzusprechen. Jede HTTP-Methode ermöglicht spezifische Aktionen, wie das Abrufen, Senden oder Löschen von Daten. Wenn unnötige HTTP-Methoden aktiviert bleiben, können sie als potenzielle Angriffsvektoren dienen, durch die Schwachstellen in das System eingeführt werden. Cyberkriminelle nutzen oft ungesicherte Methoden aus, um Angriffe wie Cross-Site Scripting (XSS), Remote Code Execution (RCE) oder Man-in-the-Middle-Angriffe durchzuführen. Daher ist es essenziell, dass Webserver nur die HTTP-Methoden aktivieren, die für die Funktion der Anwendung notwendig sind, um die Angriffsfläche zu minimieren.

Beschreibung der HTTP-Methoden

- **GET**:
  Diese Methode wird verwendet, um Informationen vom Server anzufordern, ohne dabei Daten zu verändern. GET ist sicher und idempotent, was bedeutet, dass es mehrfach ausgeführt werden kann, ohne den Zustand des Servers zu verändern. GET ist eine Standardmethode und für die meisten Webanwendungen erforderlich.

- **HEAD**:
  HEAD funktioniert ähnlich wie GET, mit dem Unterschied, dass es nur die Header-Informationen ohne den Nachrichtentext zurückgibt. Diese Methode wird häufig für Statusprüfungen von Ressourcen verwendet und ist nützlich, wenn man die Existenz einer Ressource überprüfen möchte, ohne deren Inhalt zu übertragen.

- **POST**:
  POST wird verwendet, um Daten an den Server zu senden, wie z. B. das Einreichen von Formularen. Diese Methode ist nicht idempotent, da sie den Zustand des Servers ändert. Sie ist eine der wichtigsten Methoden, die für interaktive Webanwendungen benötigt wird.

- **PUT**:
  PUT wird verwendet, um eine Ressource auf dem Server zu erstellen oder zu aktualisieren. Da diese Methode den Zustand des Servers verändert, sollte sie nur aktiviert werden, wenn der Server wirklich eine derartige Funktionalität benötigt, beispielsweise bei RESTful APIs.

- **DELETE**:
  Die DELETE-Methode wird verwendet, um Ressourcen auf dem Server zu löschen. Obwohl diese Methode für manche Anwendungen nützlich ist, stellt sie auch ein Sicherheitsrisiko dar, wenn sie nicht ordnungsgemäß geschützt ist. Daher sollte sie nur aktiviert werden, wenn sie wirklich erforderlich ist und entsprechende Sicherheitsmechanismen vorhanden sind.

- **PATCH**:
  PATCH wird verwendet, um Teildaten einer Ressource zu aktualisieren.

Ähnlich wie PUT kann diese Methode den Zustand des Servers ändern und sollte nur aktiviert werden, wenn sie für die Funktion der Webanwendung notwendig ist.[25]

- **TRACE**:
  TRACE wird verwendet, um die Route, die eine Anfrage durchläuft, zu verfolgen. Diese Methode stellt ein Sicherheitsrisiko dar, da sie Informationen über den Kommunikationsweg offenlegen kann. Dadurch könnte ein Angreifer sensible Daten abfangen und verwenden, um Angriffe wie Cross-Site Tracing (XST) zu starten. Aus diesem Grund sollte TRACE immer deaktiviert sein.[26]
- **TRACK**:
  TRACK ist eine Methode, die ähnlich wie TRACE funktioniert und oft für Debugging-Zwecke verwendet wird. Diese Methode ist anfällig für Sicherheitslücken und kann zu Cross-Site Scripting (XSS)-Angriffen führen. Daher sollte TRACK auf modernen Webservern immer deaktiviert sein.[26]

Das Deaktivieren ungenutzter HTTP-Methoden minimiert die Angriffsfläche eines Webservers. Jede aktivierte HTTP-Methode stellt einen potenziellen Angriffspunkt dar, den ein Angreifer ausnutzen könnte. Insbesondere Methoden wie TRACE oder TRACK sind häufig Ziele von Sicherheitsangriffen, da sie Informationen über die Struktur und den Kommunikationsweg des Servers preisgeben.

Durch das Deaktivieren nicht benötigter Methoden stellt man sicher, dass nur die minimal notwendigen Funktionen des Webservers aktiv sind, was die Möglichkeit von Angriffen reduziert. Dies verringert das Risiko von Sicherheitslücken, die von Angreifern ausgenutzt werden könnten, und verbessert die Gesamtsicherheit der Webanwendung.

Der Zweck dieses Tests besteht darin, zu überprüfen, dass auf dem Webserver alle nicht benötigten HTTP-Methoden deaktiviert sind. Gemäß den Best Practices der Branche sollten nur die für Standard-Webanfragen erforderlichen HTTP-Methoden wie GET, HEAD und POST aktiviert sein. Falls zusätzliche Methoden wie PUT, DELETE oder PATCH benötigt werden, muss sichergestellt werden, dass diese keine

Sicherheitslücken einführen. Besonders gefährdete Methoden wie TRACK oder TRACE dürfen nicht aktiv sein, da sie potenziell schwere Sicherheitsrisiken darstellen können.[23]

Testverfahren und Ausführungsschritte:

Vorbedingungen:

- Der Tester hat die erforderlichen administrativen Berechtigungen.
- Ein Tester-System steht zur Verfügung, von dem aus der Webserver geprüft werden kann.
- Optional: Ein automatisches Bewertungs-Tool oder angepasstes Skript ist eingerichtet, das die Prüfung der HTTP-Methoden automatisiert.

Durchführungsschritte:

1. Überprüfen Sie, ob die relevanten Systemeinstellungen und Konfigurationen so eingestellt sind, dass nur die notwendigen HTTP-Methoden aktiviert und alle nicht benötigten Methoden deaktiviert sind.
2. Verwenden Sie das konfigurierte Assessment-Tool oder führen Sie eine manuelle Überprüfung durch, um sicherzustellen, dass nur die erforderlichen HTTP-Methoden aktiviert sind.

Erwartete Ergebnisse:

- Alle relevanten Systemeinstellungen und Konfigurationen wurden überprüft und sind in einem sicheren Betriebszustand. Es wurde sichergestellt, dass für alle Web-Komponenten des Systems ungenutzte HTTP-Methoden deaktiviert sind.[23]

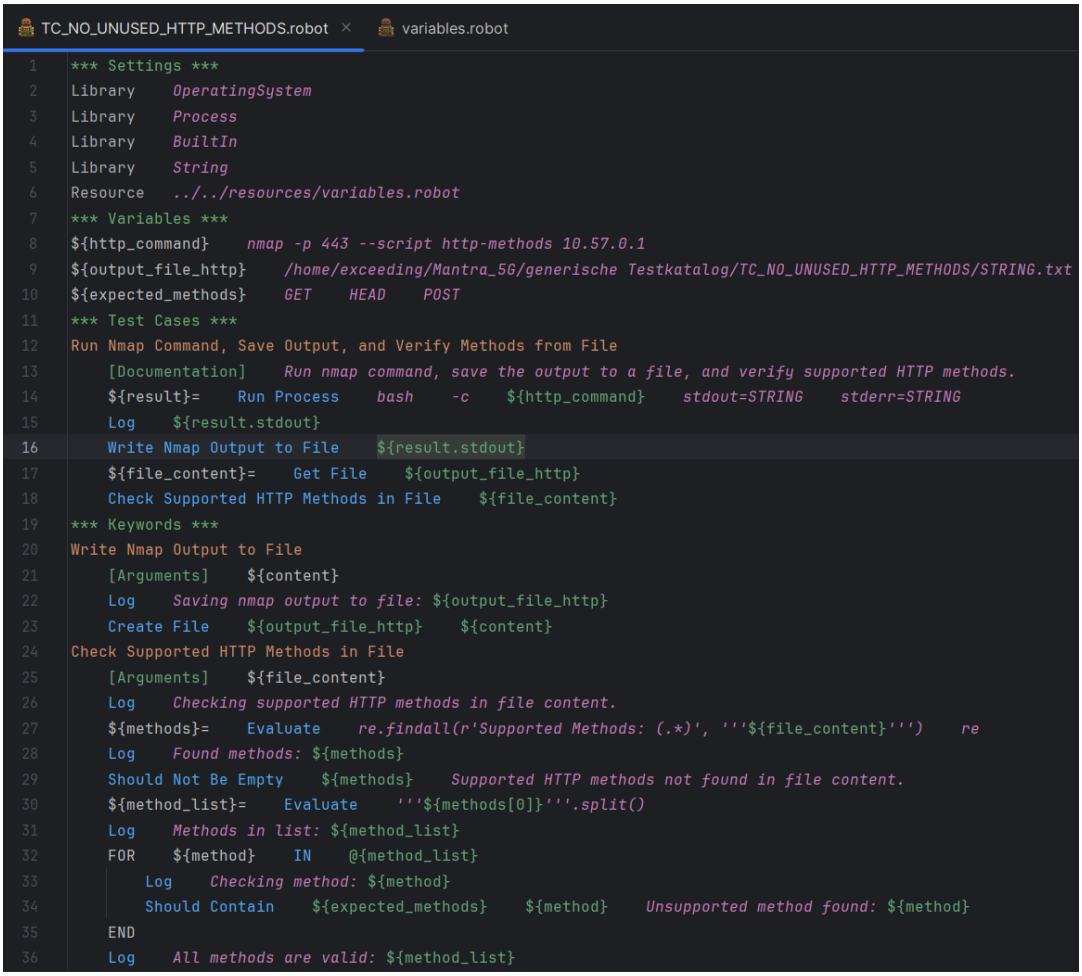

Abbildung 21: Testfall TC_NO_UNUSED_HTTP_METHODS

Der Testfall TC_NO_UNUSED_HTTP_METHODS wurde entwickelt, um sicherzustellen, dass der Server nur die benötigten und erwarteten HTTP-Methoden (GET, HEAD, POST) aktiviert hat, während ungenutzte oder potenziell unsichere Methoden wie PUT, DELETE oder TRACE deaktiviert bleiben. Mithilfe des Tools Nmap wird ein Befehl ausgeführt, um die unterstützten HTTP-Methoden auf dem Server zu ermitteln. Die Ergebnisse werden in einer Datei gespeichert und anschließend durch ein Robot-Framework-Skript analysiert. Dabei werden die gefundenen Methoden mithilfe eines regulären Ausdrucks extrahiert und mit einer Liste erlaubter Methoden verglichen. Dieser Test trägt dazu bei, Sicherheitsrisiken zu minimieren, indem die Angriffsfläche durch deaktivierte ungenutzte Methoden reduziert wird. Die Automatisierung erfolgt mit Robot Framework und Python, um eine effiziente und zuverlässige Durchführung zu gewährleisten.

Abbildung 22: Log-Datei von TC_NO_UNUSED_HTTP_METHODS

5. TC_SYN_FLOOD_PREVENTION

SYN Flood Angriff

Ein SYN-Flood-Angriff ist eine Art von Denial-of-Service (DoS)-Angriff, der auf einen Computerserver abzielt. Diese Angriffsmethode wird auch als Half-Open-Angriff bezeichnet. SYN-Flood-Angriffe gehören zu den häufigsten Schwachstellen, die die TCP/IP-Protokolle ausnutzen, um Zielsysteme zu überlasten. Der Angriff basiert auf dem TCP-Dreiwege-Handshake, einem Prozess, bei dem Client und Server Nachrichten austauschen, um eine Kommunikationsverbindung aufzubauen.

Beim Angriff sendet ein Client wiederholt SYN-Pakete (Synchronisationspakete) an alle Ports eines Servers, wobei gefälschte IP-Adressen verwendet werden. Der angegriffene Server interpretiert dies als eine Vielzahl von Kommunikationsanfragen. Daraufhin antwortet er mit SYN-ACK-Paketen (Synchronisation bestätigt) von allen offenen Ports und sendet RST-Pakete (Reset) von allen geschlossenen Ports, um die vermeintlichen Verbindungsversuche zu bearbeiten.[27]

Der TCP-Dreiwege-Handshake und seine Rolle bei SYN-Flood-Angriffen

Ein TCP-Dreiwege-Handshake umfasst die folgenden drei Schritte:

Der Client sendet ein SYN-Paket an den Server, um die Kommunikation zu initiieren.

Der Server antwortet mit einem SYN-ACK-Paket, um die Synchronisation zu bestätigen. Der Client sendet ein abschließendes ACK-Paket zurück, um zu bestätigen, dass das SYN-ACK-Paket des Servers empfangen wurde. Nach Abschluss dieser drei Schritte wird die Verbindung aufgebaut, und die Kommunikation zwischen Client und Server kann beginnen.

Bei einem SYN-Flood-Angriff kehrt der Angreifer jedoch diesen Prozess um: Der böswillige Client sendet wiederholt SYN-Anfragen an alle Ports des Servers, beantwortet jedoch das SYN-ACK-Paket des Servers nicht mit einem abschließenden ACK-Paket. Stattdessen erkennt der Angreifer, dass ein Port offen ist, wenn der Server mit einem SYN-ACK-Paket antwortet.

Da der Angreifer gefälschte IP-Adressen verwendet, kann der Server die Verbindung nicht schließen, indem er ein RST-Paket (Reset) an den Client sendet. Dadurch bleibt

die Verbindung offen, und bevor ein Timeout auftritt, sendet der Angreifer ein weiteres SYN-Paket. Dies führt zu einer sogenannten halb-offenen Verbindung (Half-Open Connection).

Der Server wird durch diese unvollständigen Verbindungen überlastet, da er Ressourcen für jede vermeintliche Anfrage reserviert. Legitimer Netzwerkverkehr wird dadurch blockiert oder erheblich eingeschränkt, was eine normale Kommunikation nahezu unmöglich macht.

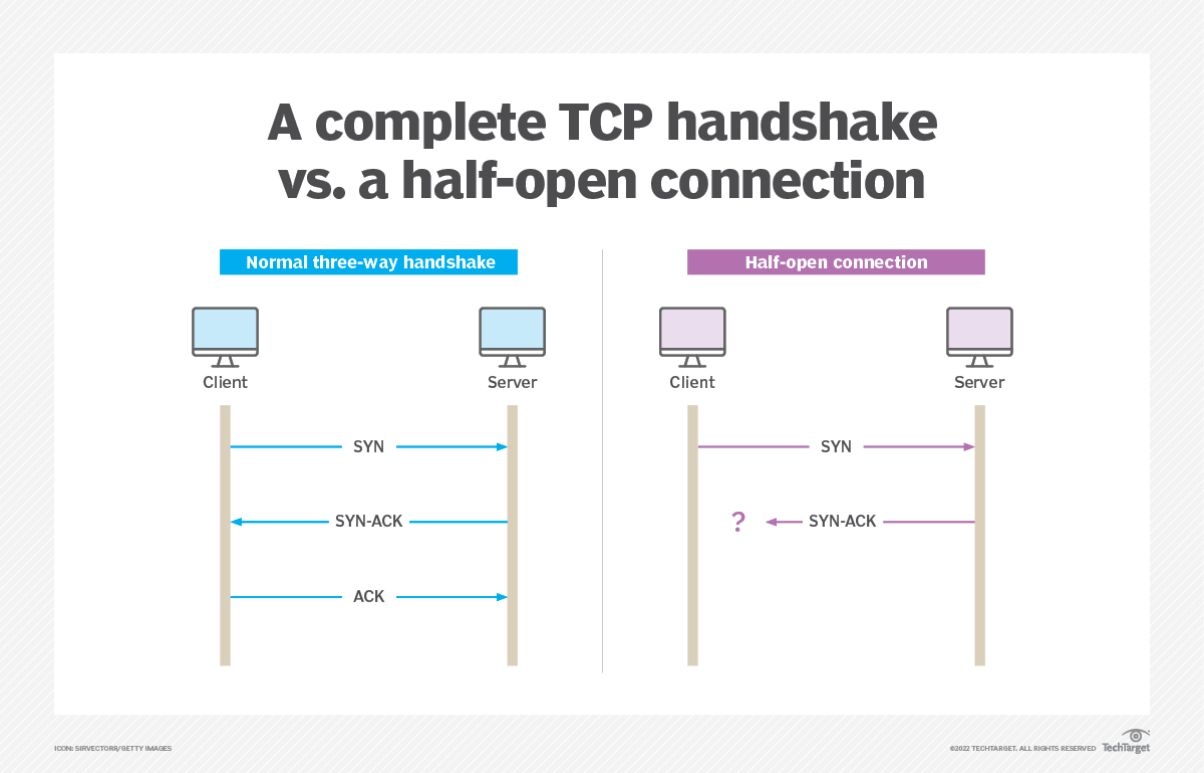

Abbildung 23: TCP-Dreiwege-Handshake vs. halb-offene Verbindung.[27]

Abbildung 5 zeigt den Vergleich zwischen einem normalen TCP-Dreiwege-Handshake und einer halb-offenen Verbindung während eines SYN-Flood-Angriffs. Links wird der vollständige Austausch von SYN, SYN-ACK und ACK-Paketen dargestellt, der zu einer erfolgreichen Verbindung führt. Rechts wird eine halb-offene Verbindung gezeigt, bei der der Angreifer das ACK-Paket nicht sendet, wodurch der Server mit unvollständigen Verbindungen überlastet wird.

SYN-Flood-Angriffe können auf drei verschiedene Arten durchgeführt werden:

Spoofed (IP-Spoofing):

Bei einem gespooften Angriff werden die IP-Adressen in jedem gesendeten SYN-Paket vom Angreifer gefälscht. Dies lässt die Pakete wie legitime Anfragen eines vertrauenswürdigen Servers erscheinen. IP-Spoofing erschwert es, die Herkunft der Pakete zu verfolgen und den Angriff zu entschärfen.

Direct (Direkter Angriff):

Im Gegensatz zu gespooften Angriffen verwendet ein direkter Angriff eine einzige Quelle mit einer realen IP-Adresse. Der Angreifer nutzt ein Gerät, um den Angriff auszuführen. Diese Methode ermöglicht es, die Quelle des Angriffs leichter zurückzuverfolgen und zu blockieren, da die IP-Adresse nicht verschleiert ist.

Distributed (DDoS-Angriff):

Ein Distributed Denial-of-Service (DDoS)-Angriff verwendet ein Botnetz, um die Quelle der schädlichen Pakete auf viele Geräte zu verteilen. Obwohl die Quellen real sind, erschwert die verteilte Natur des Angriffs die Abwehr. Zusätzlich können Geräte im Botnetz ihre IP-Adressen ebenfalls spoofen, was den Angriff weiter verschleiert. Je größer das Botnetz, desto weniger Notwendigkeit besteht, die IP-Adressen zu verschleiern, da die Vielzahl der Geräte den Angriff schwierig zu blockieren macht.

Zweck des Tests:

Der Testfall TC_SYN_FLOOD_PREVENTION dient dazu, die Fähigkeit des Systems zu überprüfen, sich gegen SYN-Flood-Angriffe zu schützen. Diese Angriffe gehören zur Kategorie der Denial-of-Service (DoS)-Angriffe und zielen darauf ab, die Netzwerkressourcen durch eine Flut von TCP-SYN-Paketen zu überlasten. Ziel des Tests ist es, sicherzustellen, dass das System Mechanismen implementiert hat, um solche Angriffe zu erkennen, zu begrenzen und abzuwehren, ohne die Verfügbarkeit für legitime Benutzer zu beeinträchtigen.

Testverfahren und Ausführungsschritte:

Für den Test wird ein Netzwerkprodukt verwendet, das auf einem TCP-Port einer seiner Schnittstellen lauscht. Um den Netzwerkverkehr während des Tests zu überwachen, wird ein Netzwerkanalysetool wie TCPDUMP eingesetzt. Ein Host, der mit der Netzwerkschnittstelle des Produkts verbunden ist, dient als Angriffssimulator und verwendet Tools wie nmap oder hping, um SYN-Flood-Angriffe zu reproduzieren.

Der Tester konfiguriert das Tool, um eine große Anzahl von TCP-SYN-Paketen an das Netzwerkprodukt zu senden. Dazu wird ein Befehl wie der folgende verwendet:

hping3 -i <Wartezeit> -S -p <TCP-Port> -c <Anzahl der Pakete> <IP-Adresse>

Während der Angriff läuft, wird geprüft, ob das Netzwerkprodukt weiterhin stabil und funktional bleibt.

Am Ende des Tests wird erwartet, dass das Netzwerkprodukt auch unter der Last eines SYN-Flood-Angriffs stabil bleibt. Es sollte in der Lage sein, legitimen Datenverkehr weiterhin zu verarbeiten, ohne dass kritische Ressourcen wie Arbeitsspeicher erschöpft werden oder die Systemverfügbarkeit beeinträchtigt wird.

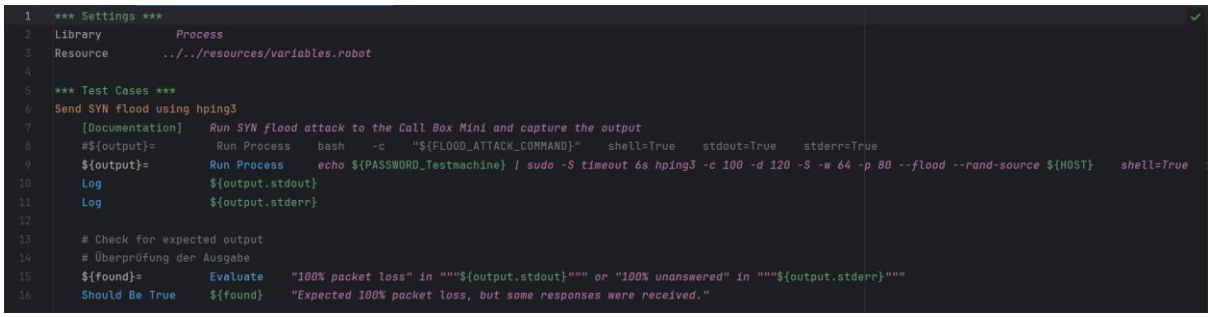

Abbildung 24: Testfall TC_SYN_FLOOD_PREVENTION

Das Robot Framework-Skript führt einen SYN-Flood-Angriff mithilfe des Tools hping3 durch. Der Test prüft, ob der Server erfolgreich auf den Angriff reagiert, indem er keine Antworten auf die gesendeten bösartigen Anfragen zurückgibt. Die Ergebnisse werden im Log analysiert, um sicherzustellen, dass 100 % der Pakete verloren gehen oder unbeantwortet bleiben, was auf die Effektivität der implementierten Sicherheitsmechanismen hinweist.

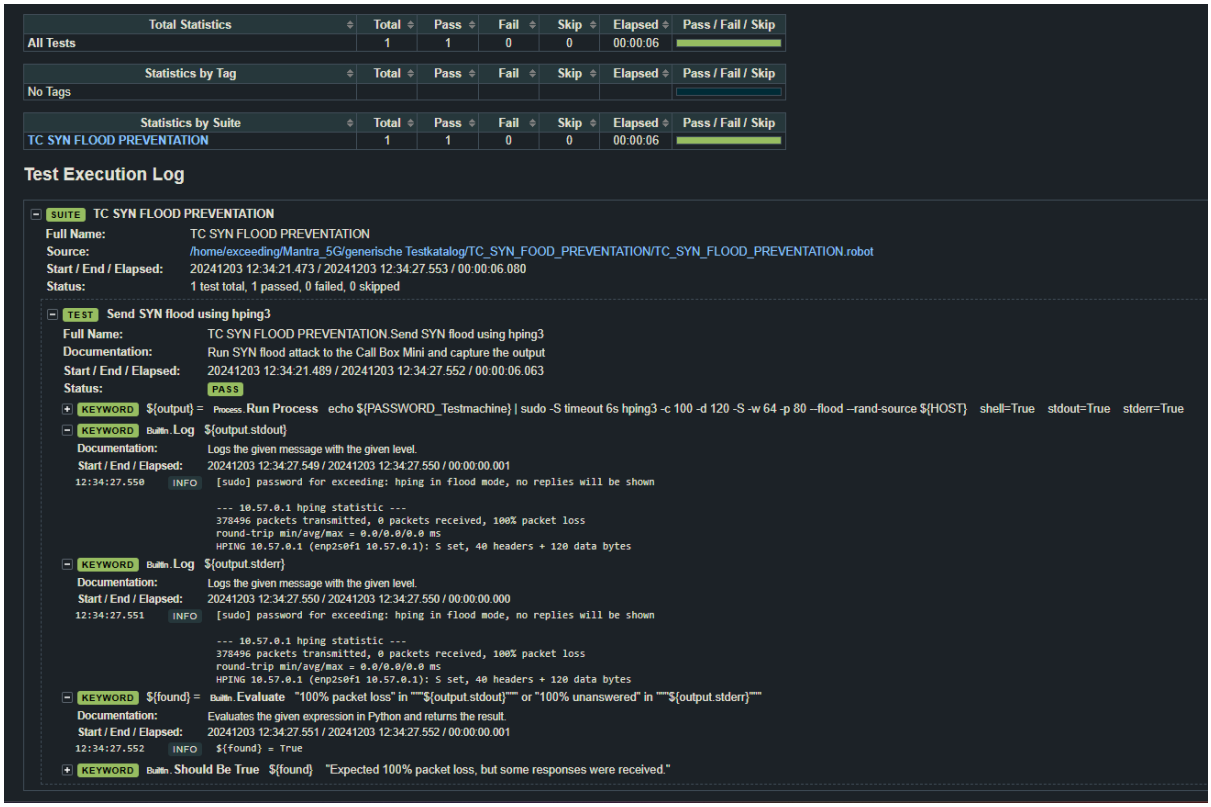

Abbildung 25: Log-Datei des Testfalls TC_SYN_FLOOD_PREVENTATION

Diese Log-Datei zeigt die erfolgreiche Ausführung des Testfalls TC_SYN_FLOOD_PREVENTATION, bei dem ein SYN-Flood-Angriff mithilfe von hping3 auf die Call Box Mini simuliert wurde. Der Test evaluiert die Resilienz des Servers gegen den Angriff, indem überprüft wird, ob alle gesendeten Pakete verloren gehen und keine Antworten auf die bösartigen Anfragen erfolgen. Die Ergebnisse bestätigen 100 % Paketverlust, was darauf hinweist, dass der Server wie erwartet auf den Angriff reagiert hat, ohne inoperative zu werden.

6. Zusammenfassung und Ausblick

6.1 Zusammenfassung der Ergebnisse

In dieser Arbeit wurde ein Testsystem für 5G-Sicherheitsfunktionen entwickelt, das auf einem privaten 5G-Netzwerk basiert. Das Testsystem nutzt Open-Source-Technologien wie Open5GS und srsRAN sowie Hardwarekomponenten wie USRP B210, um eine realistische und kontrollierte Testumgebung zu schaffen. Die entwickelten Testfälle decken sowohl generische Sicherheitsprüfungen als auch spezifische Tests für zentrale 5G-Netzwerkfunktionen wie AMF und SMF ab.

Die Automatisierung der Testfälle mithilfe des Robot Frameworks ermöglichte eine effiziente und systematische Durchführung von Tests. Die Ergebnisse zeigten, dass das Testsystem zuverlässig potenzielle Schwachstellen identifizieren und die Netzwerksicherheit verbessern kann. Durch die Integration von Tools wie Wireshark und hping3 konnten Angriffe simuliert und deren Auswirkungen evaluiert werden, wodurch die Robustheit des Netzwerks unter verschiedenen Szenarien überprüft wurde.

6.2 Empfehlungen und zukünftige Arbeiten

Die in dieser Arbeit erzielten Ergebnisse bilden eine solide Grundlage für zukünftige Weiterentwicklungen, die sowohl die Abdeckung des Testsystems als auch dessen Flexibilität und Skalierbarkeit verbessern können. Eine vielversprechende Erweiterung wäre die Entwicklung weiterer Testfälle aus dem generischen 3GPP-Testkatalog sowie spezifischer Testfälle für zusätzliche 5G-Netzwerkfunktionen wie UPF, UDM und NRF. Damit könnte die Aussagekraft des Testsystems gesteigert und eine umfassendere Prüfung von Netzwerksicherheitsfunktionen ermöglicht werden.

Zusätzlich könnte die Integration von Cloud-Technologien die Skalierbarkeit und Flexibilität des Testsystems erhöhen. Cloud-Dienste könnten beispielsweise dazu genutzt werden, Testergebnisse effizient zu speichern, zu analysieren und zentral zu verwalten. Die Einführung einer Datenbanklösung wie PostgreSQL würde dabei helfen, die Testergebnisse strukturiert und nachvollziehbar zu organisieren und eine langfristige Analyse zu unterstützen.

Darüber hinaus könnte das Testsystem so angepasst werden, dass es neben der Call Box Mini von Amarisoft auch andere 5G-Testplattformen unterschiedlicher Hersteller unterstützt. Diese Anpassung würde die Einsatzmöglichkeiten des Testsystems erweitern und sicherstellen, dass eine größere Bandbreite an Testumgebungen und Szenarien abgedeckt wird. Durch die Berücksichtigung verschiedener 5G-Testplattformen könnten auch Interoperabilitätsprüfungen und Tests unter variierenden Systemkonfigurationen durchgeführt werden, was die Robustheit und Flexibilität des Systems weiter erhöht.

Mit den vorhandenen Hardwarekomponenten, wie dem USRP B210, sowie Open-Source-Softwarelösungen wie Open5GS und srsRAN, könnten zudem realitätsnahe Testszenarien entwickelt werden. Dies schließt die Simulation komplexer Netzwerksituationen und die Implementierung erweiterter Sicherheitsmechanismen ein. Die Erweiterung der Testumgebung würde ermöglichen, auch zukünftige Sicherheitsanforderungen besser abzudecken und eine kontinuierliche Verbesserung der Testprozesse sicherzustellen.

Die Einbindung zusätzlicher 5G-Testplattformen und die Erweiterung der Testumgebung stärken die Flexibilität und die Aussagekraft des entwickelten Testsystems und machen es zukunftsfähig für die dynamischen Anforderungen der 5G-Technologie.

7. Literaturverzeichnis

[1] “Comparison of 2G 3G 4G 5G | 2G vs 3G vs 4G vs 5G | Rantcell.” Accessed: Oct. 11, 2024. [Online]. Available: https://rantcell.com/blog.html

[2] B. E.-D. Helmy, “Mobile Networking: 1G vs. 2G vs. 3G vs. 4G vs. 5G | Baeldung on Computer Science.” Accessed: Oct. 11, 2024. [Online]. Available: https://www.baeldung.com/cs/mobile-networking-generations

[3] G. Brown, “Service-Based Architecture for 5G Core Networks,” [Online]. Available: https://www.3g4g.co.uk/5G/5Gtech_6004_2017_11_Service-Based-Architecture-for-5G-Core-Networks_HR_Huawei.pdf

[4] L. Loureiro, V. Pereira, T. Cruz, and P. Simões, “Evaluating the suitability of eBPF/XDP for securing 5G networks,” 2024, doi: 10.13140/RG.2.2.34665.71527.

[5] “5G AMF UPF SMF PCF UDM DN AUSF AF functions | 5G NR Network Nodes.” Accessed: Oct. 11, 2024. [Online]. Available: https://www.rfwireless-world.com/Terminology/5G-AMF-UPF-SMF-PCF-UDM-functions.html

[6] M. D. Ph.D, “5G Core Network (5GC) Functions - Grandmetric Blog,” Grandmetric. Accessed: Oct. 11, 2024. [Online]. Available: https://www.grandmetric.com/5g-core-network-functions/

[7] “Introducing 3GPP,” 3GPP. Accessed: Oct. 11, 2024. [Online]. Available: https://www.3gpp.org/about-us/introducing-3gpp

[8] “3GPP_Scopeando310807.pdf.” Accessed: Oct. 11, 2024. [Online]. Available: https://www.3gpp.org/ftp/Inbox/2008_web_files/3GPP_Scopeando310807.pdf

[9] P. Filkins, “Private 5G: Empowering Digitalization for Enterprise and Industrial Organizations”, [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/wireless/private-5g/white-paper-sp-idc-empowering-digitalization.pdf

[10] “How is a Private 5G Network Different from a Public 5G Network? | Samsung Business Global Networks,” Samsung global_nw. Accessed: Oct. 11, 2024. [Online]. Available: https://www.samsung.com/global/business/networks/insights/blog/0503-how-is-a-private-5g-network-different-from-a-public-5g-network/

[11] Z. Zhao, “Research on 5G Security Technology for Industrial Internet,” *J. Phys.: Conf. Ser.*, vol. 1966, no. 1, p. 012044, Jul. 2021, doi: 10.1088/1742-6596/1966/1/012044.

[12] J. Cao *et al.*, “A Survey on Security Aspects for 3GPP 5G Networks,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 170–195, 2020, doi: 10.1109/COMST.2019.2951818.

[13] X. Lagrange, “What are the network functions in charge of the security ?,” Coursera. Accessed: Oct. 11, 2024. [Online]. Available: https://www.coursera.org/learn/5g-network-fundamentals/home/welcome

[14] U. Trick, *5G: eine Einführung in die Mobilfunknetze der 5. Generation*. in De Gruyter Oldenbourg STEM. Berlin ; Boston: De Gruyter Oldenbourg, 2020.

[15] E. R. Brand a National Instruments, “USRP B210 USB Software Defined Radio (SDR),” Ettus Research. Accessed: Dec. 14, 2024. [Online]. Available: https://www.ettus.com/all-products/ub210-kit/

[16] E. R. Brand a National Instruments, “Board Mounted GPSDO (TCXO),” Ettus Research. Accessed: Dec. 14, 2024. [Online]. Available: https://www.ettus.com/all-products/gpsdo-tcxo-module/

[17] “O-RAN gNB Overview — srsRAN Project documentation.” Accessed: Dec. 14, 2024. [Online]. Available: https://docs.srsran.com/projects/project/en/latest/knowledge_base/source/oran_gnb/source/index.html

[18] “4g_5g_changes.png (905×490).” Accessed: Dec. 14, 2024. [Online]. Available: https://docs.srsran.com/projects/project/en/latest/_images/4g_5g_changes.png

[19] “Robot Framework.” Accessed: Dec. 06, 2024. [Online]. Available: https://robotframework.org/#resources

[20] “5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF) 33.512.” [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3445

[21] arvindpdmn, “5G Security Algorithms,” Devopedia. Accessed: Oct. 19, 2024. [Online]. Available: https://devopedia.org/5g-security-algorithms

[22] “TS 133 515 - V16.2.0 - 5G; 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class (3GPP TS 33.515 version 16.2.0 Release 16)”.

[23] “TS 133 117 - V16.6.0 - Universal Mobile Telecommunications System (UMTS); LTE; Catalogue of general security assurance requirements (3GPP TS 33.117 version 16.6.0 Release 16)”.

[24] H. Sankar, “What is UID in Linux? How to Find UID of a User and Change it,” Scaler Topics. Accessed: Oct. 20, 2024. [Online]. Available: https://www.scaler.com/topics/linux-uid/

[25] “HTTP request methods - HTTP | MDN.” Accessed: Oct. 20, 2024. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods

[26] “Cross Site Tracing | OWASP Foundation.” Accessed: Oct. 20, 2024. [Online]. Available: https://owasp.org/www-community/attacks/Cross_Site_Tracing

[27] “What is a SYN flood? Definition and How to Prevent Attacks,” Search Security. Accessed: Dec. 03, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/SYN-flooding

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäßen und wörtlich übernommenen Textstellen wurden kenntlich gemacht.

Halle (Saale), 24.02.2025 Khashayar Valadi

Anhang