KYAMBOGO UNIVERSITY

FACULTY OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING

BACHELOR OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING

CYBER SECURITY EVALUATION AND MITIGATION FOR 5G AND FUTURE WIRELESS NETWORKS.

FINAL YEAR INDIVIDAUL PROJECT, EE421

BY:

MUHANGUZI TOBIAS, 15/U/7774/ETE/PE

SUPERVISOR:

MR. KITONE ISAAC

MAY - 2019

PROJECT REPORT IN PARTIAL FULFILLMENT OF REQUIREMENT FORAWARD OF BACHELOR OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING.

DECLARATION

I declare to the best of my knowledge that this Compilation is my original work and no part of it has been submitted at Kyambogo University or elsewhere for a Degree or any other academic award in any other University or institution of Learning".

Sign: _____ Date_____

MUHANGUZI TOBIAS NEWMAN

APPROVAL

I confirm that the project titled “Cyber security evaluation and mitigation for 5G and future wireless networks” was carried out by the candidate under my supervision and has been approved to meet the requirements for the award of a Bachelor of Engineering in Telecommunications Engineering of Kyambogo University, for the completion of fourth year project.

Sign: _____ Date_____

MR. KITONE ISAAC
(PROJECT SUPERVISOR)

DEDICATION

I dedicate this project report to my late father and mother *Mr. Kwatotyo Edward Kareireho RIP* and *Mrs. Kwatotyo Tumwiine Marydovika RIP* who gave me the inspiration to achieve my goals during this project period. I also dedicate this project to my Aunt *Mrs Semambo Angella Kemirembe* who passed on early 2018, RIP, she was a dedicated mother when I had none.

May your souls, rest in eternal peace, you will be missed!

"For God and my Country"

ACKNOWLEDGMENT

I humbly thank the **Almighty God** for granting me life, knowledge and wisdom to accomplish my project and compile this report.

My sincere thanks go to my project supervisor MR. KITONE ISAAC for all the knowledge and advice he provided to me during this period. I also thank my lecturers; Madam Gertrude Kisitu, Mr. Mbiika Ceriano, Mr. Niwareeba Roland, Madam Birabwa Denise, Mr Kuruga Johnson and Mr. Isabirye Gerald (list is endless).

Finally, to my Sponsors the *Indian Women Association Uganda*, for paying my tuition fees, I owe this Degree to you, thank you so much.

May the living God bless you abundantly!

LIST OF ACRONYMS

AES	Advanced Encryption Standard
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AN	Access Network
AS	Access Stratum
AUTN	Authentication token
AV	Authentication Vector
ASME	Access Security Management Entity
Cell-ID	Cell Identity as used in TS 36.331
CK	Cipher Key
CKSN	Cipher Key Sequence Number
C-RNTI	Cell RNTI as used in TS 36.331
CRL	Certificate Revocation List
DeNB	Donor eNB
DoS	Denial of Service
DSCP	Differentiated Services Code Point
EARFCN-DL	E-UTRA Absolute Radio Frequency Channel Number-Down Link
ECM	EPS Connection Management
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
eKSI	Key Set Identifier in E-UTRAN
EMM	EPS Mobility Management
eNB	Evolved Node-B
EPC	Evolved Packet Core
EPS	Evolved Packet System
EPS-AV	EPS authentication vector
E-UTRAN	Evolved UTRAN
gNB	Next Generation Node-B
GERAN	GSM EDGE Radio Access Network

GUTI	Globally Unique Temporary Identity
HE	Home Environment
HFN	Hyper Frame Number
HO	Hand Over
HSS	Home Subscriber Server
IK	Integrity Key
IKE	Internet Key Exchange
IMEI	International Mobile Station Equipment Identity
IMEISV	International Mobile Station Equipment Identity and Software Version number
IMSI	International Mobile Subscriber Identity
IOPS	Isolated E-UTRAN Operation for Public Safety
IRAT	Inter-Radio Access Technology
ISR	Idle Mode Signalling Reduction
KDF	Key Derivation Function
KSI	Key Set Identifier
LWIP	LTE WLAN RAN Level Integration using IPSec
LSB	Least Significant Bit
LSM	Limited Service Mode
LWA	LTE-WLAN Aggregation
MAC-I	Message Authentication Code for Integrity (terminology of TS36.323)
MACT	Message Authentication Code T used in AES CMAC calculation
MeNB	Master eNB
ME	Mobile Equipment
MME	Mobility Management Entity
MME-RN	MME serving the RN
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code for NAS for Integrity (called MAC in TS24.301)
NASDVM	Non Access Stratum - Data via MME
NCC	Next hop Chaining Counter

NH	Next Hop
OCSP	Online Certificate Status Protocol
OTA	Over-The-Air (update of UICCs)
PCI	Physical Cell Identity as used in TS 36.331
PDCP	Packet Data Convergence Protocol
PLMN	Public Land Mobile Network
PRNG	Pseudo Random Number Generator
PSK	Pre-shared Key
P-TMSI	Packet- Temporary Mobile Subscriber Identity
RAND	RANDom number
RAU	Routing Area Update
RN	Relay Node
RRC	Radio Resource Control
SCG	Secondary Cell Group
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SMC	Security Mode Command
SeNB	Secondary eNB
SgNB	Secondary gNB
SN	Serving Network
SN id	Serving Network identity
SQN	Sequence Number
SRB	Source Route Bridge
SRVCC	Single Radio Voice Call Continuity
S-TMSI	S-Temporary Mobile Subscriber Identity
TAI	Tracking Area Identity
TAU	Tracking Area Update
UE	User Equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	Universal Integrated Circuit Card

UMTS	Universal Mobile Telecommunication System
UP	User Plane
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
WT	WLAN Termination as used in TS 36.300
XRES	Expected Response
GSM	Global System for Mobile communications
IMS	International Mobile Subscriber Identifier, used in GSM to identify subscribers
MAC	Message Authentication Code
NAI	Network Access Identifier
secSDLC	Security/Secure systems development life cycle

LIST OF SYMBOLS

|| Concatenation Operator

$\oplus$ Exclusive-OR Operator

K, Ki Encryption or Authentication Key

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

5G is proposed to be launched by 2020 (as per the date of compiling this report, 2018-2019). 5G and other subsequent next generation networks will be characterized by; low latency, improved throughput, low transmit-receive power, and consequently improved QoS. mmwave, MU-MIMO, SDR(C-RAN), MEC, NFV, and SDN are the technologies that have been proposed, with IoT and Cloud computing as the major enablers. Due to softwarization (SDN), and network slicing (NFV), new cyber security threat vectors, are introduced. For 5G to be cloud native and support IoT, will require a proper security architecture, with a strong authentication system to be developed ensuring total QoS. In this report, I have covered;

(1) The basic cyber security concepts, like; risk management, assurance, secSDLC models [11], encryption and ACs models, the 5G, IoT and Cloud computing security architectures/frameworks, and cyber security policy review of Uganda.[1]

(2) For each of the architectures, I shall demonstrate the countermeasures to the threat vectors cited, demonstrate network security techniques, and encryption and authentication algorithms. Countermeasures were classified as, Defensive (Proactive), and Offensive (Reactive). The concept of 5G security was approached in a use case scenario, and building technologies of the access network

[1] https://www.nita.go.ug/sites/default/files/publications/Uganda%20CMM.pdf

CHAPTER ONE: INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The development in IoT (Critical and Massive) and Cloud Computing (deployment and service model) have raised the need for a network the can seamlessly support these services, 5G is both cloud native and support critical/ massive IoT. 2G, 3G and 4G where not developed for these future QoS demands. The major enablers for 5G are; cloud computing and IoT. 5G is on trial in most parts of Africa, including Uganda, as per the time of carrying out this research (2018). There are four fundamental requirements for a modern communication network, which include, Data rate/throughput capacity, processing power of network equipment, Functional Redundancy and ether channels, and most importantly cyber-security, all of which contribute to QoS Realization. Security of huge amounts of data (big data) on 5G, IoT, and Cloud computing networks, should be handled with great concern. Due to the rise of cybercrimes, the field of cyber security has grown in the recent years, with well-defined Common Body of Knowledge (CBK)[2], and approaches.

1.2 PROBLEM STATEMENT

The increasing demands for real-time communication/ streaming 4k videos, gaming , VR, MR and AR and IoT (smart home, smart grid, smart city, v2x) that put a constraint on traditional storage, raising need for cloud computing. The data on a network includes personal health data, agriculture, education, e-government, e-commerce including, the increasing electronic money transfers etc., with the effort of the government to digitize all communication. All these services, and efforts generate huge amounts of data, Big-data, this poses a problem ensuring cyber security. I have singled out cyber-security to be the focus of this paper. The security of data on the network both in transit, and in cloud has to be handled with great concern. 5G is proposed to be rolled-out by 2020, I advocate for a secure architecture, by reviewing the security frameworks and models.

1.3 OBJECTIVES

1.4 GENERAL OBJECTIVE

To carry out Cyber security evaluation and mitigation for future wireless networks, 5G for IoT and cloud computing networks.

[2] https://searchsecurity.techtarget.com/definition/Common-Body-of-Knowledge-CBK

1.4.1 Specific Objectives

- To carry out research on cyber security risk management, models, frameworks, and roadmaps, encryption and authentication algorithms of wireless networks, and Access control models.
- To carry out research on 5G, IoT and Cloud network architecture.
- To develop two MATLAB Applications; one that hinds the characters of a password on login and implements minimum login requirements, and another that generates munged passwords to ensure password hardening and perform ***network security*** hardening and monitoring.
- To carry out research on ***cyber security policies*** both national and international.

1.5 PROJECT JUSTIFICATION AND PROJECT SIGNIFICANCE

The two major enablers for 5G are NFV, and SDN, and is the ideal network for IoT and cloud computing networks. The network virtualization and softwarization introduces new attack vectors that will require different Countermeasures. Therefore, it is worth it, to review the proposed 5G security architecture. Uganda is currently in 5G trial stages. Most start-ups are implementing cloud systems, and IoT systems, like automation of different activities in health, agriculture, power grid, government(CCTV public surveillance cameras) and mobile banking/mobile money and education(e-learning platforms) all of which require a fast connectivity achieved by 5G cellular networks. Security of data should be ensured, hackers can cost a company a great deal of money, reputation, and test its competence to protecting the information of its customers [check: case, https://en.wikipedia.org/wiki/Sony_Pictures_hack]

1.5.1 Project Significance

This study will create a practical understanding of cyber security, policies and practices that include Computer security, Security Systems Software Development Life Cycle (secSDLC), and Network security for the future wireless networks (IoT and Cloud)

1.6 RESEARCH QUESTIONS

1.6.1 General Research Question

How secure is the 5G network, with its complex design for the realization of a sustainable Nextgen system.

1.6.2 Specific Research Questions

How is security implementation in 5G –Next Gen different from the previous generations of 2G, 3G and 4G?

1.7 SCOPE OF THE STUDY

1.7.1 Subject and Content Scope

The following activities were carried out during the course of the project:

1.7.1.1 Cyber security concept research

- Research about (secSDLC), ACs and Cyber Security risk management models.
- Demonstration of Wireless Encryption algorithms, and MUNGED passwords with MATLAB.
- Cyber security policies, including the GDPR and CERT.UG activity review.
- 5G, IoT cyber security and cloud computing network security concerns and countermeasures with focus on; SDN, and Virtualization security.
- 5G security architecture, Cloud computing security architecture, IoT security architecture.

1.7.1.2 Network cyber security

- Penetration testing, social engineering and vulnerability tests with kali Linux for wireless networks (Ethical hacking). [8][9]
- Security in the network layer with Wireshark, Snort (IDS/IPS, honey pots, DNZ) with GNS3 simulation
- Python programming for Security

1.7.2 Geographical scope

The research under taken was only considering 5G network security frameworks being employed around the world and Uganda.

1.7.3 Time Scope

Depending on the scope of the content, the project consumed 5 months from start (research and documentation), through design, programming and testing.

CHAPTER 2: LITERATURE REVIEW

3.1 INTRODUCTION TO 5G NETWORK SECURITY

The vision of the 5G wireless networks lies in providing very high data rates, greater coverage through dense base station deployment with increased capacity, significantly better Quality of Service (QoS), and extremely low latency. 5G is considered to provide broadband access everywhere, entertain higher user mobility, enable connectivity of a massive number of devices running integrated services which are ever evolving and the different operating systems (e.g. IoT, VR, AR, Cloud computing), and the connectivity will be ultra-reliable and affordable to cover and address OpEx and CapEx of industrial players. The development towards an all-IP-based communication, for example in 4G, has already helped develop new business opportunities, provide new online services and connect industrial machines, home appliances and business units. However, with this development, the security challenges and threat vectors have also increased.

Wireless communication systems were prone to security vulnerabilities from the very beginning. In the first generation (1G) wireless networks, mobile phones and wireless channels were targeted for illegal cloning and masquerading. In the second generation (2G) of wireless networks, message spamming became common, not only by pervasive attacks but also by injecting false information or broadcasting unwanted marketing information. In the third generation (3G) wireless networks, IP-based communication enabled the migration of Internet security vulnerabilities and challenges in the wireless domains. With the increased necessity of IP-based communication, the fourth Generation (4G) wireless networks enabled the proliferation of smart devices, multimedia traffic, and new services into the mobile domain. This development lead to a more complicated and dynamic threat landscape. With the advent of the fifth generation (5G) wireless networks, the security threat vectors will be bigger than even before, with greater concerns for privacy.

One haunting fact that has always stayed alive during the development towards the 5G is that the IP-based communication not only increased the variety of services and network traffic but opened new doors to develop new cracking and hacking mechanisms for wireless networks and mobile devices. Wireless networks and user equipment, however, had difficulty in keeping up the pace with the increasing security challenges surfacing due to IP connectivity. Hence, new solutions and technologies have always been sought to protect the network, user traffic and services. In

this chapter, we will provide an overview of the new types of security threats, and then present the solutions proposed for those threats.

3.1.1 The fundamental efforts of cyber security practices

Attributes referred as (CIA Triad) to these data

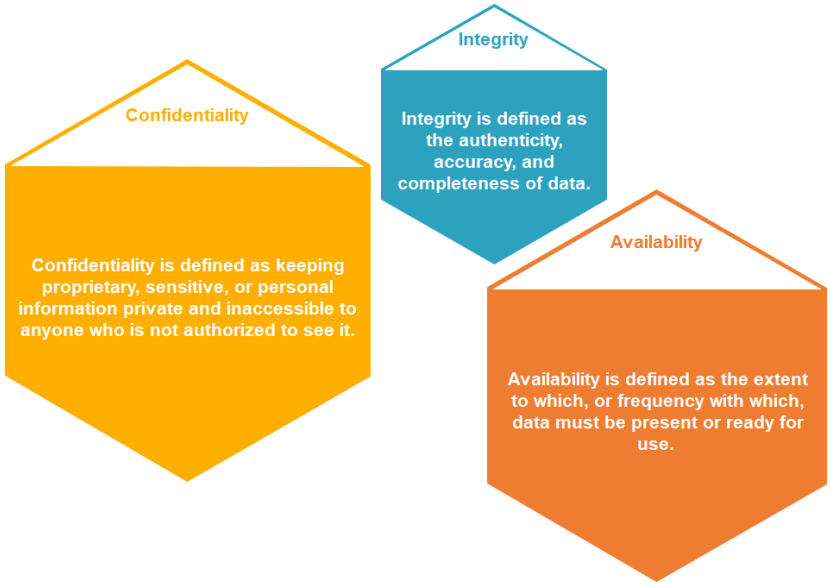


Figure 3:1: CIA Triad

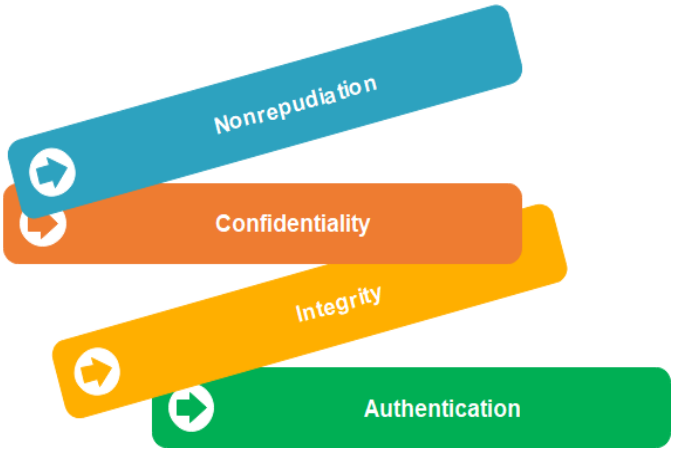


Figure 3:2: Other data attributes

These definitions are adapted from the book "Managing Information Security Risks: The OCTAVE Approach" [Alberts 2002].

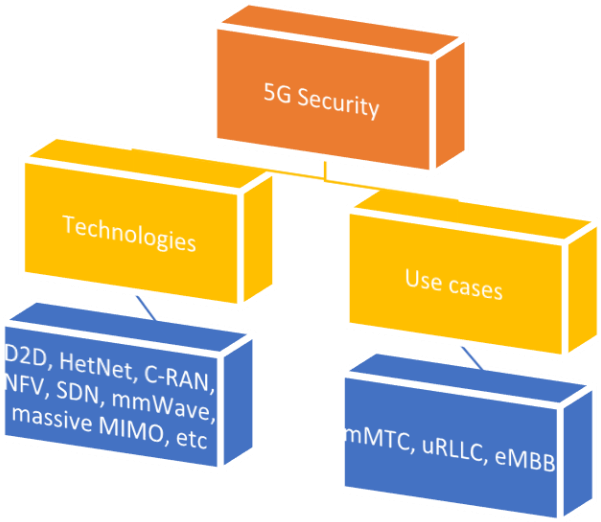
3.1.1.1 **Violation of the data attributes:**[11]

- Disclosure of data (violation of the confidentiality attribute)
- Modification of data (violation of the integrity attribute)
- Insertion of false data (violation of the integrity attribute)
- Destruction of data (violation of the availability attribute)
- Interruption of access to data (violation of the availability attribute)
- System destruction, destabilization, or degradation (violation of the availability attribute)

Further discussions on cyber security, enroll for cisco introduction to cyber security course, I compiled notes for the whole course here[3]

[3] https://drive.google.com/open?id=1Y27hT6ZYCBX_553JcbLjcqjjcMIuzuvk

3.2 5G SECURITY APPROACHES



The concept of data:

It can be static, stored on servers, and storage media, or it can be dynamic, the one on an active network, this data in 5G is referred to as 'bigdata', from how it arises, so the nature of data also determines the security approach techniques to securing it.

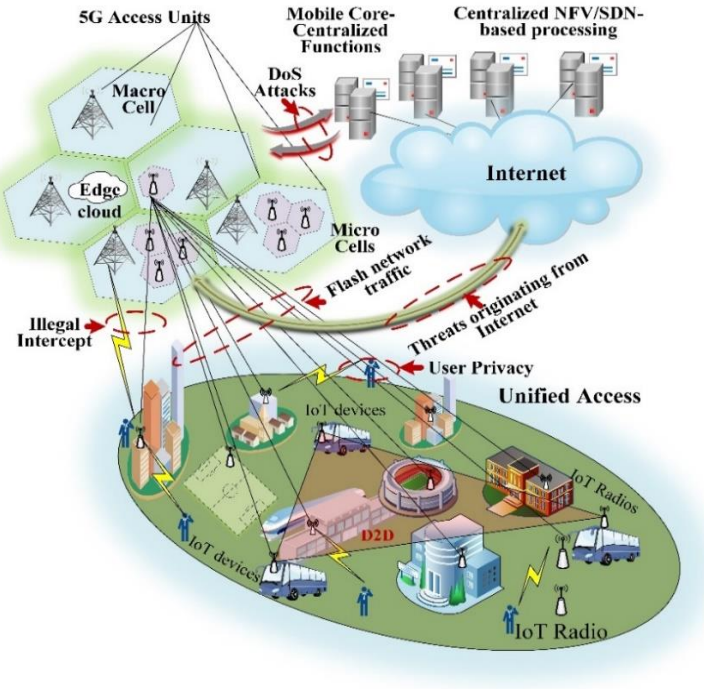


Figure 3:3: 5G Threat Landscape

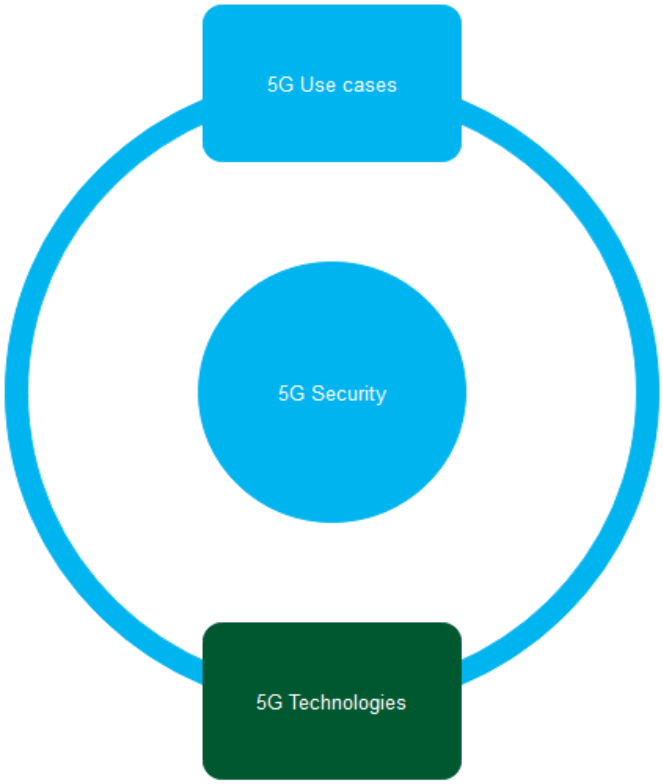


Figure 3:4: 5G Security approaches

3.2.1 5G Use cases Security approach

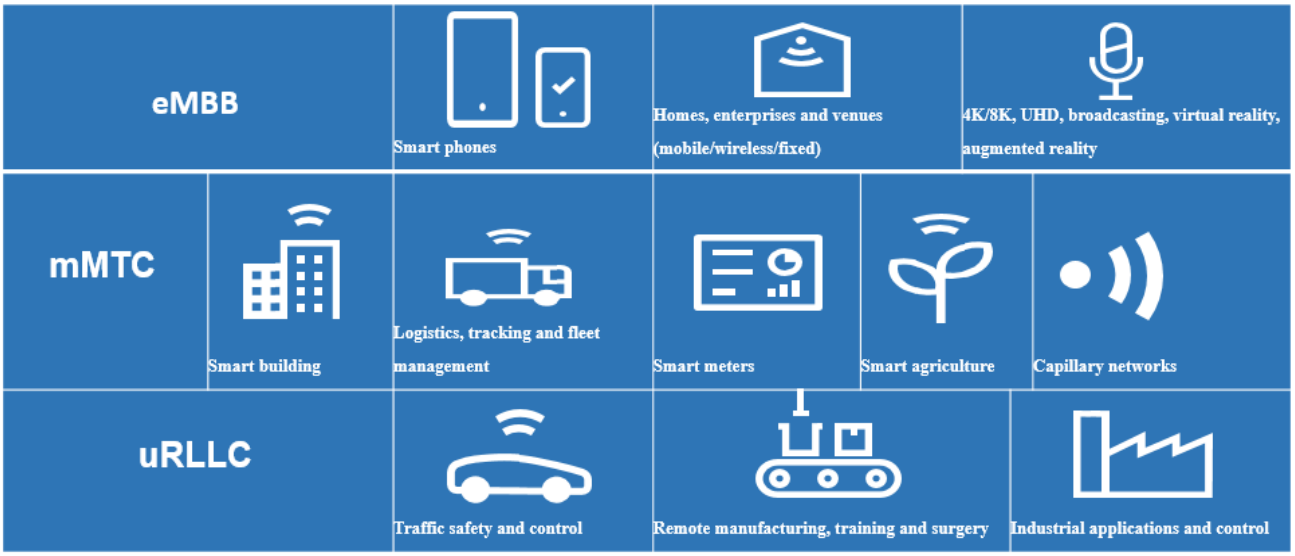


Figure 3:5: 5G Use cases / scenarios

3.2.2 5G technologies Security approach

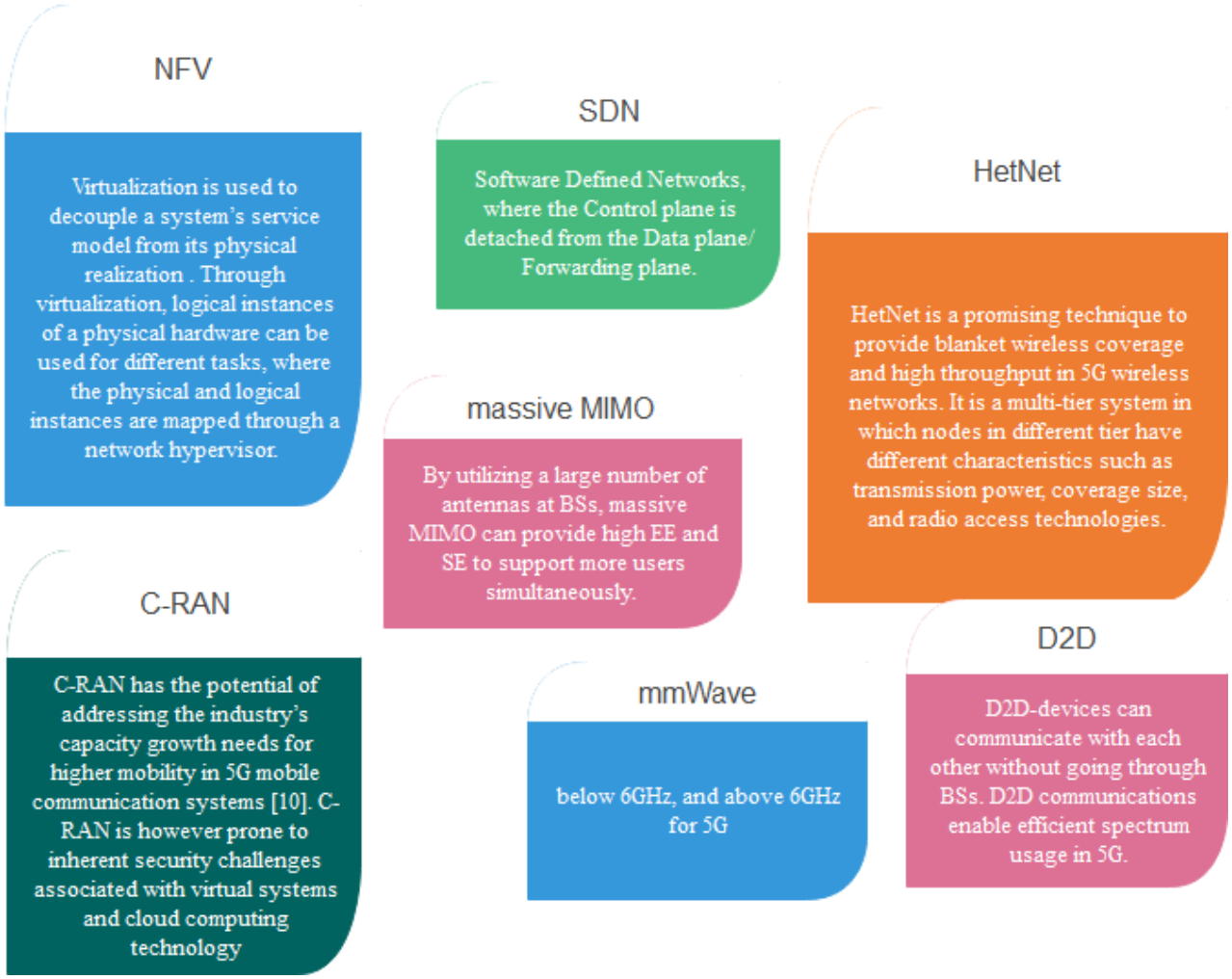


Figure 3:6: 5G technologies/enablers Security approach

Below is a brief description of each use case scenario; [23]

Massive MIMO, by utilizing a large number of antennas at BSs, massive MIMO can provide high EE and SE to support more users simultaneously. The large number of antennas at BSs can significantly improve the throughput, EE performance, and shift the most of signal processing and computation from user terminals to BSs . Moreover, massive MIMO can improve the security of communications. In [23] the authors considered PLS for a downlink K-tier HetNet system with multiple eavesdroppers. A minimum of four antenna arrays for reliability and that support beam steering and beam tracking.

HetNet is a promising technique to provide blanket wireless coverage and high throughput in 5G wireless networks. It is a multi-tier system in which nodes in different tier have different characteristics such as transmission power, coverage size, and radio access technologies. With the heterogeneous characteristics, HetNet achieves higher capacity, wider coverage and better performance in Energy Efficiency (EE) and Spectrum Efficiency (SE). However, HetNet architecture, compared to single-tier cellular network, makes UE more vulnerable to eavesdropping [24]. Moreover, with the high density of small cells in HetNet, traditional handover mechanisms could face significant performance issues due to **too frequent handovers between different cells**

For enhancing communication coverage in HetNet, coordinated multipoint transmission (CoMP) can be applied. However, CoMP can increase the risk of being eavesdropped for the legitimate users. Multiple BSs are selected to transmit the message. A dynamic BS selection scheme is proposed based on the secure coverage probability. [23]

To tackle the eavesdropping attacks in HetNet, a secret mobile association policy is proposed based on the maximum truncated average received signal power (ARSP). The maximum ARSP should be higher than a pre-set access threshold in order for mobile to keep active. Otherwise, the mobile device remains idle

The intrusion detection-based approach is considered as one way to provide secure communications. Intrusion detection techniques for mobile cloud computing in heterogeneous 5G. Several detection methodologies are studied as signature-based detection, anomaly-based detection, specification-based detection, stateful protocol analysis, hybrid intrusion detections with principles of these approaches.

Due to the high density of small cells, the knowledge of the cell a user is associated with can easily reveal the location information of that user. In [23], the authors investigated the location privacy based on physical layer of association algorithms in 5G. A differential private Gale-Shapley algorithm is proposed to prevent the leakage of location information with certain QoS for users. The evaluation of the algorithm based on different privacy levels is presented with the influence on utility of users

D2D-devices can communicate with each other without going through BSs. D2D communications enable efficient spectrum usage in 5G. Moreover, D2D communications can effectively offload traffic from BSs. However, the lack of a D2D security infrastructure makes the D2D communications less secure than the device to network communications. To improve the SE, dynamic spectrum access is usually adopted for D2D links, which can yield security threats such as **jamming**.

Cooperation between D2D nodes is a popular way to secure the D2D communications against **eavesdroppers**. The legitimate transmitters with a common receiver can improve their reliable transmission rate through cooperation scheme to secure D2D communications considering distance. Before the cooperation, devices can check the distance to test whether cooperation can improve the security of the communications. The distance constraints can be used to determine cooperation jointly, cooperation from one side, or no cooperation to maximize the achievable secrecy rate. With no specific requirements for the D2D communications, the proposed scheme can be applied to all D2D communications scenarios.

Besides cooperation, **power control** and **channel access** are also considered in securing D2D communications. Optimal power control and channel access of D2D link are proposed to maximize the achievable rate of cellular users and the physical layer secrecy rate of D2D links.

A certificateless public key cryptography is applied to achieve the security requirements. Security objectives of m-health network are defined as data confidentiality and integrity, mutual authentication, anonymity to anyone except intended physician, unlinkability, forward security and contextual privacy.

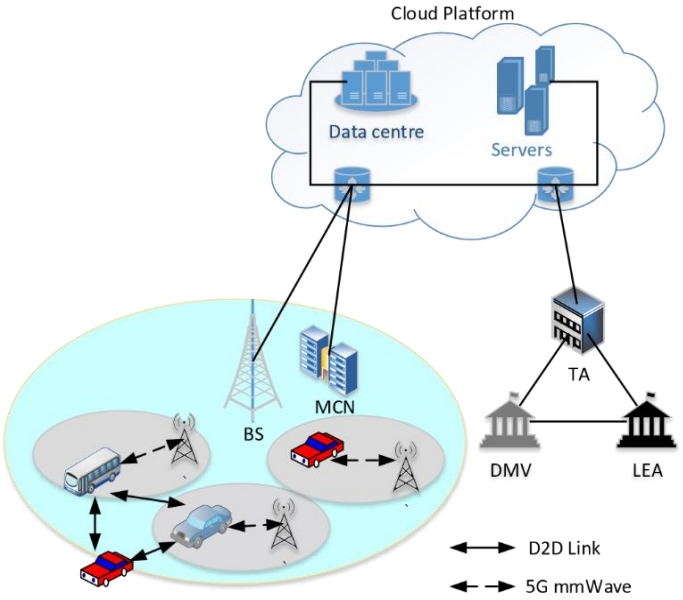


Figure 3:7: D2D Network setup **[23]**

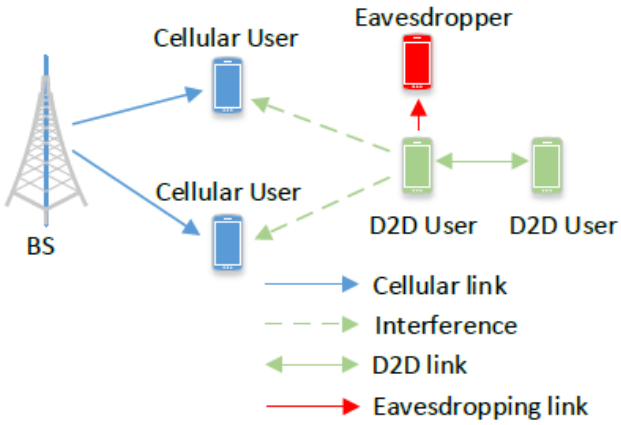


Figure 3:8: D2D Eavesdropper attack

Cloud Radio Access Network (C-RAN):

Cloud Radio Access Network (C-RAN) is another key area of interest in analyzing the security challenges in 5G mobile clouds. C-RAN has the potential of addressing the industry's capacity growth needs for higher mobility in 5G mobile communication systems [23]. C-RAN is however prone to inherent security challenges associated with virtual systems and cloud computing technology, for instance, the centralized architecture of C-RAN suffers the threat of single point of failure. Other threats like intrusion attacks where adversaries break into the virtual environment to monitor, modify, or run software routines on the platform while undetected also constitutes substantial threats to the system. [23]

Security Solutions for Mobile Clouds:

Most proposed security measures in MCC revolve around the strategic use of virtualization technologies, the redesign of encryption methods and dynamic allocation of data processing points. Hence, virtualization comes as a natural option for securing cloud services since each end-node connects to a specific virtual instance in the cloud via a Virtual Machine (VM). This provides security through the isolation of each user's virtual connection from other users. Attacks in this category include Wi-Fi sniffing, DoS attacks, address impersonation, and session hijacking [23]

3.2.3 Standardization on 5G security

Standardization body	Activities
3GPP SA3	Threat analysis, Requirements on security, Security architecture and protocol specifications Definition of 17 security domains (Architecture, Authentication, RAN security, Key Management, etc.)
ETSI ISG NFV	Security monitoring and administration for NFV Security assessment for NFV platform • etc.
GSMA	5G trust model, etc.
NGMN	5G security requirements (DoS protection, Network slicing, MEC)
5GPPP	5GPPP-ENSURE, review report here[4]
Others	IETF (5GIP, NETSLICING, etc.) ONF(Open Networking Foundation) – SDN related security

Table 3.1: Security standardization in 5G, work groups

Below is a review of 5G Security,[5]

3.2.4 5G technologies and security

Technologies	Merits (Security Aspects)	Problems
5G radio access		Jamming Physical layer security
Network slicing	Support on different security requirements using slice separation Partial security damage	Secure slice separation Attacks to slice management function Management between slice communication
Virtualization (NFV/SDN)	Enhancement to countermeasures of Cybersecurity DoS mitigation, Virtual Firewall, etc.)	Secure slice separation Attacks to orchestrator/controller Trust (NFVI, 3rd Party VNF)
Edge computing	Offload of security functions (From devices to edges)	Low security capability compared with core equipment (Risk of cryptographic key leakage, fraud on charging, etc.)

Table 3.2: 5G technologies and security

[4] https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf
[5] http://engine.scichina.com/doi/pdf/a3938e128872456f8d87c0527260a0d8

Software Defined Networks SDN, has been defined above, below I introduce mitigation techniques for teleportation in SDN switches. As I have started in the next chapters, the networking equipments have embedded software, which should be developed through a secure software development life cycle, as described in the reference of that topic. Now the concern is usually, that a flaw in the software design, will create back doors which are exploited by attackers, and a zero day, would mean lots of loss to the enterprise implementing SDN Switches, more information is available at…the advantages of SDN are quiet many, but SDN simply enables centralized control, automation, reconfiguration, and softwarization of a network. However, security threats introduced by SDN teleportation are also worth reviewing, these include; bypassing security mechanisms like firewalls, exfiltration, Eavesdrop, attack coordination, man-in-the-middle attacks, etc. A review has been provided in the appendix.
The attack techniques include; the concept involves exploiting the control platform for hidden communication as shown by the red dotted line in the Figure: 2:12

a. Out of band forwarding

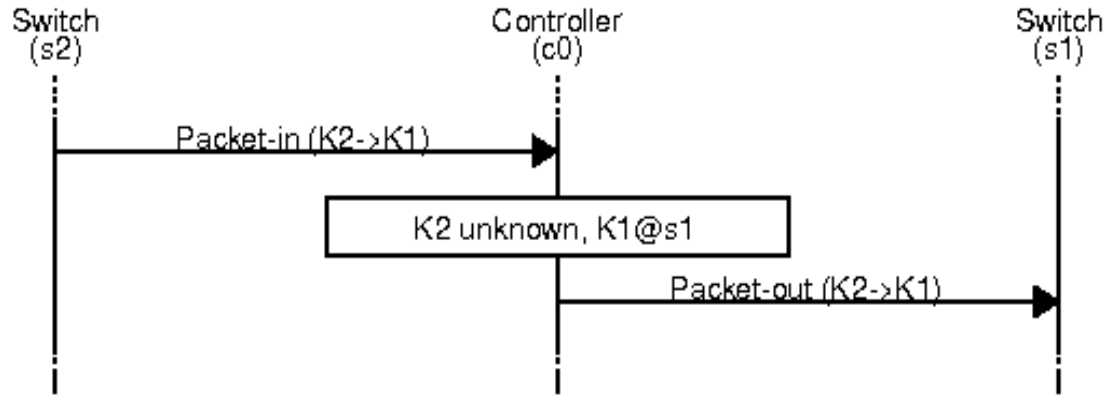


Figure 3:9: Out of band forwarding

b. Flow (re-)configuration

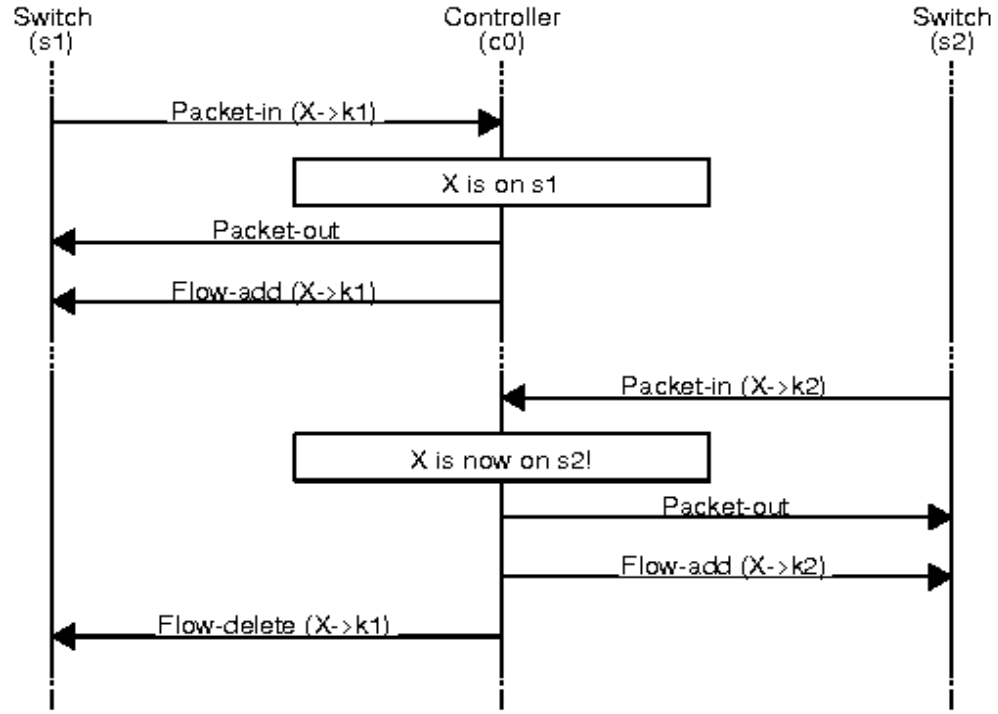


Figure 3:10: Flow (re-)configuration

c. Switch identification teleportation

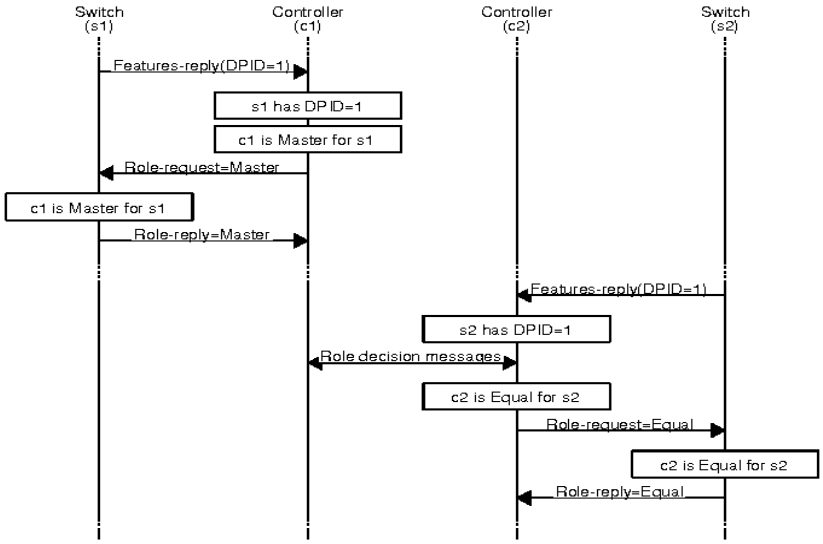


Figure 3:11: Switch identification teleportation

Source for Figure 2:9-2:11: https://www.semanticscholar.org/paper/Outsmarting-Network-Security-with-SDN-Teleportation-Thimmaraju-Schiff/395f0aeaf28c47110040d79bf9da01a211a79ec0

For further research, a reader can go to:

i. https://wiki.onosproject.org/download/attachments/12422167/onos-brigade-workshop-openflowhandshake.pdf?version=1&modificationDate=1526041574410&api=v2

ii. https://www.guardicore.com/wp-content/uploads/2018/02/Outsmarting-Network-Security-with-SDN-Teleportation-euroSnP2017.pdf

Possible mitigations for SDN Teleportation:

- Packet-in-Packet-Out Watcher
- Audit-Trails and Accountability
- Enhanced IDS with Waypoint Enforcement

As proposed 5G is built on technologies mentioned above, and a typical SDN Switch is shown below, with a centralized control for the different switches, a flowvisor like openFlow is used to link to the control plane and the data plane, It is itself a controller that enable network virtualization

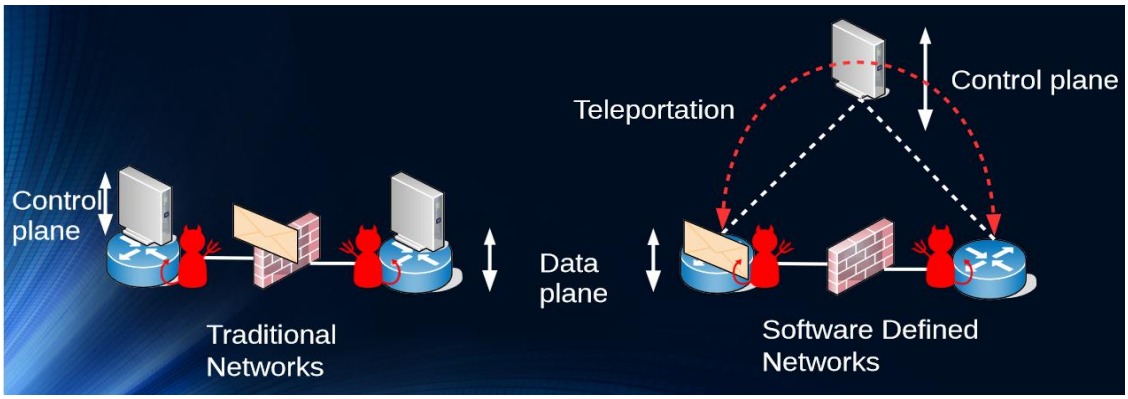


Figure 3:12: SDN, networking paradigm, showing teleportation

Summing up on the security approach of 5G, I have reviewed NFV, as defined above, NFV introduces the security challenges as shown below, however, NFV, improves security through …and the body responsible for the development of NFV is ETSI. The NFV Orchestrator and VNF Manager, is known as NFV MANO.

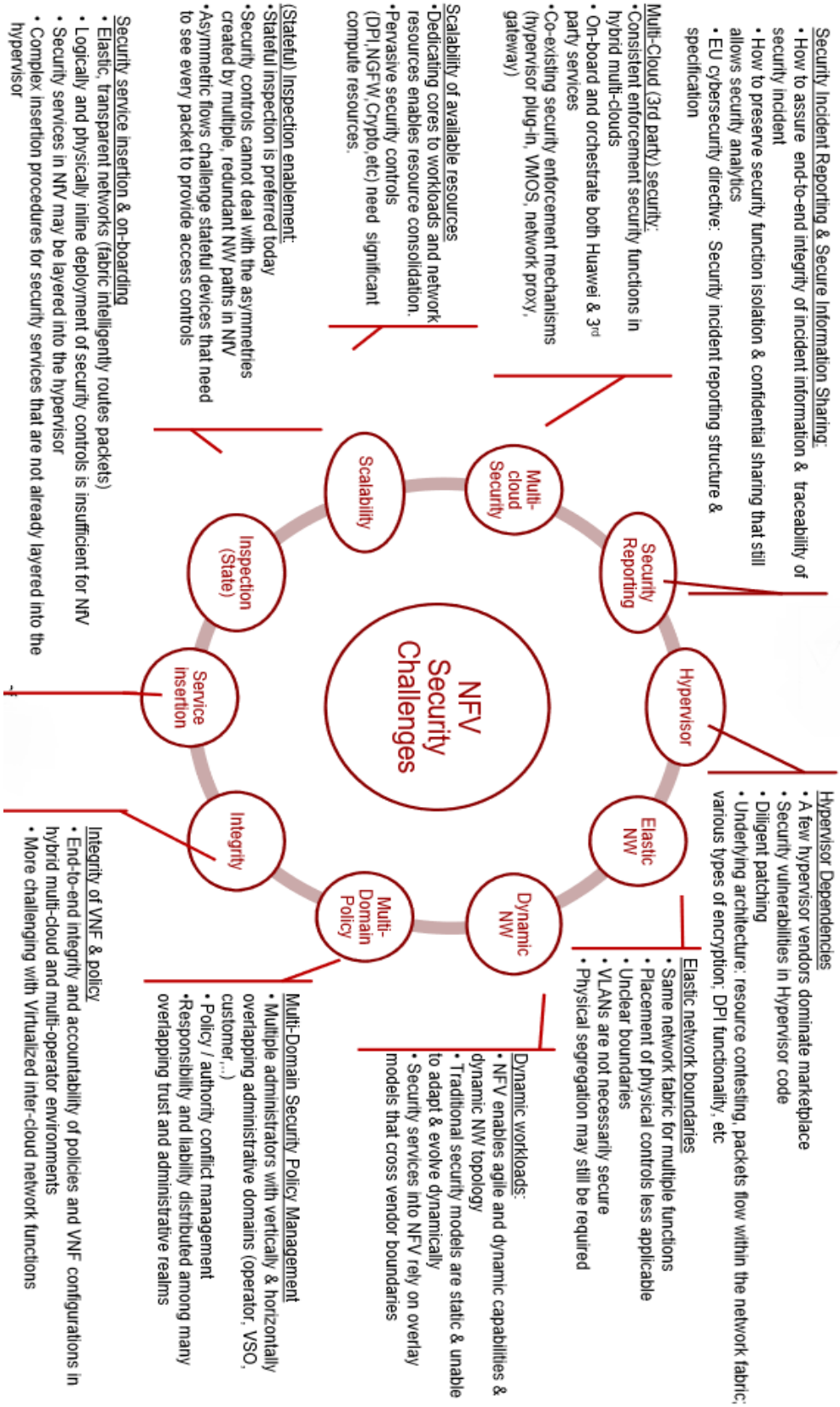


Figure 3:13: NFV security challenges

Source: Security Challenges and Guidance for Protecting NFV on Cloud IaaS, 2017 https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/05_NFVSECURITY/S01_CHALLENGES/HUAWEI_DIMITRAKOS.pdf

3.3 Counter measures Approach

My main work way done as such to reflect counter measures as proactive and reactive tools as applied to cyber security.

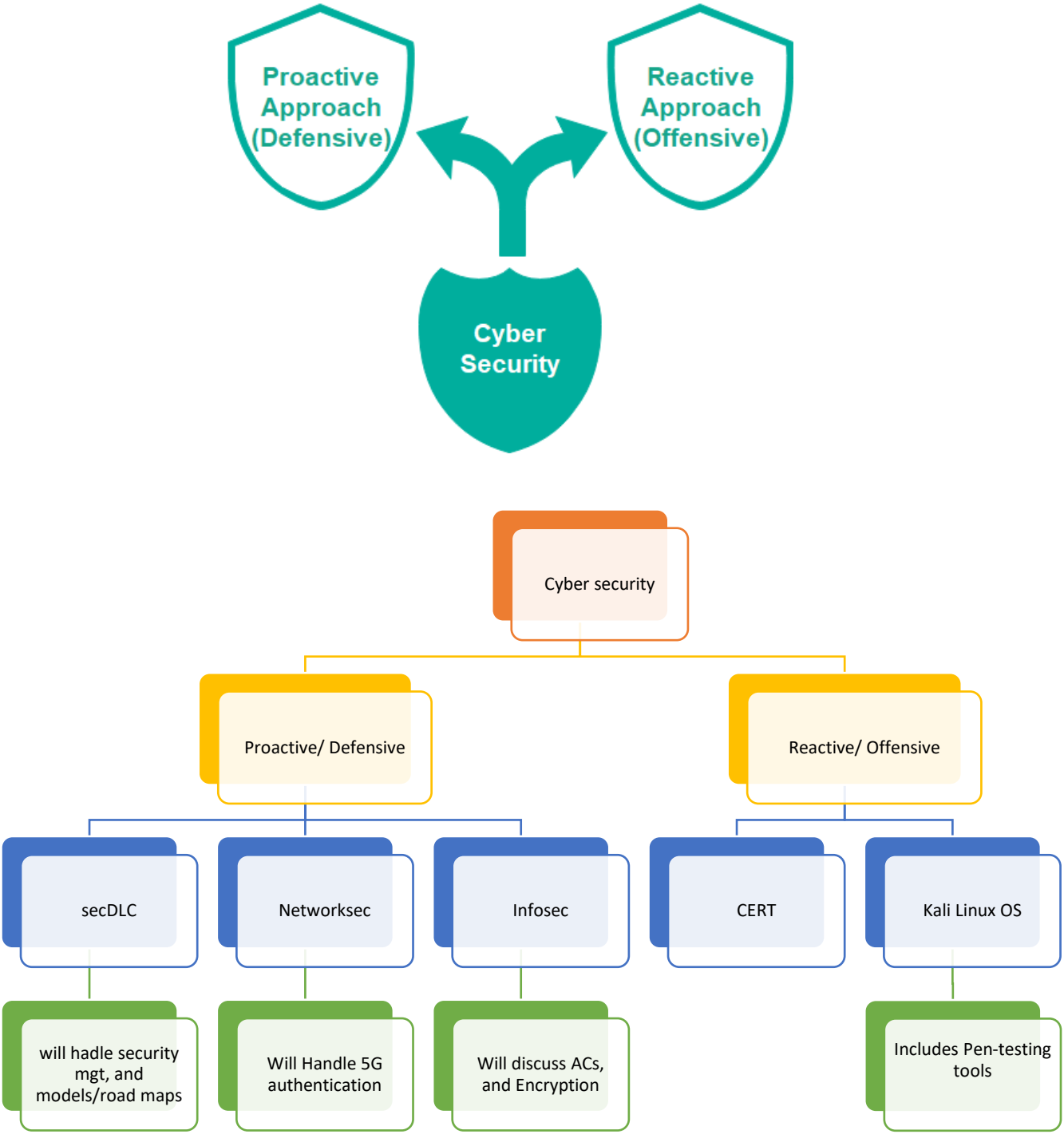


Figure 3:13: cyber security approach

CHAPTER 3: METHODOLOGY

Objectives	Method	Description
To carry out research on cyber security risk management, models, frameworks, and roadmap	Text books, cyber security websites, consultations	Text book used, Cyber Security Engineering by Nancy R. Mead and Carol C. Woody
To carry out research on encryption algorithms of wireless networks, and Access control models.	Text books, cyber security websites, consultations	Text book used, Handbook Of Security And Networks, editors Yang Xiao, Frank H Li, Hui Chen ISBN-13 978-981-4273-03-9, and internet
To carry out research on 5G, IoT and Cloud network architecture.	Text books, cyber security websites, tutorials,	Accessed the 5GPPP, 3GPP websites
To develop two MATLAB Applications; one that hinds the characters of a password on, and another that generates munged passwords	Text books, and website, tutorials, consultations	Accessed the MATWORKS website
To perform network security hardening and monitoring.	Tutorials, surfing internet	Simulation using Kali Linux, Snort, Wireshark and GNS3
To carry out research on cyber security policies both national and international.	Trainings, workshops, meetups, tutorials, consultations, questionnaires	Carried out apprenticeship at CERTUganda CERT (NITA-Uganda, CERT/CC) and (UCC CERT) https://www.ug-cert.ug/, and https://www.cert.ug/

Table 4.1: Summary of methodology

4.1 RESEARCH DESIGN

Information about Cyber security orange book, X.800, CBK-Common Body of Knowledge, Encryption, ACs models, Security Software Development Life Cycle. Software assurance, Competency levels, and Risk management Models, Roadmaps, and Framework. InfoSec and DevOps, Vulnerability assessment, patch management, and artefact handling. Cyber Threats. and information about 5G, IoT and Cloud security architectures was gathered from text books, and online CERT websites and 5GPPP, 3GPP etc.

Information about Attack history statistics and their impact, Law and policy for Cyber security was got from Uganda CERT (NITA-Uganda, CERT/CC) and (UCC CERT on their website and by carrying out apprenticeship at CERT

What CERT[6] does: ***Attack history and public security information dissemination with include;*** *Incident Handling, Incident analysis, Incident response support, Incident response coordination, Incident response on site, Vulnerability Handling, Vulnerability analysis, Vulnerability response, Vulnerability response coordination (Alerts and Warnings, to customers), Recovery handling.*

A detailed act on communications in Uganda is described in *THE UGANDA COMMUNICATIONS ACT, 2013,* accessible at;[7]

Simulation and design phase:

- Simulation of traditional security network tools was done using GNS3, to demonstrate **honeypots**, **DMZ**, and I will leave out **Fire Walls**, **VPNs**, and **VLANs** [10]
- Snort can be used to demonstrate IDS and IPS to secure networks, under the reactive tools
- Wireshark can be used as a security monitoring tool for network monitoring this is also under the reactive tools

Application development phase:

- Developing a Character substitution and Pin hardening on login pages for cloud and IoT APIs with Matlab and python.
- Development of Security Tools; MUNGED passwords application with Matlab and python.

[6] www.certug.org

[7] https://www.ug-cert.ug/files/downloads/UCC%20Act%202013.pdf

CHAPTER 4: MAIN WORK

5.1 PROACTIVE/ DEFENSIVE TOOLS

This part will review the proactive tools for cyber security mitigation, which are carried out before attacks occur, and for defense. These activities include encryption, access control, secure software development life cycle, network security.

5.1.1 Encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot.[10]

Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor.

In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm. A cipher – generating ciphertext that can be read only if decrypted, with an encryption key.

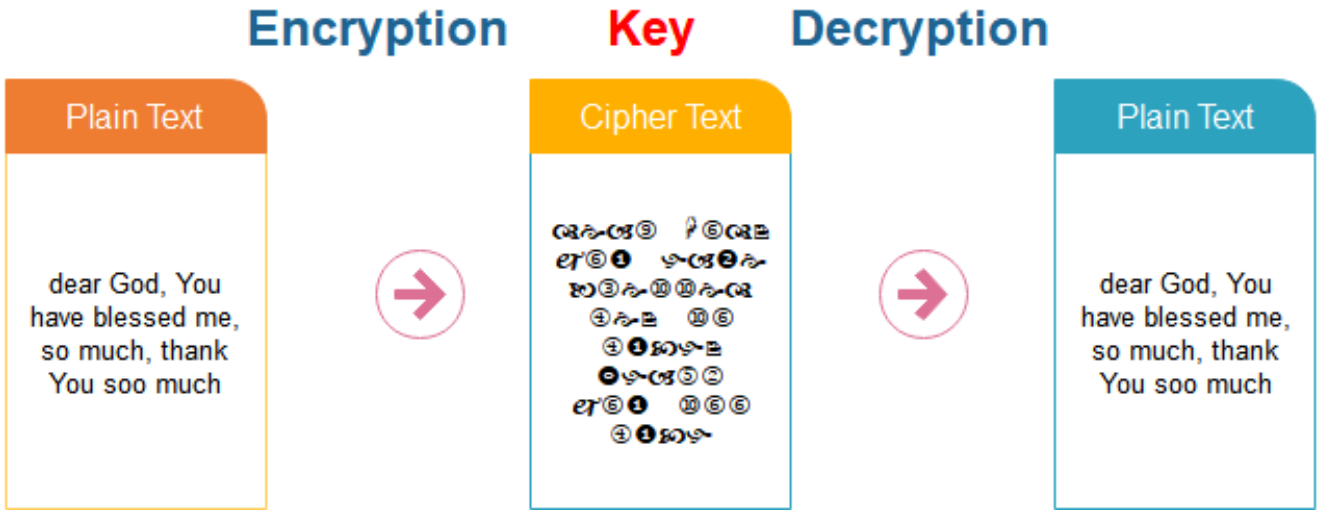


Figure 5:1: Encryption process

5.1.1.1 Symmetric encryption

In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their messages, the encryption and decryption keys are the same.

Symmetric encryption.

Algorithm

Step 1

A and B agree on a cryptosystem

Step 2

A and B agree on the key to be used

Step 3

A encrypts the messages using the shared key

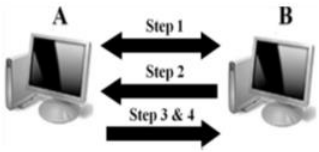
Step 4

B decrypts the ciphered messages using the shared key

Figure 5:2: Symmetric encryption

5.1.1.2 **Asymmetric Encryption**

Asymmetric encryption is the type of encryption where two keys are used. What Key1 can encrypt only Key2 can decrypt. It is also known as Public Key Cryptography (PKC), because users need two keys: public key, which is known to the public and private key, which is only known to the user. Eg. RSA



Asymmetric encryption.

Algorithm

Step 1

A and B agree on a cryptosystem

Step 2

B sends its public key to A

Step 3

A encrypts the messages using the negotiated cipher and B's public key received in S

Step 4

B decrypts the ciphered messages using its private key and the negotiated cipher

Figure 5:3: Asymmetric encryption

Another classification of Block and stream ciphers

5.1.1.3 **Block Cipher**

In this method, data is encrypted and decrypted in the form of blocks. In its simplest mode, the plain text is divided into blocks, which are then fed into the cipher system to produce blocks of cipher text.

5.1.1.4 **Stream Cipher**

Stream cipher works on a stream of data by operating on it bit by bit. Stream cipher consists of

two major components: a key stream generator, and a mixing function. Eg RC4, WEP

Mixing function is usually just an XOR function, while key stream generator is the main unit in the stream cipher encryption technique.

5.1.2 Access Control Models

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

- A *subject* is an active entity, such as a process or a user.
- An *object* is a passive entity, such as a file.
- A *right* describes what a subject is allowed to do to an object; for example, the read right gives permission for a subject to read a file.
- The *protection state* of a system simply refers to the rights held by all subjects on the system.

Figure 5:4: Types of Access Control

Physical ACs include biometrics, etc., but I have discussed logical ACs which are implemented in software

5.1.2.1 Types of Logical Access Controls Models

- **Access-Control Matrix Model**
- ***Typed access-control matrix model*, TAM**
- ***Mandatory access control*, (MAC):** This rule is called *mandatory* because it must be followed, without exception
- ***Discretionary*. *Discretionary access control*, (DAC):** Access-control methods allow the owner of the entity to control access
- ***Originator-controlled access control*, (ORCON):** Access controls contain elements of both mandatory and discretionary access controls. Allow the originator to determine who can access a resource or data.
- ***Role-based access control* (RBAC):** In real life, job function often dictates access permissions. The bookkeeper of an office has free access to the company's bank accounts,

whereas the sales people do not. If Anne is hired as a salesperson, she cannot access the company's funds. If she later becomes the bookkeeper, she can access those funds. So the access is conditioned not on the identity of the person but on the role, that person plays.

- **Bell-LaPadula model:** The Bell-LaPadula model is a formalization of the famous government classification system using UNCLASSIFIED, CONFIDENTIAL, SECRET, and TOP SECRET levels.
- **Clark-Wilson Model:** for commercial integrity models:
- **Chinese Wall Model. (*Brewer-Nash model*):** The goal of the Chinese Wall model is to prevent conflicts of interest. It does so by grouping objects that belong to the same company into *company data sets* and company data sets into *conflict-of-interest classes*.[19][10]

5.2 CYBER SECURITY RISK MANAGEMENT AND SECURE SOFTWARE DEVELOPMENT AND ORGANIZATIONAL MODELS

Everything we do these days involves system and software technology: Cars, planes, banks, restaurants, stores, telephones, appliances, and entertainment rely extensively on technology. The operational security of these software-intensive systems depends on the practices and techniques used during their design and development. Lifecycle processes must consider the security-related risks inherent in the operational environments where systems are deployed.

Increased system complexity, pervasive interconnectivity, and widely distributed access have increased the challenges for building and acquiring operationally secure capabilities. Therefore, the aim of this inquiry is to show you how to create and ensure persistent operational assurance practice across all of the typical activities that take place across the system and software lifecycle. It should be noted that all telecommunications equipment have embedded software in them, therefore this is a worthwhile undertaking as a part of my project. [11]

5.3 SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

5.3.1 Software Assurance definitions.

• "The level of confidence we have that a system behaves as expected and the security risks associated with the business use of the software are acceptable" [Woody 2014] [11]

• "Software Assurance: Implementing software with a level of confidence that the software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software, throughout the lifecycle" [Woody 2014] [11]

5.3.2 Commercial Off-The-Shelf, COTS dilemma:

Further challenges to effective operational security come from the increased use of commercial off-the-shelf (COTS) and open source software as components within a system. The resulting operational systems integrate software from many sources, and each piece of software is assembled as a discrete product. Therefore, systems cannot be constructed to eliminate security risk but must incorporate capabilities to recognize, resist, and recover from attacks.

5.3.3 Creation malware in systems [11]

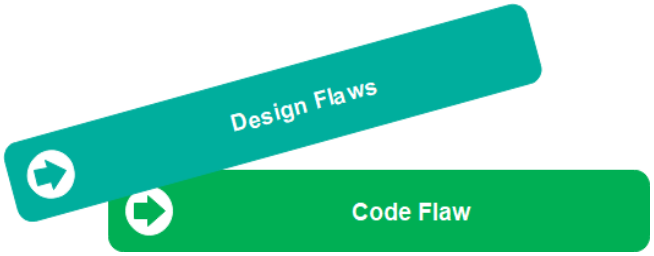


Figure 5:5: Malware types

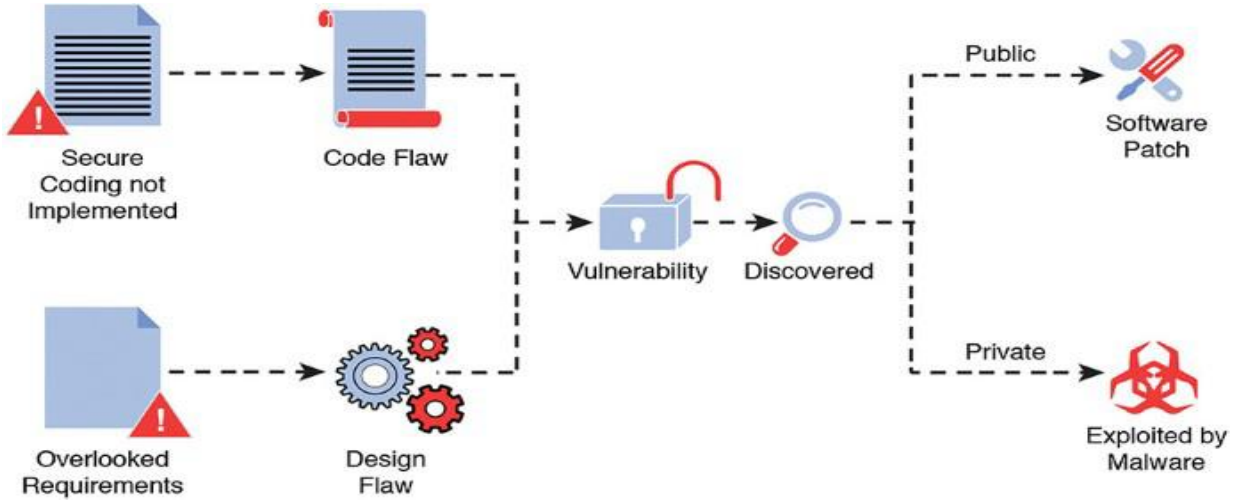


Figure 5:6: Malware life cycle management

5.3.4 DevOps and cyber security for secSDLC;

DevOps is a portmanteau of 'Development' (coding team) and Operations (testing and automation team). Focused on the integration of the two teams, its aim is to increase the speed of productivity in a business.

The first aspect of DevOps that endears itself to security is the ability to decrease the downtime of a system. DevOps engineers have the skills to incorporate self-healing characteristics into a system, meaning that if it is affected by a cyber attack, it can, in theory, begin to mend itself if it can be immediately accessed by a security team.[8]

[8] https://www.quora.com/Is-DevOps-used-in-cyber-security

5.4 CASE STUDY OF CYBER SECURITY FRAMEWORK AND MODEL [11]

Some of the frameworks and models include following as in [11]

1. Building Security In Maturity Model (BSIMM)
2. International Process Research Consortium (IPRC) Roadmap
3. Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM)
4. Microsoft Security Development Lifecycle (SDL)

5.4.1 Metrics for Cyber Security Engineering

List of metrics could be collected for cyber security, such as the number of security requirements, lines of validated code, vulnerabilities found by code checkers, process steps that include security considerations, hours needed to fix a security bug, and data validation tests passed and failed. [Source: www.iso.org/iso/catalogue_detail?csnumber=42106]

5.4.2 Software Security Frameworks, Models, and Roadmaps

5.4.2.1 Open Web Application Security Project (OWASP) Software Assurance Maturity Model (SAMM)

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

• Evaluating an organization's existing software security practices

• Building a balanced software security assurance program in well-defined iterations

• Demonstrating concrete improvements to a security assurance program

• Defining and measuring security-related activities throughout an organization

SAMM was built on the following principles:

• **An organization's behavior changes slowly over time**: A successful software security program should be specified in small iterations that deliver tangible assurance gains while incrementally working toward long-term goals.

• **There is no single recipe that works for all organizations**: A software security framework must be flexible and allow organizations to tailor their choices based on their risk tolerance and the way in which they build and use software.

- **Guidance related to security activities must be prescriptive**: All the steps in building and assessing an assurance program should be simple, well defined, and measurable. This model also provides roadmap templates for common types of organizations.

Governance	Construction	Verification	Deployment
Strategy & Metrics	*Threat Assessment*	*Design Review*	*Vulnerability Management*
Overall strategic direction of the software assurance program & instrumentation of processes & activities to collect metrics about an organization's security posture	Identify and characterize potential attacks on software to better understand the risks and facilitate risk management	Inspect artifacts created from the design process to ensure provision of adequate security mechanisms and adherence to expectations for security	Establish consistent process for managing internal and external vulnerability reports to limit exposure and gather data to enhance the security assurance program
Policy & Compliance	*Security Requirements*	*Code Review*	*Environment Hardening*
Set up a security and compliance control and audit framework to achieve increased assurance in software under construction and in operation	Promote the inclusion of security-related requirements during the software development process to specify correct functionality from inception	Assess source code to aid vulnerability discovery and related mitigation activities as well as establish a baseline for secure coding expectations	Implement controls for the operating environment in which software executes to bolster the security posture of applications that have been deployed
Education & Guidance	*Secure Architecture*	*Security Testing*	*Operational Enablement*
Increase security knowledge among personnel in software development through training and guidance on security topics relevant to individual job functions	Bolster the design process with activities to promote secure-by-default designs and control over technologies and frameworks upon which software is built	Test software in its runtime environment in order to discover vulnerabilities and establish a minimum standard for software releases	Identify and capture security-relevant information needed by an operator to properly configure, deploy, and run software

Figure 5:7: OWASP SAMM (refer to website for the current version of the model)

5.4.2.2 Microsoft Security Development Lifecycle (SDL)

The Microsoft Security Development Lifecycle (SDL) is an industry-leading software security process; the SDL has played a critical role in enabling Microsoft to embed security and privacy in its software and culture. Combining a holistic and practical approach, the SDL introduces security and privacy early and throughout all phases of the development process.

5.4.2.2.1 *Secure by Design*

Secure architecture, design, and structure. Developers consider security issues part of the basic architectural design of software development.

- *Threat modeling and mitigation*. Threat models are created, and threat mitigations are present in all design and functional specifications.
- *Elimination of vulnerabilities*. No known security vulnerabilities that would present a significant risk to the anticipated use of the software remain in the code after review. This

review includes the use of analysis and testing tools to eliminate classes of vulnerabilities.

- *Improvements in security*. Less secure legacy protocols and code are deprecated, and, where possible, users are provided with secure alternatives that are consistent with industry standards.

5.4.2.2.2 ***Secure by Default***

• *Least privilege*. All components run with the fewest possible permissions.

• *Defense in depth*. Components do not rely on a single threat mitigation solution that leaves users exposed if it fails.

• *Conservative default settings*. The development team is aware of the attack for the product and minimizes it in the default configuration.

• *Avoidance of risky default changes*. Applications do not make any default changes to the operating system or security settings that reduce security for the host computer. In some cases, such as for security products, it is acceptable for a software program to strengthen (increase) security settings for the host computer.

The most common violations of this principle are games that either open firewall ports without informing the user or instruct users to open firewall ports without informing users of possible risks.

• *Less commonly used services off by default*. If fewer than 80 percent of a program's users use a feature, that feature should not be activated by default.

Measuring 80 percent usage in a product is often difficult because programs are designed for many different personas. It can be useful to consider whether a feature addresses a core/primary use scenario for all personas. If it does, the feature is sometimes referred to as a P1 feature.

5.4.2.2.3 ***Secure in Deployment***

• *Deployment guides*. Prescriptive deployment guides outline how to deploy each feature of a program securely, including providing users with information that enables them to assess the security risk of activating non-default options (and thereby increasing the attack surface).

• *Analysis and management tools*. Security analysis and management tools enable administrators to determine and configure the optimal security level for a software release.

• *Patch deployment tools*. Deployment tools aid in patch deployment.

5.4.2.2.4 *Communications (CERT)*

• *Security response*. Development teams respond promptly to reports of security vulnerabilities and communicate information about security updates.

• *Community engagement*. Development teams proactively engage with users to answer questions about security vulnerabilities, security updates, or changes in the security landscape.

5.5 SECURING THE WEB APPLICATION:

Development of Security Tools;

5.5.1 Character substitution password login MATLAB application

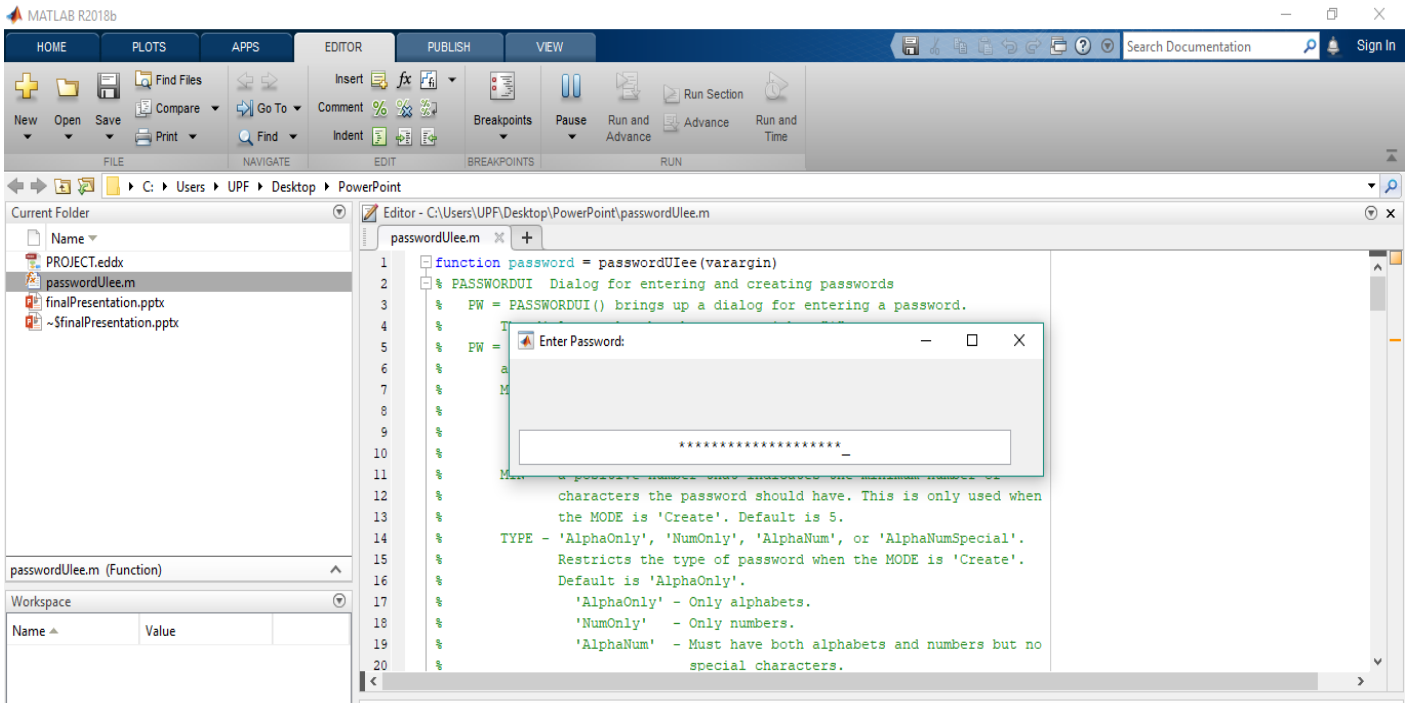


Figure 5:8: password login MATLAB application

Apart from character substitution with asterisk or dots, account lock out should be also set, for a number of minimum trials on login, and a proper way of account recovery should also be put in place, which is effective, and which can't be bypassed. Authentication of users should be done at secure stages to avoid system compromise (refer to Oauth 2.0). This is an important aspect because most Cloud computing providers, provide login API, and IoT API platforms, used mostly in the orchestration layers and management. More on secure web application development practices[9]

[9] https://www.keycdn.com/blog/web-application-security-best-practices and

5.5.2 Munged password application in python.

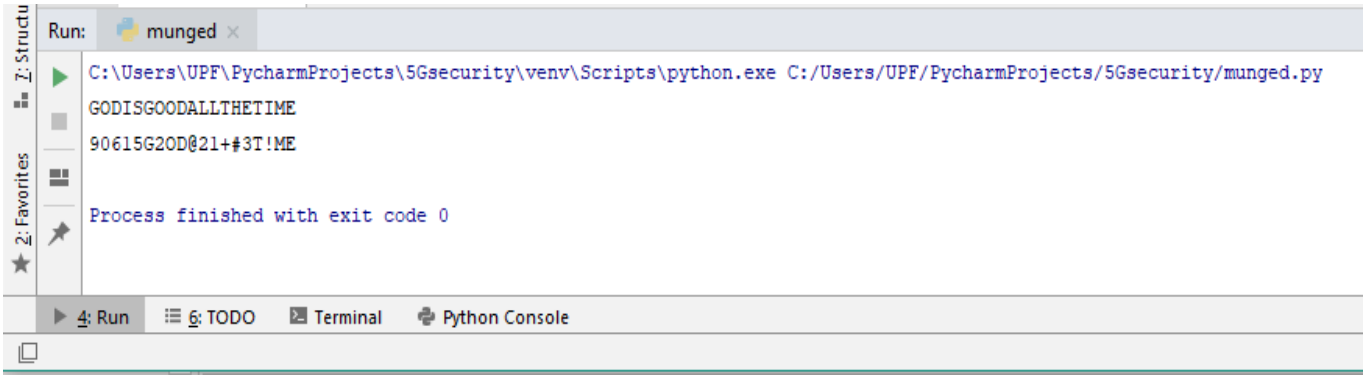


Figure 5:9: MUNGED passwords application with python.

5.6 TRADITIONAL NETWORK SECURITY

These include, but not limited to:

- Understanding the TCP/IP stack.
- Device configuration for security, and disabling inactive protocols.
- Hardware and software security tools like, **honey pots/ honeynets**, **DMZ**, **Fire Walls**, **IDS +IPS**, **VPNs**, and **VLANs**, **IPsec, MPLS.**

5.6.1 Understanding the TCP/IP stack, and security protocols:

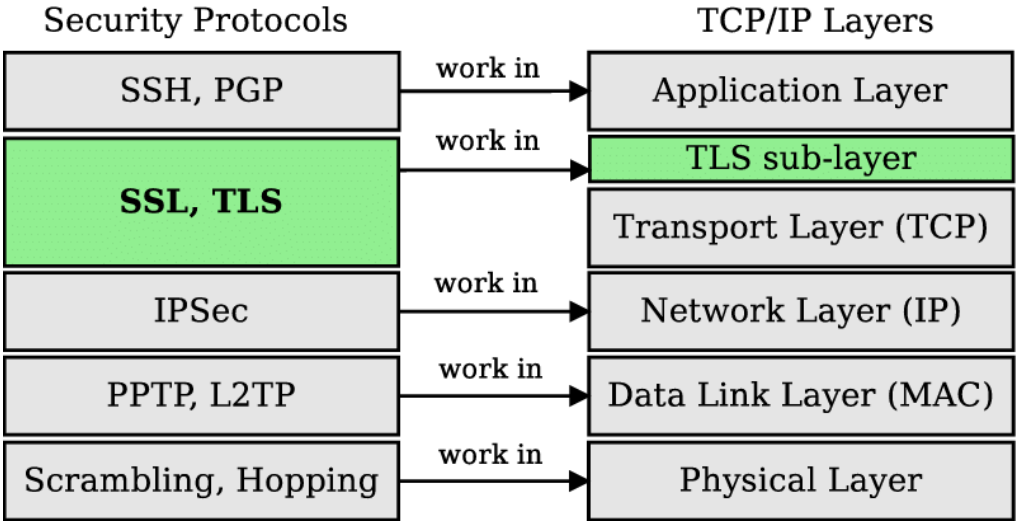


Figure 5:10: TCP/IP stack, and security protocols

Source:https://www.researchgate.net/publication/321347130_Service-Level_Monitoring_of_HTTPS_Traffic

https://blog.sqreen.com/best-practices-build-secure-applications/

5.6.2 Network Device configuration (cisco router)

A part from back doors, and software vulnerability of network devices, misconfiguration can result to weak points in a network, below is a sample of security config of a cisco router/switch

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access Only! $
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration... [OK]
R1#
```

Disabling CDP on some parts of the network, and using SSH, instead of Telnet is recommended for remote access/monitoring of device, this be because while using SSH, passwords are encrypted, whereas in Telnet, passwords are sent in plain text. It is also very important to apply the **shutdown** command on an interface that is not in use.

```
Switch1>enable
Switch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)#interface fastEthernet 0/1
Switch1(config-if)#no cdp enable
Switch1(config)#end
```

5.6.3 Demonstration of DMZ implementation:

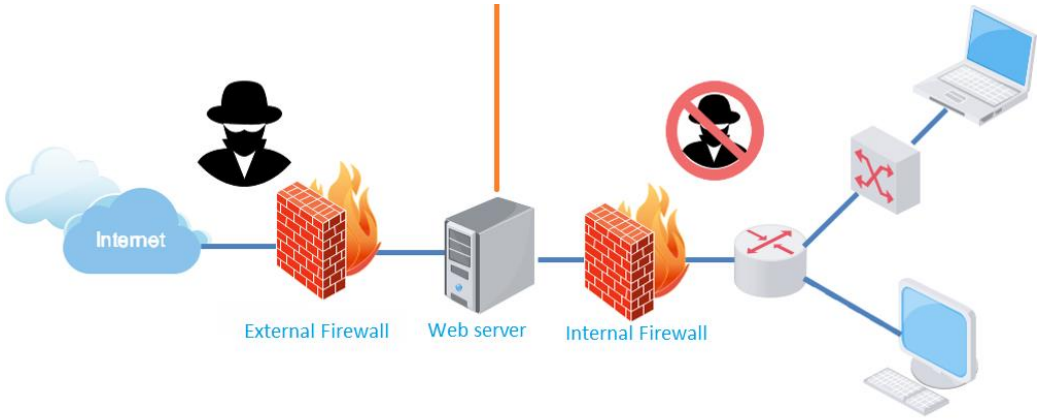


Figure 5:11: DMZ implementation

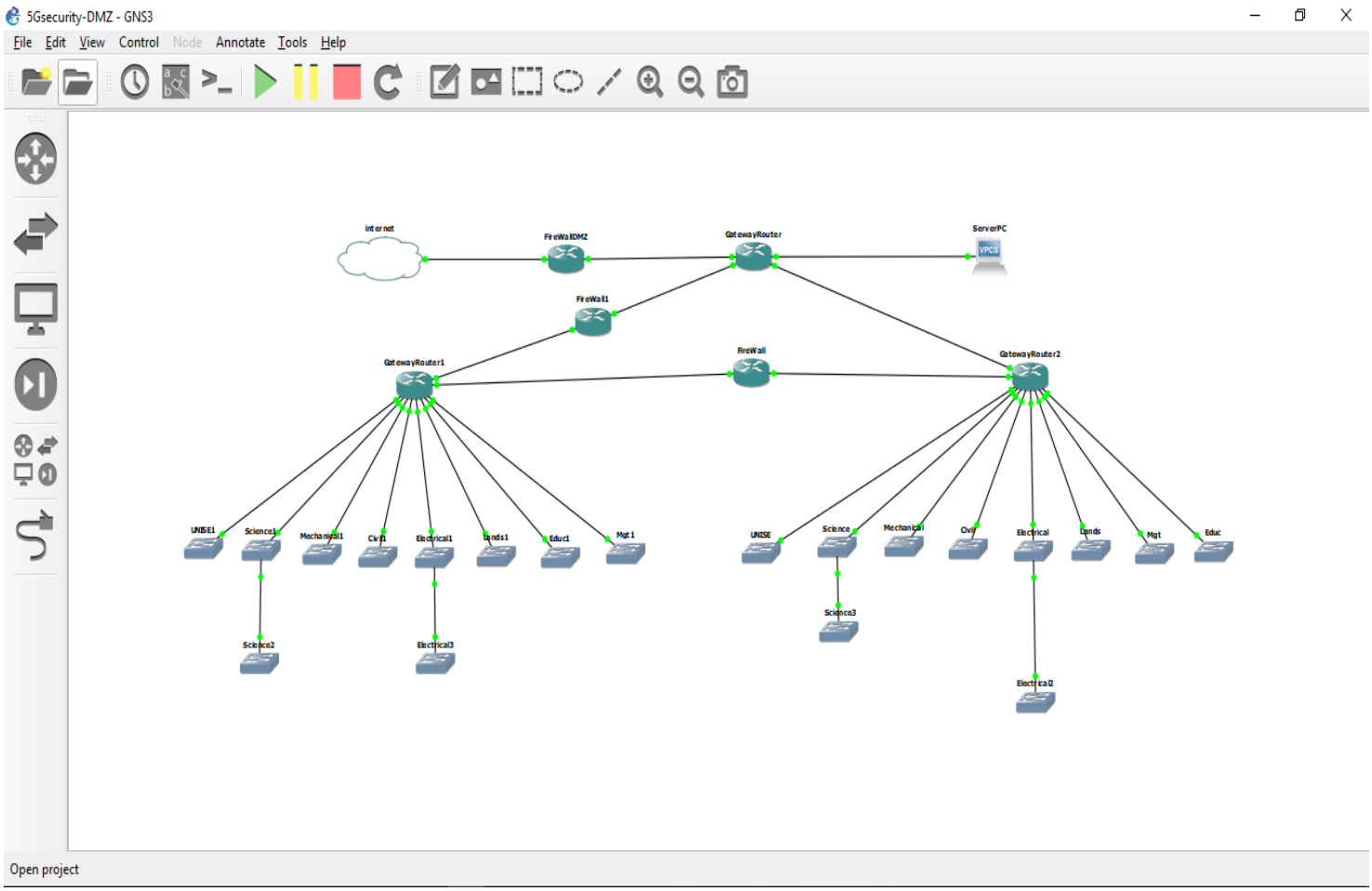


Figure 5:12: DMZ implementation in gns3

A **DMZ** or **demilitarized zone**/ **perimeter network**/ screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network (the Internet). The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN). Therefore, an external network node can access only what is exposed in the DMZ, like Web, FTP, Mail, and VoIP servers available to the public.

5.6.4 Demonstration of Honeynet

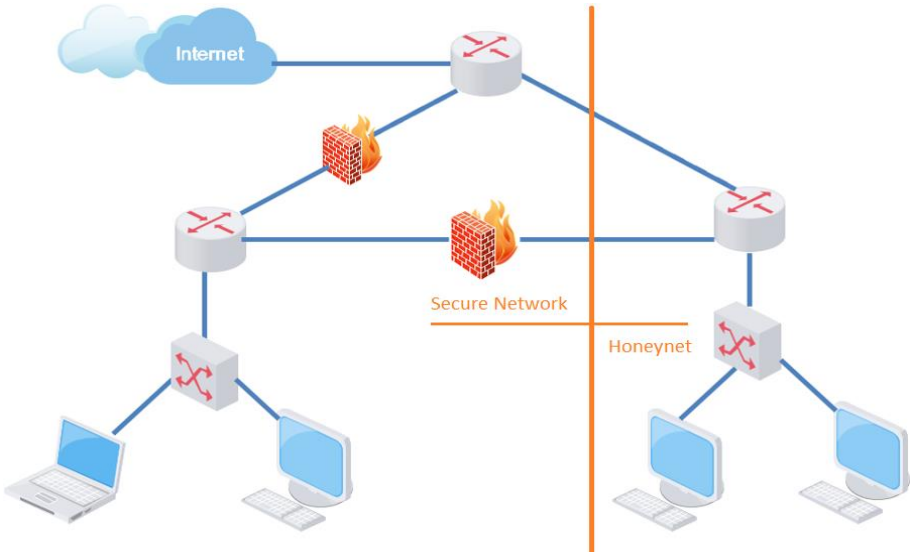


Figure 5:13: Demonstration of Honeynet

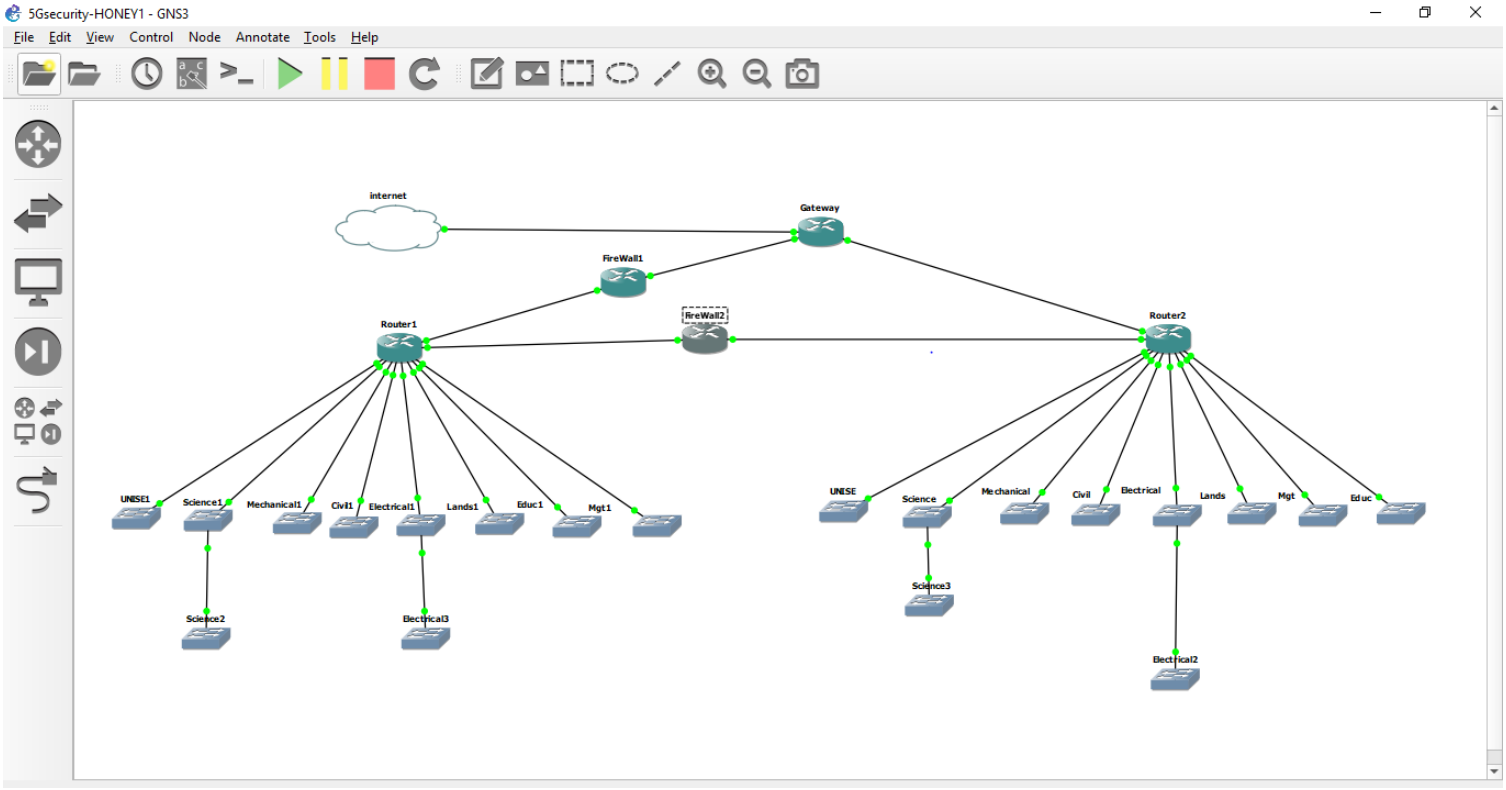


Figure 5:14: Demonstration of Honeypot in gns3

A **honeynet** is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more **honey pots**, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Refer to the honeynet project; https://www.honeynetproject.com/ and https://github.com/honeynet

Authentication Protocols used in 3GPP access technologies brief:

EAP is part of the ratified IEEE 802.11i standard, is defined in RFC 3748, which made RFC 2284 obsolete, and is updated by RFC 5247. Used for authentication in wireless networks and point-to-point connections

Advantages of EAP - AKA

The use of the AKA also as a secure PPP authentication method in devices that already contain an identity module.

The use of the 3rd generation mobile network authentication infrastructure in the context of wireless LANs

Relying on AKA and the existing infrastructure in a seamless way with any other technology that can use EAP.

- EAP-SIM is an Extensible Authentication Protocol (EAP) [RFC3748] mechanism for authentication and session key distribution using the GSM Subscriber Identity Module (SIM).

EAP-SIM uses a SIM authentication algorithm between the client and an Authentication, Authorization and Accounting (AAA) server providing mutual authentication between the client and the network. AAA Server is replaced with AuC

- EAP-AKA is used in 3G, and 4G
- EAP-AKA' and 5G-AKA is used in 3GPP access for 5G, and non-3GPP technology such as IEEE 802.11 WLANs. [Source: https://tools.ietf.org/html/]

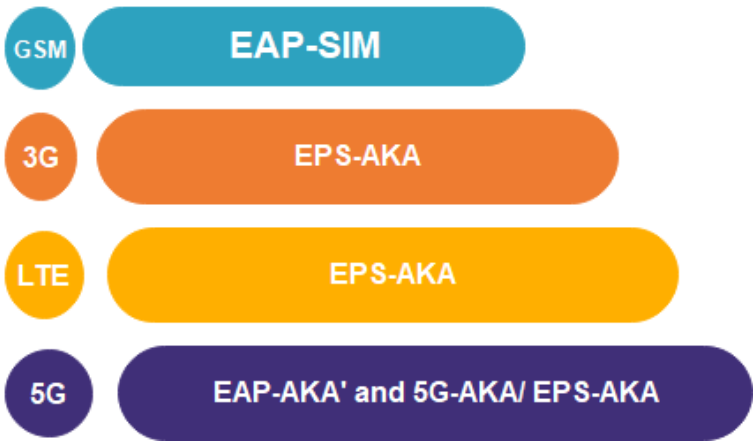


Figure 5:15: Authentication in 3GPP access

5.6.5 Security Evolution for 3GPP Access technologies

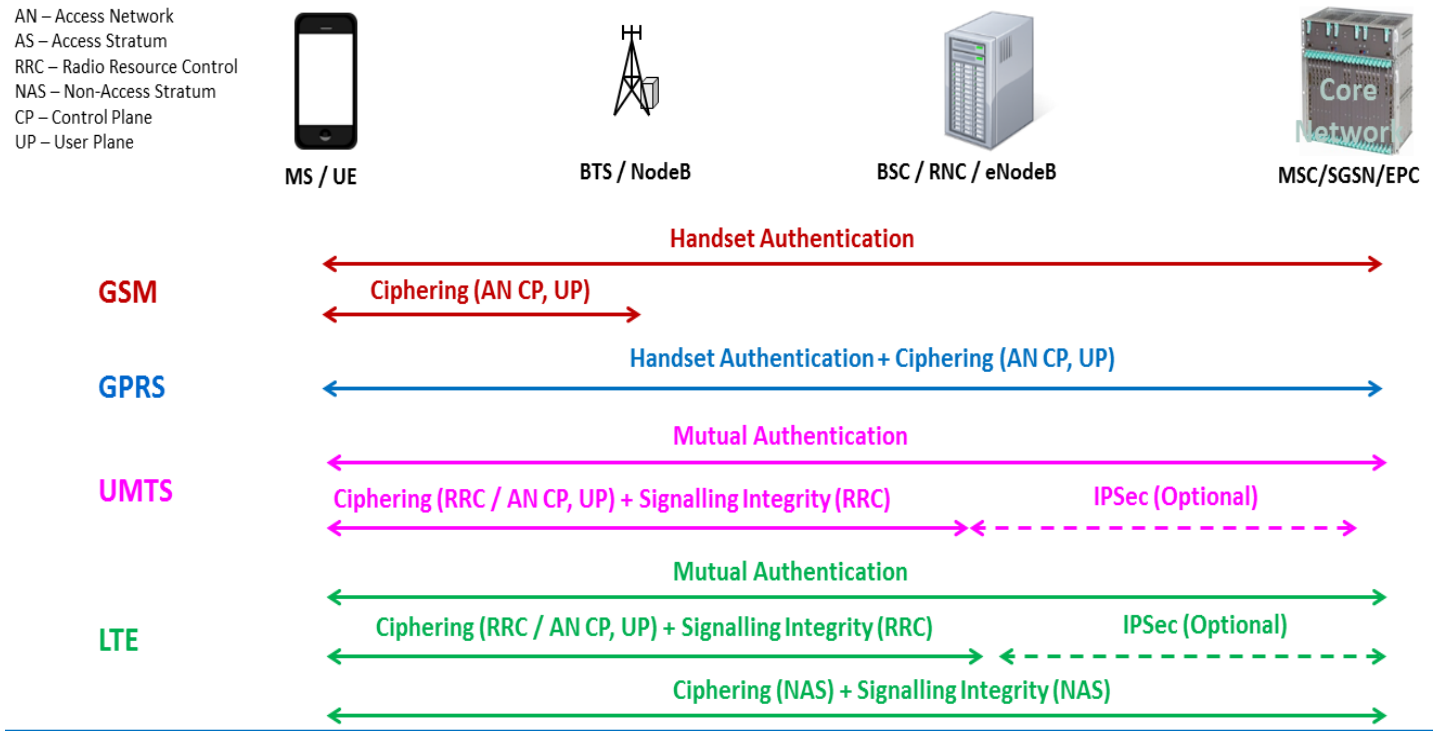
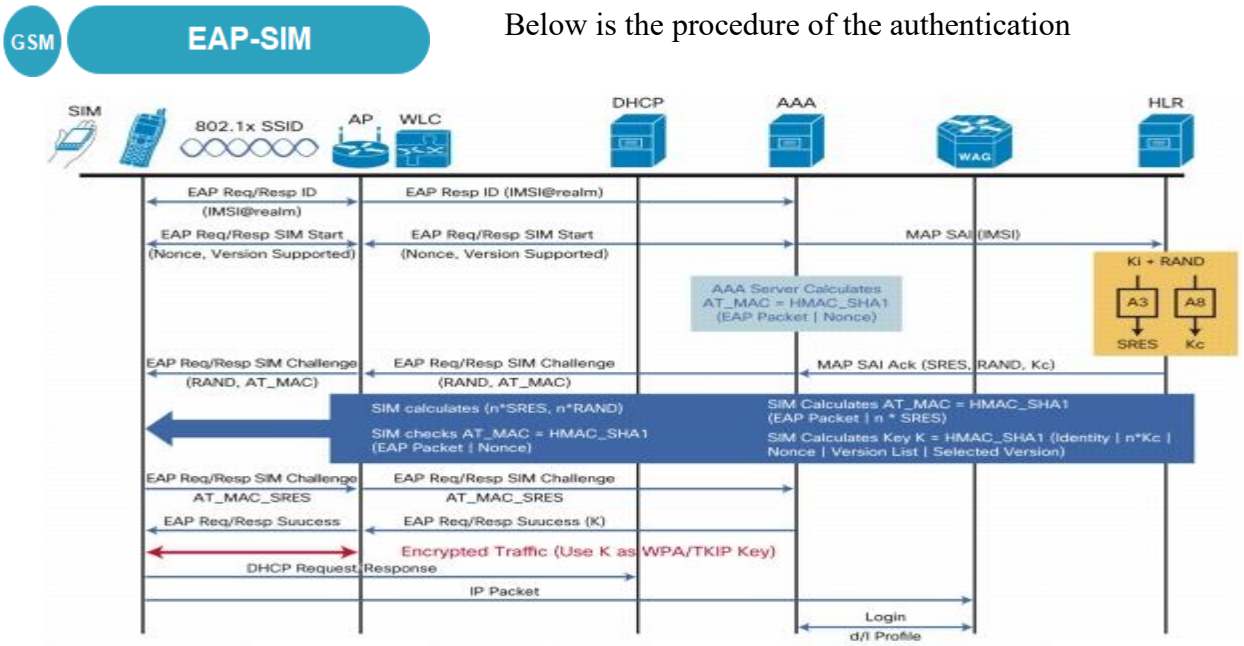


Figure 5:16: Security Evolution for 3GPP Access technologies

5.6.6 EAP-SIM



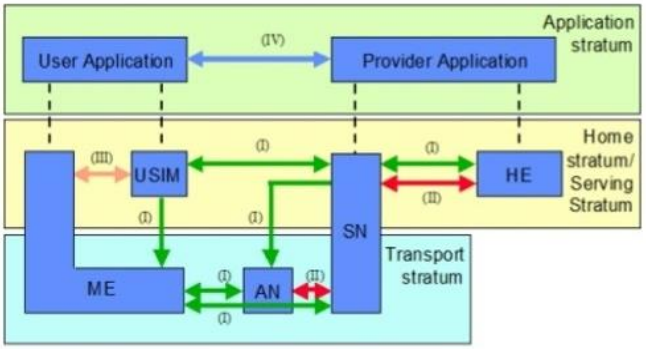
Below is the procedure of the authentication

Figure 5:17: EAP-SIM for GSM

Source:https://community.cisco.com/t5/wireless-mobility-documents/eap-sim-and-eap-aka/ta-p/3143656#toc-hId--85007361

1. EAP SIM is based on the authentication and encryption algorithms stored on the Global System for Mobile Communications (GSM) SIM.
2. It's based on a challenge-response mechanism and employs a shared secret key, Ki, which is stored on the SIM and otherwise known only to the GSM operator's Authentication Center (AuC).
3. When a GSM SIM is given a 128-bit random number (RAND) as a challenge, it calculates a 32-bit response (SRES) and a 64-bit encryption key (Kc)
4. EAP SIM also enhances the basic GSM authentication mechanism by providing for mutual authentication between the client and the AAA server
5. Secure keyed hashing algorithm, HMAC-SHA1 (one way hashing)

5.6.7 3G Security architecture



- 3GPP TS 33.102: 3G Security; Security architecture
- 3GPP TS 33.401: 3GPP System Architecture Evolution (SAE); Security architecture

Five security feature groups are defined. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to services, and which in particular protect against attacks on the (radio) access link.
- **Network domain security (II):** the set of security features that enable nodes to securely exchange signalling data, user data (between AN and SN and within AN), and protect against attacks on the wireline network.
- **User domain security (III):** the set of security features that secure access to mobile stations.
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Figure 5:18: 3G Security architecture

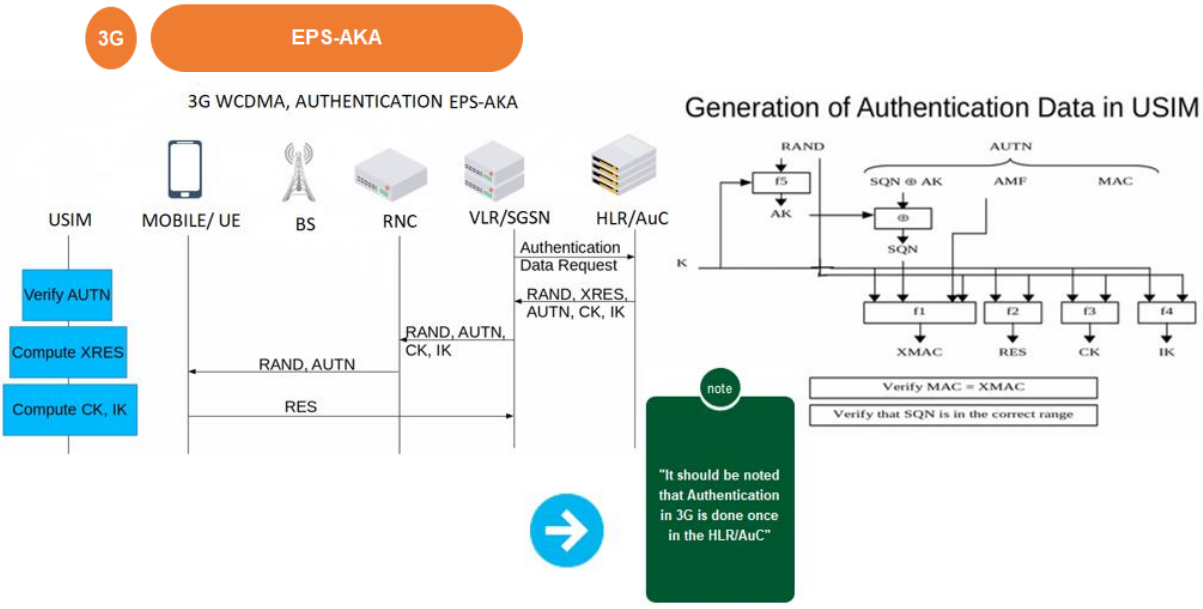
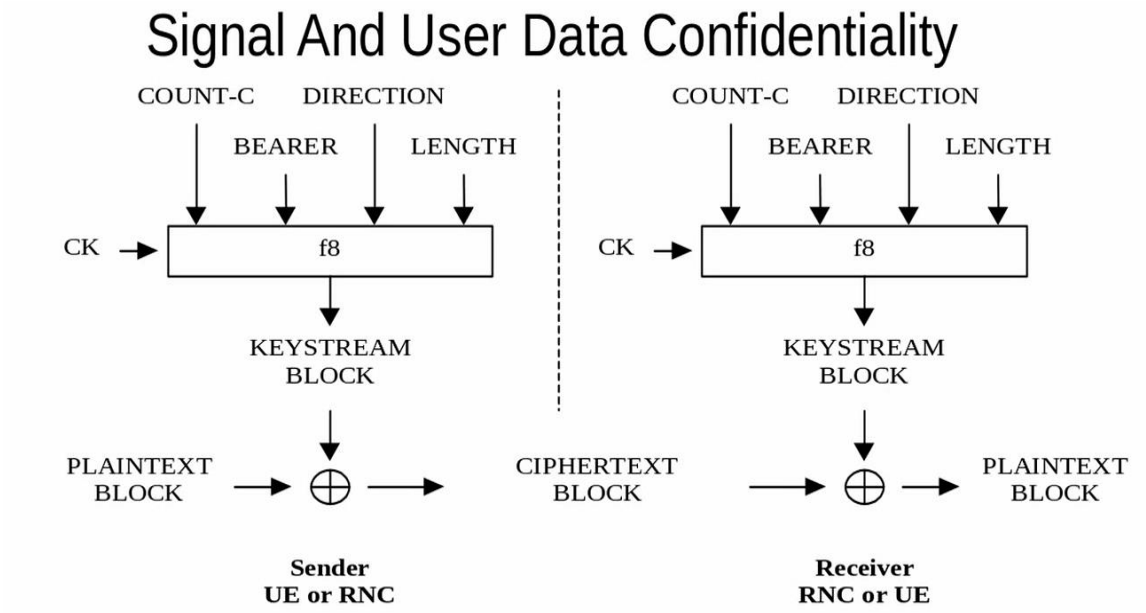


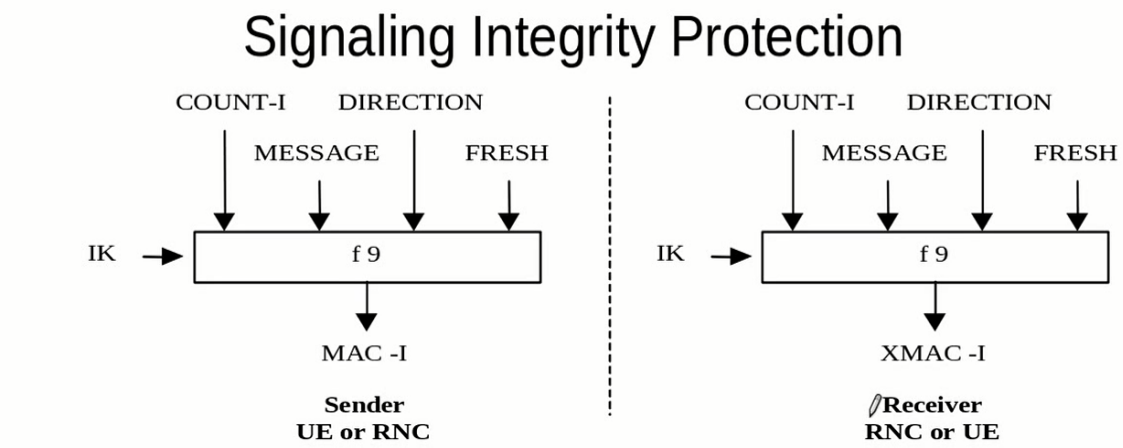
Figure 5:19: EPS AKA for 3G WCDMA

5.6.7.1 **3G Data Confidentiality and Integrity**



- BEARER – 5-bit Radio Bearer ID.
- LENGTH – 16-bit length of the plain text block. Used to determine the length of the kev stream block.

Figure 5:20: 3G Data Confidentiality



- IK – 128-bit Integrity Key
- MESSAGE – Signaling message .
- COUNT-I – 32-bit counter,
- DIRECTION – 1 bit set to 0 for Uplink and 1 for Downlink.
- FRESH – 32-bit random number generated by the RNC and sent to the UE in the Security

Figure 5:21: 3G Signaling Integrity

5.6.8 4G Security architecture, 4G LTE

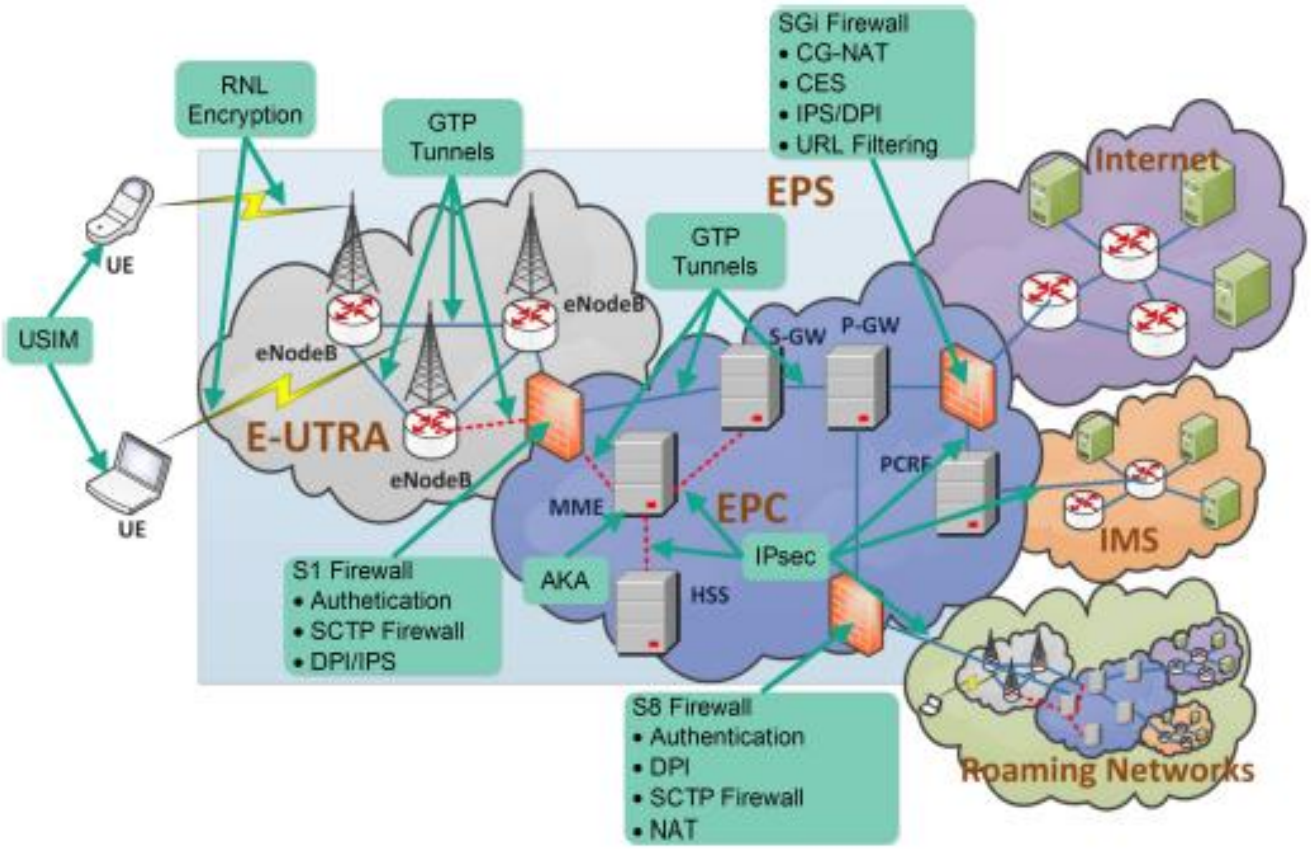


Figure 5:22: 4G Security architecture, 4G LTE

5.6.9 5G Security architecture, 4G vs 5G

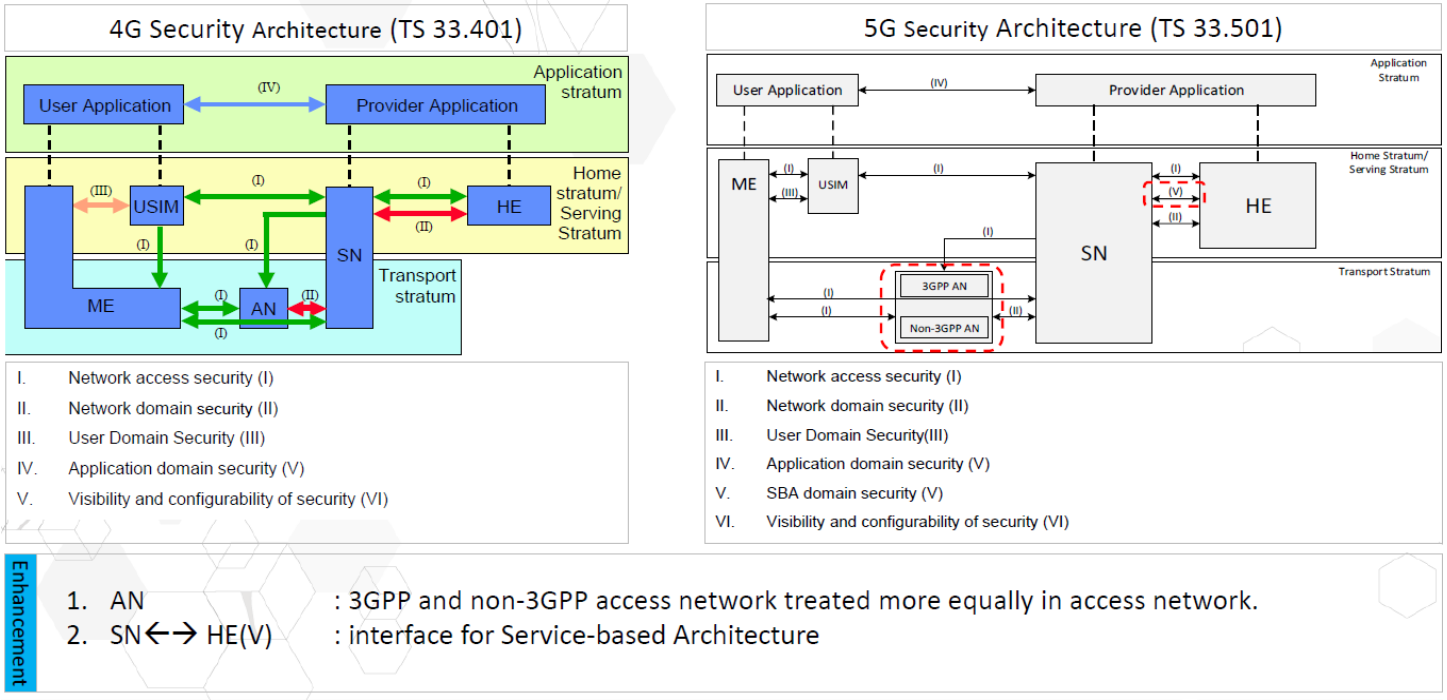


Figure 5:23: 5G Security architecture, 4G vs 5G

5.6.10 5G architecture, EPS-AKA vs 5G-AKA

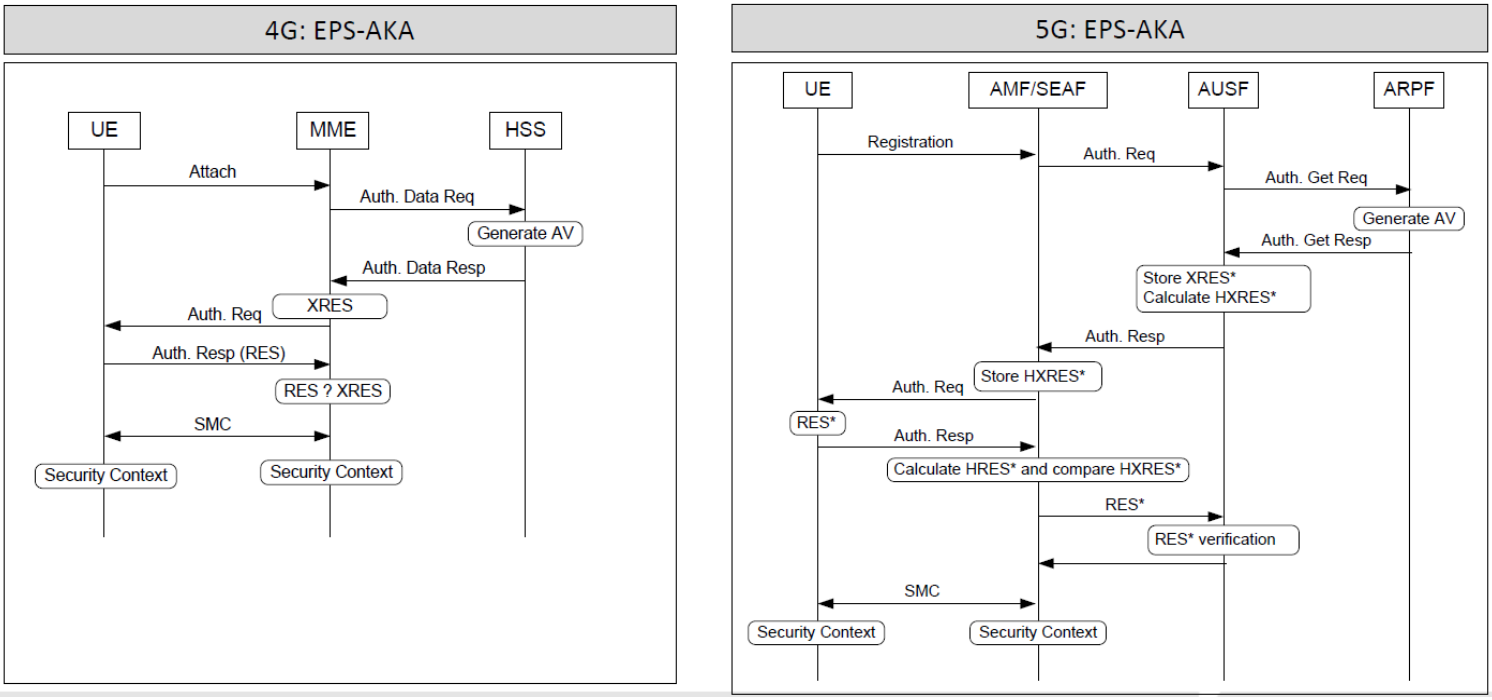


Figure 5:24: 5G architecture, EPS-AKA vs 5G-AKA

5.6.11 3GPP TS 23.501 Service Based Architecture for the 5G System.

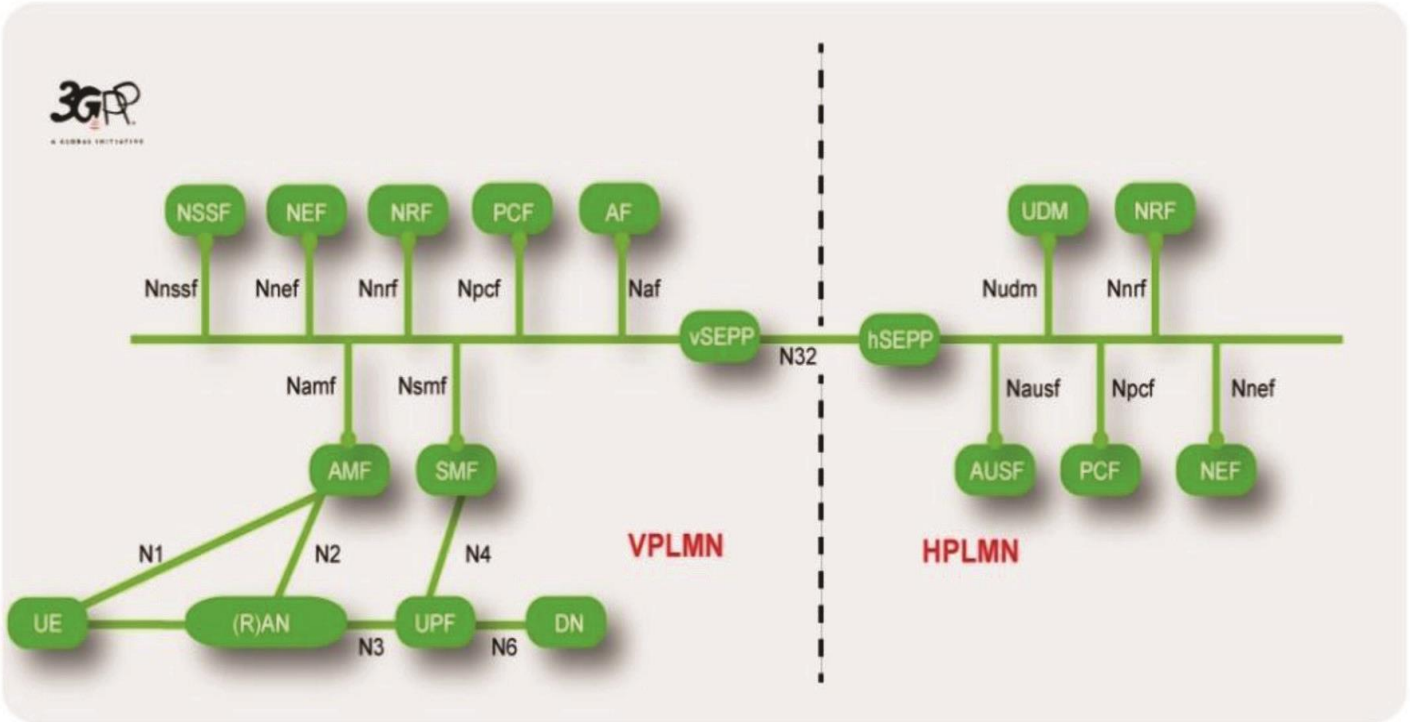


Figure 5:25: 3GPP TS 23.501 SBA for the 5G System

Source: 3GPP TS 23.501 – System Architecture for the 5G System; Stage 2

5.6.12 5G architecture, EAP-AKA' in 5G

Basic procedure:

1. UE send registration request to AUSF and ARPF
2. ARPF decide authentication method
3. AUSF start EAP-AKA'
4. UE and AUSF perform mutual authentication
5. AUSF send anchor key to SEAF/AMF for further key derivation
6. UE derive keys for communication.

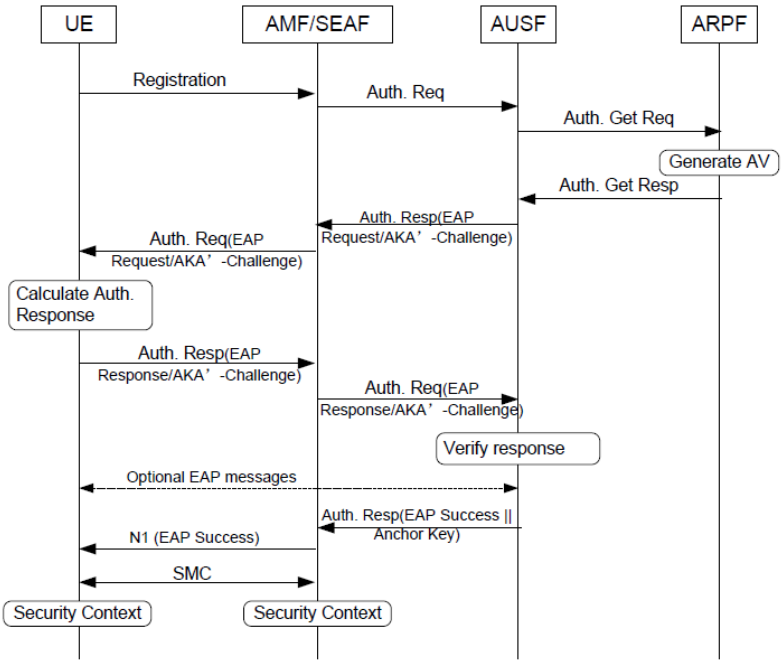


Figure 5:26: 5G architecture, EAP-AKA' in 5G

5.6.12.1 5G Architecture, Key Hierarchy

- Key hierarchy extended to also include:
  - K_{AUSF} at home network
  - K_{SEAF} at visited network
- Reasons for K_{AUSF}
  - Quick reauthentication
  - Protecting home to UE traffic, e.g. steering of roaming under discussion
- Reasons for K_{SEAF}:
  - Separate security anchor from mobility anchor
  - Pre-empts AMF at insecure locations

3GPP SA3 - 5G Security

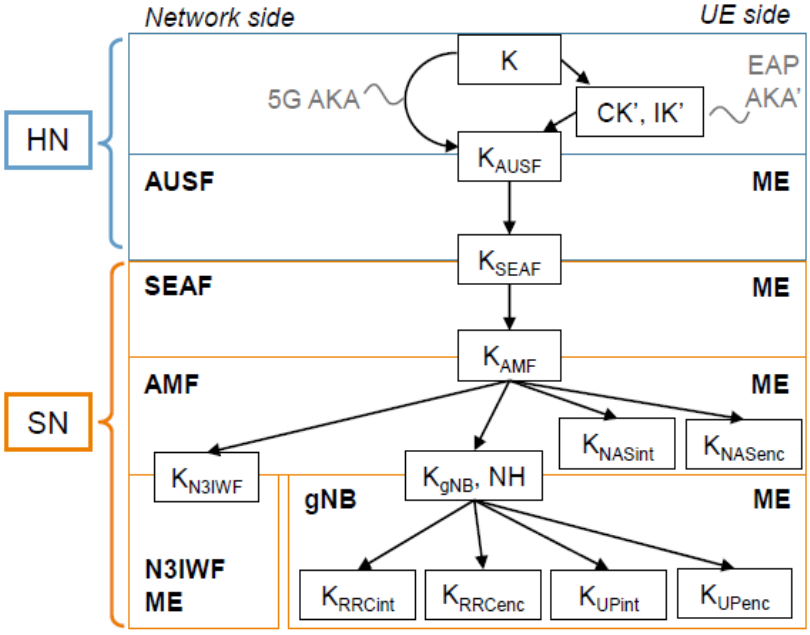


Figure 5:27: 5G Architecture, Key Hierarchy

5.6.13 5G Architecture, 5G-AKA

The 5G-AKA protocol is the flagship "Authentication and Key Agreement" protocol within the newly proposed 5G standard. The protocol is specified within §6.1.3.2 of 3GPP Technical Specification 33.501 (we model v0.7.0) [1], and is proposed as the main method of authentication and key agreement between a mobile device and its Home Network. The design of the 5G-AKA protocol is directly based on the EPS-AKA* protocol as used by 4G/LTE [2].1 5G-AKA is a four-party protocol (in both the roaming and non-roaming context). These parties are:

- UE: the 'User Equipment'. This can be for example mobile phones or USB 5G dongles. Each UE is uniquely identified by its SUbscription Permanent Identifier (SUPI). In 5G, the SUPI performs the same role as the 'IMSI' in pre-5G standards.
- SEAF: the 'Security Anchor Function'. In the roaming context, this is within the Serving Network.
- AUSF: the 'Authentication Server Function'. This role falls within the Home Network.
- ARPF: the 'Authentication credential Repository and Processing Function'. This also falls within the Home Network, and may typically reside within a secure location, such as a Hardware Security Module. [20][21]

Below is a complete guide I have compiled for a complete understanding of 5G authentication
In addition, some useful links to a researcher looking to understand more about the subject.
A complete guide to 5G-AKA has been provided below for further revision
https://drive.google.com/open?id=1vWAFqnvO3mGR8NqMqdiLqqLYlXpx-FBU
Also video at;
https://www.youtube.com/watch?v=86ntDaIcS4c&t=12s

Vulnerabilities in 5G AKA are defined in details in[22]

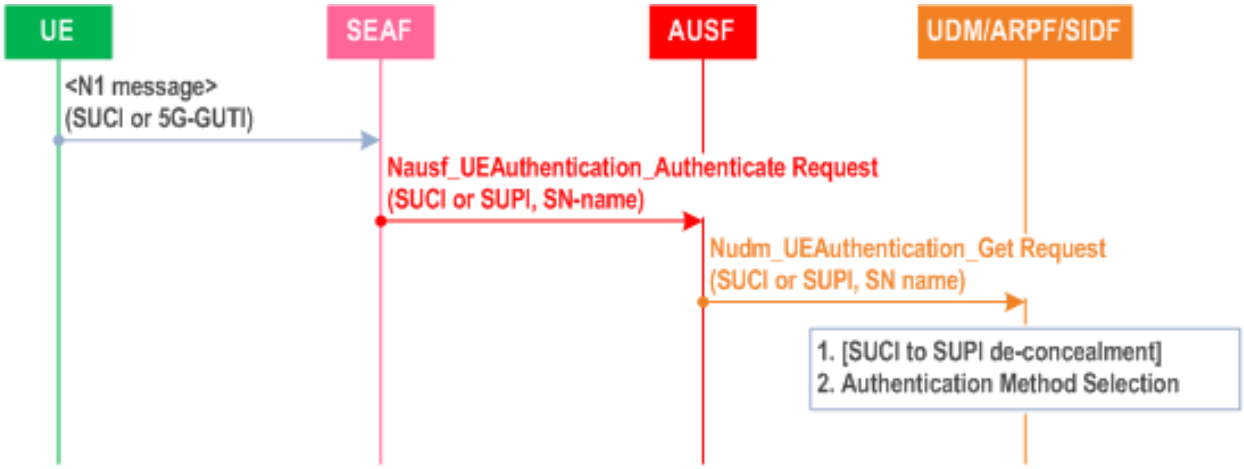


Figure 5:28: initiation of authentication & selection of auth. method

This step in 5G authentication is necessary because of two methods used for authentication ie, 5G-AKA, and EAP-AKA'.

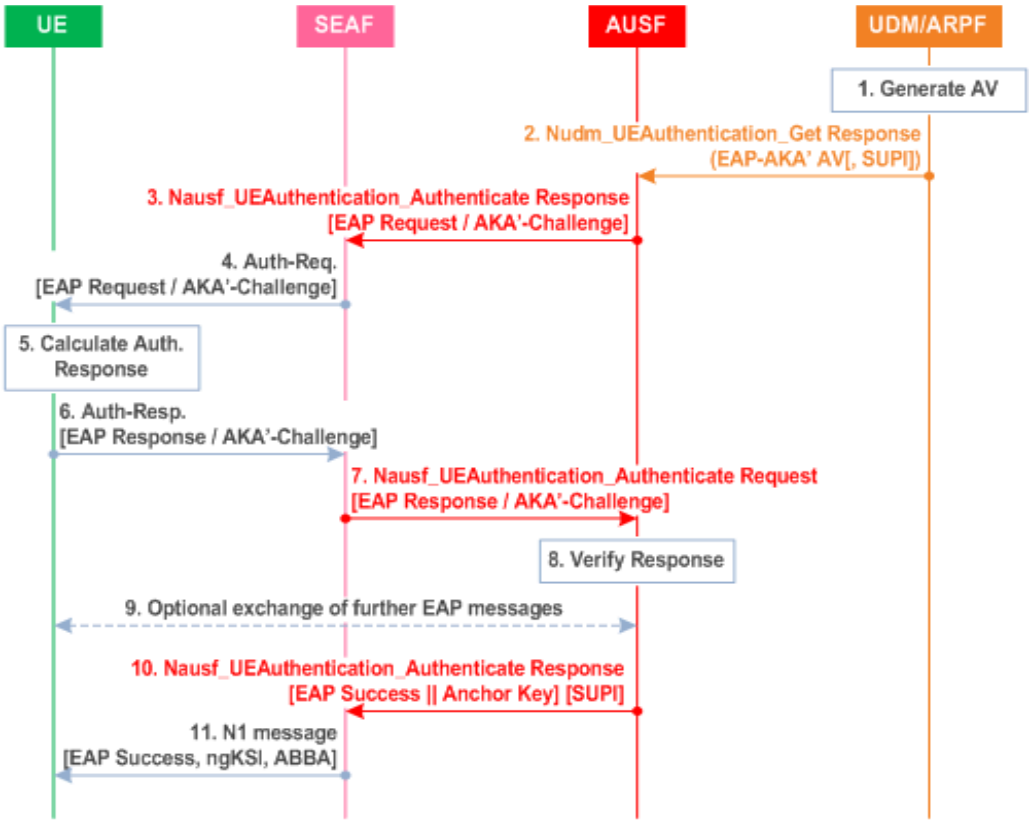


Figure 5:29: Authentication procedure for EAP AKA'

Further research on 5G-AKA, EAP-AKA'
https://www.semanticscholar.org/paper/The-5G-AKA-Authentication-Protocol-Privacy-Koutsos/240d9e8c7511c437f6deea8db7aba16134c03a76

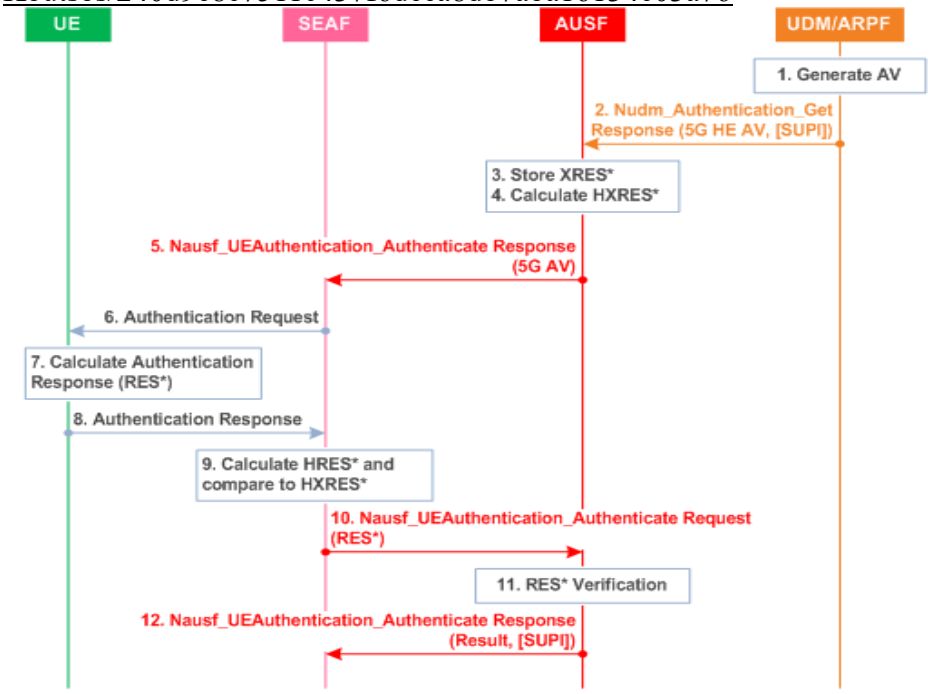


Figure 5:30: Authentication procedure for 5G AKA

source: https://www.tech-invite.com/3m33/toc/tinv-3gpp-33-501_c.html

5.7 REACTIVE/ OFFENSIVE TOOLS

These are activities and security measures taken after an attack has been recorded; these tools are carried out using Kali Linux operating system tools/ "backtrack" which is a package of cyber security tools, like Wireshark, metasploit, etc.

Activities done in Kali Linux operating system include, but not limited to the following;

- Pen-testing models
- Social Engineering

Documentations are available at https://www.kali.org/ and certification in offensive security at https://www.offensive-security.com/, the latter created Kali linux OS

5.7.1 CERT Operations

As also part of the reactive approach to cyber security, CERT operations can also be used to provide pre attack information, like discovered vulnerabilities, exploits, etc. although some activities are proactive too, a review is at https://www.cert.ug/, and https://www.ug-cert.ug/data/news/Alerts.html

Activities of Computer Emergency Response Team CERT;

Incident Handling;

- Incident analysis,
- Incident response support,
- Incident response coordination,
- Incident response on site.

Vulnerability Handling;

- Vulnerability analysis,
- Vulnerability response,
- Vulnerability response coordination, and
- Recovery handling, among others.

I have not demonstrated how **Snort** is used as IDS and IPS the operation of Wireshark, all of which are Kali Linux tools, the reader interested in advancing in pen-testing/ ethical hacking should refer to the links given above.

CHAPTER 5: RESULTS AND DISCUSSIONS

6.1 Wireless Encryption discussion:

6.1.1 WPA

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

6.1.2 WPA3

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. The new standard uses 128-bit encryption in WPA3-Personal mode (192-bit in WPA3-Enterprise) and forward secrecy. The WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals resulting in a more secure initial key exchange in personal mode. The Wi-Fi Alliance also claims that WPA3 will mitigate security issues posed by weak passwords and simplify the process of setting up devices with no display interface.

6.1.3 TKIP

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and provides a message integrity check. These avoid the problems of WEP.

6.1.4 EAP

The WPA-improvement over the IEEE 802.1X standard already improved the authentication and authorization for access of wireless and wired LANs. In addition to this, extra measures such as the Extensible Authentication Protocol (EAP) have initiated an even greater amount of security. This, as EAP uses a central authentication server. Unfortunately, during 2002 a Maryland professor discovered some shortcomings. Over the next few years, these shortcomings were addressed with the use of TLS and other enhancements. This new version of EAP is now called Extended EAP and is available in several versions; these include EAP-MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP, EAP-FAST, EAP-TLS, EAP-TTLS, MSCHAPv2, and EAP-SIM.

6.1.5 3GPP Authentication discussion:

EAP-SIM, EAP-AKA and EAP-AKA' are very similar. The TLV and packet format are virtually identical. The major differences are the Pseudo-Random Function (PRF) and Key Derivation Function (KDF) used to generate sessions keys, and the type of the authentication vectors used. The purpose of this KDF is usually to increase the key size, to modify the keys in such a way that they cannot be reused, and in the case of AKA' to bind the use of the keys to a particular network. EAP-SIM is the weakest, and EAP-AKA' is the strongest.

EAP-SIM should only be used with legacy 2G AuC that can only generate GSM authentication vectors. EAP-AKA should only be used where the supplicant does not support EAP-AKA'.

Advantages of EAP-SIM

- Easy to test locally as vectors can be generated and re-used and Works with all SIM cards.

Advantages of EAP-AKA over EAP-SIM

- Can optionally protect the identity negotiation portion of the exchange with a Checkcode (a digest of all identity packets).
- Stronger authentication and ciphering keys.
- AuC Supplicant authentication.
- Authentication vector re-use prevention with SQN.

Advantages of EAP-AKA' over EAP-AKA

- Stronger MAC digest (SHA-256 instead of SHA1).
- Stronger Checkcode digest (SHA-256 instead of SHA1).
- Stronger KDF (SHA-256 digest instead of SHA1).
- Network ID binding. Network ID is rolled into derived CK', IK' keys to prevent KDF output to prevent Network/SSID spoofing.

6.2 EXPENDITURE

The following was incurred durthe project goes on to completion; source of income is from Indian Women Association Uganda, my sponsors who gave me 2million Uganda shillings.

Item	Amount (Uganda Shillings)
LAPTOP	1,400,000
TEXT BOOKS	220,000
SOFTWARE	300,000
Total	1,920,000

Table 6.1: Implementation Costs

6.3 PROJECT SCHEDULE

The following Gantt chart was used as a timeline reference for the development process of the system expected towards the end of the project tasks.

2018/2019	2018					2019				
	Aug	Sept	Oct	Nov	Dec	Jan	Feb	March	April	May
Research/ Title selection										
Title submission/ Approval										
Proposal writing										
Proposal Presentation										
Literature Review										
Programming										
Kali Linux tool practice										
Policy Research										
Program Testing										
Report Writing										
Presentation										

Table 6.2: Gantt chart for the schedule

CHAPTER 6: CONCLUSION, RECOMMENDATIONS AND FUTURE RESEARCH WORK

7.1 SECURITY RECOMMENDATIONS BY ITU-T

Security dimensions are proposed by ITU-T in its security recommendation [6] to address almost all the aspects of network security. The security dimensions include a set of security measures that can be used to protect the users and network against all major security threats. These dimensions are:

Access Control: security measures that ensure only authorized personnel or devices access the network resources.

Authentication: security mechanisms that ensure identities of the communicating parties and that a user or device is not attempting a masquerade or unauthorized replay of previous communications.

Non-Repudiation: ensure that a particular action has been performed by a specific user or device is non-repudiation. Proper identities are used to ensure that authentic user or device can access particular services and resources.

Data Confidentiality: security mechanisms to protect the data from unauthorized access. Encryption, access control mechanisms and file permissions are used to ensure data confidentiality.

Communication Security: ensure that the data flows between the authorized endpoints and is not diverted or intercepted in between.

Data Integrity: ensures the correctness or accuracy of data in transmission and protects it from unauthorized modification, deletion, creation and replication.

Availability: ensures that there is no denial of authorized access to network resources and applications. Events affecting the network, such as system failures or disasters, scalability and security compromise, must not limit access to authorized users and devices.

Privacy: mechanisms that ensure protection of information, which might be derived from observing network activities.

7.2 CONCLUSION ON CIA TRIAD IN 5G

Authentication:

There are two kinds of authentications, namely, entity authentication and message authentication.

Entity authentication is used to ensure the communicating entity is the one that it claims to be. In the legacy cellular networks, mutual authentication between user equipment (UE) and mobility management entity (MME) is implemented before the two parties communicating to each other. The mutual authentications between UE and MME is the most important security feature in the traditional cellular security framework. The authentication and key agreement (AKA) in 4G LTE cellular networks is symmetric-key based.

However, 5G requires authentication not only between UE and MME but also between other third parties such as service providers.

Confidentiality:

Consists of two aspects, i.e., data confidentiality and privacy. Data confidentiality protects data transmission from passive attacks by limiting the data access to intended users only and preventing the access from or disclosure to unauthorized users.

Integrity:

Although message authentication provides the corroboration of the source of the message, there is no protection provided against the duplication or modification of the message.

Availability:

Availability is defined as the degree to which a service is accessible and usable to any legitimate users whenever and wherever it is requested.

7.3 5G SECURITY ARCHITECTURE CONCLUSION:

5G uses mobile clouds, SDN and NFV to meet the challenges of massive connectivity, flexibility, and costs as already stated. With all the benefits, these technologies also have inherent security challenges. Due to the limited standalone and integrated deployment of these technologies in 5G, the security threat vectors cannot be fully realized at this time. Security and privacy challenges will be more visible when more user devices e.g. IoT are connected and new diverse sets of services are offered in 5G, it is highly likely that new types of security threats and challenges will arise along with the deployment of novel 5G technologies and services. However, considering these challenges right from the initial design phases to the deployment will minimize the likelihood of potential security and privacy lapses.

Other applications like; Near-field communication **(NFC),** used in contactless payment systems, similar to those used in credit cards and electronic ticket smart cards and allow mobile payment to replace or supplement these systems. This is sometimes referred to as NFC/CTLS (contactless) or CTLS NFC. NFC is used for social networking, for sharing contacts, photos, videos or files,[wikipedia] also **D2D** applications in health care systems will require strong security systems, not forgetting massive **IoT** and **RFID** security improvements required for applications in 5G, as stated in the introduction, new futuristic applications will demand new security approaches due to their inherent security challenges.

REFERENCES

[1] https://5g-ppp.eu/white-papers/

[2] http://www-file.huawei.com//media/CORPORATE/PDF/ 5g_security_architecture_white_paper_en-v2.pdf?la=en

[3] https://www.huawei.com/en/press-events/news/2016/2/Demonstrate-5G-E2E-Network-Slicing-Technology

[4] https://www.survivingwithandroid.com/2016/06/iot-project-tutorial-smart-plant-system.html

[5]https://en.wikipedia.org/wiki/European_Technology_Platform_for_the_Electricity_Networks_of_the_Future

[6] Big Data for Dummies by Judith Hurwitz, Alan Nugent, Dr. Fern Halper, and Marcia Kaufman

[7] https://www.nist.gov/

[8] https://github.com/offensive-security/kali-arm-build-scripts

[9] https://www.offensive-security.com/kali-linux-arm-images/

[10] Handbook Of Security And Networks, editors Yang Xiao, Frank H Li, Hui Chen ISBN-13 978-981-4273-03-9

[11] Cyber Security Engineering A Practical Approach for Systems and Software Assurance, Nancy R. Mead and .Carol C. Woody, ISBN-13: 978-0-134-18980-2

[12] 3GPP TS 33.401, “Technical Specification Group Services and System Aspects: 3GPP System Architecture Evolution (SAE) Security architecture”.

[13] 3GPP TS 33.501, “Security architecture and procedures for 5G system”.

[14] Anand R. Prasad, Sivabalan Arumugam, Sheeba B and Alf Zugenmaier, “3GPP 5G Security”, Journal of ICT Standardization (River Publishers, Vol. 6, Iss. 1&2)-August (2016).

[15] “Key Points of 5G Security”, Opinion Pieces on Cyber Security (River Publishers)

[16] Tobias Engel. (December 2014). "SS7: Locate. Track. Manipulate" (Chaos Computer Club Berlin)

[17] GSMA RIFS: "Diameter Roaming Security - Proposed Permanent Reference Document".

[18] 3GPP TR 33.899, “Study on the security aspects of the next generation system”, Release 14, v 1.3.0-August (2017).

[19] https://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC

[20] 3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects (SA3): TS 33.401: 3GPP System Architecture Evolution (SAE); Security architecture (January 2018), version 15.2.0.

[21] Meier, S., Schmidt, B., Cremers, C., Basin, and D.A.: The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In: Computer Aided Verification - 25th International Conference, CAV. pp. 696–701 (2013)

[22] Martin Dehnel-Wild and Cas Cremers “Security vulnerability in 5G-AKA” draft (3GPP TS 33.501 draft v0.7.0), Department of Computer Science, University of Oxford. 8th February (2018)

[23] DONGFENG FANG , YI QIAN, ROSE QINGYANG HU “Security for 5G Mobile Wireless Networks”, Digital Object Identifier 10.1109/ACCESS.2017.2779146, Received October 25, 2017, accepted November 20, 2017, date of publication December 4, 2017, date of current version February 28, 2018.

APPENDICES

Table 9.1: SECURITY CHALLENGES IN 5G TECHNOLOGIES

Security Threat	Target Point/Network Element	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	X	X		X	
Hijacking attacks	SDN controller, hypervisor	X	X			
Signalling storms	5G core network elements			X	X	
Resource (slice) theft	Hypervisor, shared cloud resources		X		X	
Configuration attacks	SDN (virtual) switches, routers	X	X			
Saturation attacks	SDN controller and switches	X				
Penetration attacks	Virtual resources, clouds		X		X	
User identity theft	User information data bases				X	X
TCP level attacks	SDN controller-switch communication	X		X		
Man-in-the-middle attack	SDN controller-communication	X		X		X
Reset and IP spoofing	Control channels			X		
Scanning attacks	Open air interfaces			X		X
Security keys exposure	Unencrypted channels			X		
Semantic information attacks	Subscriber location			X		X
Timing attacks	Subscriber location				X	X
Boundary attacks	Subscriber location					X
IMSI catching attacks	Subscriber identity			X		X

Table 9.2: SECURITY TECHNOLOGIES AND SOLUTIONS

Security Technology	Primary Focus	Target Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS, DDoS detection	Security of centralized control points	X	X			
Configuration verification	Flow rules verification in SDN switches	X				
Access control	Control access to SDN and core network elements	X	X		X	
Traffic isolation	Ensures isolation for VNFs and virtual slices		X			
Link security	Provide security to control channels	X		X		
Identity verification	User identity verification for roaming and clouds services					X
Identity security	Ensure identity security of users					X
Location security	Ensure security of user location					X
IMSI security	Secure the subscriber identity through encryption					X
Mobile terminal security	Anti-malware technologies to secure mobile terminals					X
Integrity verification	Security of data and storage systems in clouds				X	
HX-DoS mitigation	Security for cloud web services				X	
Service access Control	Service-based access control security for clouds				X	

CODES FOR THE CHARACTER SUBSTITUTION

```
function password = passwordUIee(varargin)
% PASSWORDUI  Dialog for entering and creating passwords
%   PW = PASSWORDUI() brings up a dialog for entering a password.
%      The dialog masks the characters with a "*".
%   PW = PASSWORDUI(...) accepts up to 3 optional input arguments. The
%      arguments can be:
%      MODE - 'Query' or 'Create'. 'Query' asks the user to type the
%            password. 'Create' asks the user to create a new password.
%            This requires the user to type the password twice. Default
%            is 'Query'.
%      MIN  - a positive number that indicates the minimum number of
%            characters the password should have. This is only used when
%            the MODE is 'Create'. Default is 5.
%      TYPE - 'AlphaOnly', 'NumOnly', 'AlphaNum', or 'AlphaNumSpecial'.
%            Restricts the type of password when the MODE is 'Create'.
%            Default is 'AlphaOnly'.
%             'AlphaOnly' - Only alphabets.
%             'NumOnly'   - Only numbers.
%             'AlphaNum'  - Must have both alphabets and numbers but no
%                         special characters.
%             'AlphaNumSpecial' - Must have alphabets, numbers, and
%                         special characters.
%            Special characters:  !"#$%&'()*+,-./:;<=>?@[\]^_`{|}
%   Examples:
%      pw = passwordUI()
%      pw = passwordUI('Create', 'AlphaNum')
%      pw = passwordUI('Create', 'AlphaOnly', 8)
% Version History:
%   1.0 - Oct 2010.
% Jiro Doke
% Copyright 2010 The MathWorks, Inc.
%
            %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
             % This project has been used as demo for password hardening for educational                    purpose,
not commercial,%
            % by Muhanguzi Tobias
            %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
error(nargchk(0, 3, nargin, 'struct'));
% Defaults
uiMode = 'Query';
minChar = 5;
passwordType = 'AlphaOnly';
% Process input arguments
for id = 1:nargin
   if ischar(varargin{id})
      val = validatestring(varargin{id}, ...
         {'Query', 'Create', 'AlphaOnly', 'NumOnly', 'AlphaNum', ...
         'AlphaNumSpecial'});
      switch val
         case {'Query', 'Create'}
            uiMode = val;
         case {'AlphaOnly', 'NumOnly', 'AlphaNum', 'AlphaNumSpecial'}
            passwordType = val;
      end
   elseif isnumeric(varargin{id})
      validateattributes(varargin{id}, {'numeric'}, ...
```

```
            {'scalar', 'integer', 'positive'}, mfilename, 'MIN_CHAR');
        minChar = varargin{id};
    else
        error('JDUTILS:passwordUI:InvalidArguments', ...
            ['Invalid input arguments. Arguments must be a number ', ...
            '(minimum number of characters), "Query", "Create" ', ...
            '(UI mode), "AlphaOnly", "NumOnly", "AlphaNum", ', ...
            '"AlphaNumSpecial" (password type)']);
    end
end
num = 1;
canceled = false;
while true
    if strcmp(uiMode, 'Query')      % Query Mode
        dialogTitle = 'Enter Password:';
    else                            % Create Mode
        if num == 1     % First Try
            dialogTitle = sprintf('Create Password: %s', passwordType);
        else            % Re-type
            dialogTitle = sprintf('Retype Password: %s', passwordType);
        end
    end

    fh = figure(...
        'Visible', 'off', ...
        'Name', dialogTitle, ...
        'NumberTitle', 'off', ...
        'Units', 'Pixels', ...
        'Position', [0, 0, 500, 50], ...
        'Toolbar', 'none', ...
        'Menubar', 'none', ...
        'CloseRequestFcn', @closeFcn, ...
        'WindowStyle', 'modal', ...
        'KeyPressFcn', @passwordKeyPressFcn);

    th = uicontrol(...
        'Style', 'edit', ...
        'Units', 'Pixels', ...
        'Position', [10, 10, 480, 30], ...
        'BackgroundColor', 'white', ...
        'Enable', 'inactive', ...
        'String', '_', ...
        'FontName', 'FixedWidth', ...
        'FontSize', 10);

    movegui(fh, 'center');
    set(fh, 'Visible', 'on');

    % Default password
    password = '';

    uiwait(fh);
    drawnow;

    if canceled
        password = '';
        break;
    elseif strcmp(uiMode, 'Query')
        % "password" already has the characters
```

```
        break;
    else
        if num == 1  % First time through
            if isempty(password)
                return;
            end

            % Make sure the valid characters were typed
            s = validatePassword();
            if s   % if so, save that, and go to "retype"
                password1 = password;
                num = 2;
            end
        else        % Retype
            % Check to see if the two passwords match
            if isequal(password, password1)  % if so, break (OK)
                break;
            else   % if not, notify that they did not match, and go back to first try
                uiwait(warndlg('The passwords do not match', 'Error', 'modal'));
                num = 1;
            end
        end
    end

end
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Nested Functions
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%---------------------------------------------------------------------------
    function closeFcn(obj, edata) %#ok<INUSD>
        canceled = true;
        delete(obj);
    end
%---------------------------------------------------------------------------
    function success = validatePassword()
        success = false;

        % Check password length
        if length(password) < minChar
            uiwait(warndlg(sprintf('The password must be at least %d characters long.', minChar), 'Error', 'modal'));
            return;
        end

        % Check valid use of characters
        switch passwordType
            case 'AlphaOnly'        % Only alphabets
                if ~all(isstrprop(password, 'alpha'))
                    uiwait(warndlg('The password must be all alphabets.', 'Error', 'modal'));
                    return;
                end
            case 'NumOnly'          % Only numbers
                if ~all(isstrprop(password, 'digit'))
                    uiwait(warndlg('The password must be all numbers.', 'Error', 'modal'));
                    return;
                end
            case 'AlphaNum'         % Alphabets and numbers
                if ~all(isstrprop(password, 'alphanum')) || ...
                        ~(any(isstrprop(password, 'alpha')) && any(isstrprop(password, 'digit')))
                    uiwait(warndlg('The password must have alphabets and numbers.', 'Error', 'modal'));
```

```
                return;
            end
        case 'AlphaNumSpecial'  % Alphabets, numbers, and special characters
            if ~all(isstrprop(password, 'graphic')) || ...
                ~(any(isstrprop(password, 'alpha')) && any(isstrprop(password, 'digit')) && ...
                any(~(isstrprop(password, 'alpha') | isstrprop(password, 'digit'))))
                uiwait(warndlg('The password must have alphabets, numbers, and special characters.', 'Error',
'modal'));
                return;
            end
    end
    success = true;
  end
%--------------------------------------------------------------------------
  function passwordKeyPressFcn(obj, edata)
    switch edata.Key
        case 'return'
            delete(obj);
            return;
        case 'escape'
            canceled = true;
            delete(obj);
            return;
        case {'backspace', 'delete'}
            if ~isempty(password)
                password(end) = '';
            end
        otherwise
            c = edata.Character;
            if ~isempty(c)
                if c >= '!' && c <= '}'
                    password = [password, c];
                else
                    disp('Unrecognized character');
                end
            end
    end
    set(th, 'String', [repmat('*', 1, length(password)), '_']);
  end
end
```

CODE FOR MUNGED PASSWORDS

```
##   this application is used to convert a password according to the munged rules
## Munge my password
##Common words should still be avoided to be used as passwords. This challenge is about coding a very simple program that munges a given password
##(Modify Until Not Guessed Easily).
##Input
##A word, which is a string written in the alphabet abcdefghijklmnopqrstuvwxyz. It does not matter if the letters are lowercase or uppercase.
##Munging
##1.  Change any repeated sequence of a same letter to itself preceded by the number of times the letter was repeated (LLLL with 4L)
##2.  Change the first a with @
##3.  Change the first b with 8
##4.  Change the first c with (
##5.  Change the first d with 6
##6.  Change the first e with 3
##7.  Change the first f with #
##8.  Change the first g with 9
##9.  Change the first h with #
##10.  Change the first i with 1
##11.  Change the second i with !
##12.  Change the first k with <
##13.  Change the first l with 1
##14.  Change the second l with i
##15.  Change the first o with 0
##16.  Change the first q with 9
##17.  Change the first s with 5
##18.  Change the second s with $
##19.  Change the first t with +
##20.  Change the first v with >
##21.  Change the second v with <
##22.  Change the first w with uu
##23.  Change the second w with 2u
##24.  Change the first x with %
##25.  Change the first y with ?
##Rule 1 must be applied the needed number of times until it is not possible to apply it more. After that the rest of the rules are applied.
##Output The munged word
##Examples
##•  codegolf --> (0639o1#
##•  programming --> pr09r@2m1ng
##•  puzzles --> pu2z135
##•  passwords --> p@25uu0r6$
##•  wwww --> 4uu
##•  aaaaaaaaaaa --> 11a
##•  lllolllolll --> 3103io3l
##•  jjjmjjjj --> 3jm4j
import re
import tkinter
S =re.sub(r'(.)\1+', lambda m: str(len(m.group(0))) + m.group(1), input())
for a,b in zip('abcdefghiiklloqsstvvxyww',[*'@8(63#9#1!<1i095$+><%?','uu','2u']):S=S.replace(a,b,1)
for a,b in
zip('ABCDEFGHIIKLLOQSSTVVXYWW',[*'@8(63#9#1!<1i095$+><%?','UU','2U']):S=S.replace(a,b,1)
print(S)
```

DEFINITION OF TERMS

Application Function (AF):

The Application Function (AF) enables application influence on traffic routing, accessing NEF, interaction
User Plane Function (UPF)
The UPF implements part of the SGW and PGW functionality from LTE's EPC. In particular, it supports

Network Exposure Function (NEF):

The Network Exposure Function (NEF) enables external exposure capabilities of network functions for supporting Monitoring, Provisioning and Policy/Charging

Session Management Function (SMF):

The Session Management Function (SMF), as the name implies, handles management of UE sessions while also allocating IP addresses to UEs. It also selects and controls the UPF for data transfer.

Authentication Server Function (AUSF):

The AUSF component handles authentication requests for 3GPP access and non-3GPP access networks.
The AUSF interacts with the Security Anchor Function (SEAF) in order to authenticate the User Equipment (UE).

The major network functions in the control plane of the next generation core are identified in TR 23.799, which are utilized in our proposed security architecture as follows:

Access and mobility management function (AMF):

The function is applied to manage access control and mobility, which is implemented in MME for legacy cellular network. This can be vary with different use cases. Mobility management function is not necessary for fixed access applications.

Session management function (SMF):

Based on network policy, this function can set up and manage sessions. For a single AMF, multiple SMF can be assigned to manage different sessions of a single user.

Unified data management (UDM):

UDM manages subscriber data and profiles (such as authentication data of users) for both fixed and mobile access in the next generation core.

Policy control function (PCF):

This function provides roaming and mobility management, quality of service, and network slicing. AMF and SMF are controlled by PCF. Differentiated security can be provided with PCF.
AMF and SMF are integrated in the legacy cellular networks as MME. The separation of AMF and SMF can support a more flexible and scalable architecture. In the network function-based control plane, different network functions can be applied to different use cases