ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιθέσεις και Άμυνες στην Τεχνολογία 5G

(Attacks and Defenses in 5G Technology)

Νικόλαος Καραμάνης
Α.Μ. 20006
Νικόλαος Μουντάκης
Α.Μ. 20003

Εισηγήτρια: Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια

(Κενό φύλλο)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιθέσεις και Άμυνες στην Τεχνολογία 5G

(Attacks and Defenses in 5G Technology)

Νικόλαος Καραμάνης
Α.Μ. 20006
Νικόλαος Μουντάκης
Α.Μ.20003

Εισηγήτρια:
Καντζάβελου Ιωάννα, Επίκουρη Καθηγήτρια

Ioanna Kantzavelou Digitally signed by Ioanna Kantzavelou Date: 2022.07.12 11:30:32 +03'00'

Εξεταστική Επιτροπή:

Μπόγρης Αντώνιος, Καθηγητής Antonios Bogris Digitally signed by Antonios Bogris Date: 2022.07.12 23:51:08 +03'00'

Μάμαλης Βασίλειος, Καθηγητής Vasileios Mamalis Digitally signed by Vasileios Mamalis Date: 2022.07.13 02:53:41 +03'00'

Ημερομηνία εξέτασης 07/07/2022

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΩΝ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Καραμάνης Νικόλαος του Ηλία, με αριθμό μητρώου mcse20006 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών με ειδίκευση δικτύων υπολογιστών και κατανεμημένων συστημάτων του Τμήματος Μηχανικών πληροφορικής και υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:
«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Ο κάτωθι υπογεγραμμένος Μουντάκης Νικόλαος του Ιωάννη, με αριθμό μητρώου mcse20003 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών με ειδίκευση δικτύων υπολογιστών και κατανεμημένων συστημάτων του Τμήματος Μηχανικών πληροφορικής και υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:
«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Θα θέλαμε να ευχαριστήσουμε πολύ την κυρία Ιωάννα Καντζάβελου για την βοήθεια που μας παρείχε και την άψογη συνεργασία που είχαμε κατά την εκπόνηση της διπλωματικής μας εργασίας. Επίσης θα θέλαμε να ευχαριστήσουμε τις οικογένειες μας για την στήριξη και την υπομονή που έδειξαν καθ' όλη την διάρκεια της μεταπτυχιακής μας φοίτησης.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Οι επικοινωνίες πέμπτης γενιάς 5G, θα ενσωματώσουν αρκετές από τις υπάρχουσες τεχνολογίες αιχμής με νέες τεχνολογίες και τεχνικές. Αυτή η ολοκλήρωση θα οδηγήσει σε μεγάλές προκλήσεις στον τομέα της ασφάλειας για τα μελλοντικά́ δίκτυα κινητής τηλεφωνίας πέμπτης γενιάς. Το θέμα της διπλωματικής αυτής εργασίας, στοχεύει να αναδείξει τα ανοιχτά προβλήματα στην ασφάλεια των δικτυών 5G. Αρχικά, εντοπίζονται και περιγράφονται απειλές και μέθοδοι επιθέσεων, ενώ παράλληλα αντιστοιχούνται σε αυτές υπάρχοντες μηχανισμοί ασφάλειας που προσφέρουν μιας μορφής άμυνα, προστασία ή ανίχνευση. Θα εστιάσουμε και θα μελετήσουμε την αρχιτεκτονική και την ασφάλεια της τεχνολογίας 5G,τους πυλώνες της , τα πλεονεκτήματα και τους κινδύνους που κρύβει η συγκεκριμένη τεχνολογία. Ειδικότερα, αναμένεται ότι ένα ευρύ φάσμα θεμάτων ασφάλειας θα τεθεί σε 5G δίκτυα λόγω συγκεκριμενών παραγόντων που περιλαμβάνουν:

- Την ανοικτή αρχιτεκτονική της IP που βασίζεται στην IP 5G.
- Την πληθώρα διασυνδεδεμένων συσκευών επικοινωνίας.
- Την ετερογένεια των συσκευών.
- Τα ανοικτά λειτουργικά συστήματα των συσκευών.
- Τη χρήση διασυνδεδεμένων συσκευών από μη επαγγελματίες χρήστες σε θέματα ασφαλείας.

Τέλος, περιγράφονται τα ανοιχτά́ θέματα ασφάλειας που προκύπτουν από την ερευνητική́ αυτή εργασία, αξιολογείται η σοβαρότητα και η προτεραιότητά τους, και προτείνονται τρόποι αντιμετώπισής τους.

Η Διπλωματική αυτή αποτελείται από επτά κεφάλαια. Αρχικά, στο 1ο κεφάλαιο γίνεται μια εισαγωγή στην αρχιτεκτονική του 5G και αναφέρονται οι τυπικές περιπτώσεις χρήσεις των 5G δικτύων. Στο 2ο κεφάλαιο αναλύεται η ασφάλεια στα ασύρματα δίκτυα από τη γενιά του 1G έως και στο 5G. Στη συνέχεια αναφέρονται οι αρχές σχεδίασης για την ασφάλεια σε τεχνολογίες που χρησιμοποιούνται στο 5G όπως στο SDN, NFV και Cloud. Στο 3ο κεφάλαιο πραγματοποιείται μια αναφορά στην ασφάλεια IOT συσκευών και γίνεται ανάλυση των επιθέσεων και αντιμέτρων σε τέτοιου είδους συσκευές. Στο 4ο κεφάλαιο παρουσιάζεται η ταξινόμηση των απειλών στο 5G κατά ENISA. Στη συνέχεια στο 5ο κεφάλαιο μελετώνται μερικά σενάρια περιπτώσεων χρήσης και οι πιθανοί́ φορείς απειλής στις υποδομές του 5G. Τα σενάρια χρήσης περιλαμβάνουν περιπτώσεις στην πολιτική ,τα πρότυπα ,την αρχιτεκτονική και την εφοδιαστική αλυσίδα στο 5G. Λίγο πριν το τέλος στο 6ο κεφάλαιο αναλύονται με λεπτομέρειες οι πιο σύγχρονες ευπάθειες στα δίκτυα 5G αλλά και οι επιθέσεις σε αυτά. Καταληκτικά, στο 7ο και τελευταίο κεφάλαιο, γίνεται ο επίλογος της παρούσας διπλωματικής εργασίας, παρουσιάζοντας τα συμπεράσματα με βάση τα αποτελέσματα των σεναρίων, και προτείνοντας λύσεις για εφαρμογή στη συγκεκριμένη θεματική περιοχή.

ABSTRACT

Fifth generation 5G communications will integrate several of the existing cutting-edge technologies with new technologies and techniques. This integration will lead to major security challenges for future fifth-generation mobile networks. The subject of this dissertation aims to highlight the open problems in the security of 5G networks. Initially, threats and methods of attacks are identified and described, while at the same time existing security mechanisms corresponding to them, offer a form of defence, protection or detection. We will focus on and study the architecture and security of 5G technology, its pillars, the advantages and risks of this technology. In particular, it is expected that a wide range of security issues will be addressed in 5G networks due to specific factors including:

-The open IP architecture based on IP 5G.
-The variety of interconnected communication devices.
-The heterogeneity of the devices.
-Open operating systems of devices.
-The use of interconnected devices by non-professional users in security issues.

Finally, the open safety issues arising from this research work are described, their severity and priority are assessed, and ways of dealing with them are suggested.

This Thesis consists of seven chapters. Initially, the first chapter introduces the 5G architecture and mentions the typical uses of 5G networks. Chapter 2 analyzes security in wireless networks from the 1G up to 5G generation. Furthermore, there is a reference to the design principles for the security technologies used in 5G such as SDN, NFV and Cloud. Chapter 3 reports on the security of IoT devices and analyzes attacks and countermeasures on such devices. Chapter 4 presents the classification of threats in 5G according to ENISA. Chapter 5 then examines some use case scenarios and potential threat to 5G infrastructure. Use case scenarios include cases in 5G policy, standards, architecture and supply chain. Shortly before the end, in Chapter 6, the most modern vulnerabilities in 5G networks and the attacks on them are analyzed in detail. Finally, in the 7th and last chapter, the conclusion of this dissertation is referred, presenting the conclusions based on the results of the scenarios, and proposing solutions for implementation in the specific thematic area.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια στα δίκτυα 5G
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: 5G Security,5G Threats, Attacks on 5G Networks, Defences on 5G Networks

Πίνακας Περιεχομένων:

Κατάλογος Εικόνων

Κατάλογος Πινάκων

ΚΕΦΑΛΑΙΟ 1ο

ΕΙΣΑΓΩΓΗ

Μετά από σχεδόν τέσσερις δεκαετίες εξέλιξης και το πέρασμα από τέσσερις γενιές κινητών κυψελοειδών συστημάτων, τα συστήματα έχουν αλλάξει σημαντικά, από τα αναλογικά ή βασισμένα σε κυκλώματα ,σε συστήματα επικοινωνίας βασισμένα σε πακέτα. Στις δυο πρώτες γενιές είχαμε υποστήριξη φωνής και μετέπειτα κειμένου. Στο 3G είχαμε την μετάβαση στην ευζωνική πρόσβαση με την υποστήριξη ταχυτήτων δεδομένων εκατοντάδων kilobits/sec. έως μερικών megabits/sec με τεχνολογίες όπως η EVDO, HSPA και UMTS, ενώ με το 4G και τεχνολογίες όπως το WiMAX και LTE έχουμε υποστήριξη ρυθμού δεδομένων εκατοντάδων megabits/sec. Όπως είναι αντιληπτό είναι τεράστιες οι αλλαγές που έχουν γίνει με την εξέλιξη στο πέρασμα των χρόνων, όσων αφορά την ταχύτητα, το εύρος ζώνης αλλά και τον αριθμό των συνδεδεμένων συσκευών, ο οποίος έχει τεράστια αύξηση στις μέρες μας και ξεπερνά τα 30 δισεκατομμύρια συσκευές. Από αυτές ένας σημαντικός αριθμός, περίπου πάνω από τις μισές αφορά συσκευές που σχετίζονται με το Internet of Things (IoT). Αυτή η αύξηση των συσκευών που προκύπτει ουσιαστικά λόγω της μεγάλης αύξησης της ζήτησης των χρηστών που συμβαίνει λόγω και της εμφάνισης νέων υπηρεσιών, αλλά και την αύξηση επικοινωνιακών αναγκών από τομείς όπως η γεωργία, η αυτοκινητοβιομηχανία, η υγεία και οι μεταφορές, επέβαλλαν την ανάπτυξη της επόμενης γενιάς κινητού συστήματος του 5G.

1.1 Τι είναι το 5G

Τι είναι όμως το 5G. Το 5G είναι συντομογραφία της τεχνολογίας 5ης γενιάς για τα δίκτυα κινητής τηλεφωνίας, η εξέλιξη του ευρέως διαδεδομένου προτύπου 4G LTE. Άρχισε να αναπτύσσετε, για να διαδεχθεί το 4G ακριβώς όπως αυτό διαδέχθηκε το 3G. Το 5G όμως δεν αποτελεί απλά το επόμενο βήμα από το 4G, αλλά αποτελεί μια μεγάλη αλλαγή, καθώς έρχεται φέρνοντας μια νέα αρχιτεκτονική δικτύου πρόσβασης αξιοποιώντας πολλές βασικές αλλά και νέες τάσεις της τεχνολογίας , με τέτοιο τρόπο που του επιτρέπει πολύ μεγαλύτερη καινοτομία. [1]

Όπως το 3G έφερε την μετάβαση στην ευζωνική σύνδεση, έτσι και το 5G έρχεται φέρνοντας την υπόσχεση για μετάβαση από την ευζωνική συνδεσιμότητα σε μια πλούσια συλλογή υπηρεσιών και συσκευών. Έχει σχεδιαστεί για να παρέχει πολύ υψηλές ταχύτητες δεδομένων , πολύ μεγάλη χωρητικότητα δικτύου, μεγάλη διαθεσιμότητα και αξιοπιστία, δίνοντας ομοιόμορφη εμπειρία χρήστη σε περισσότερους ανθρώπους. Με όλα τα παραπάνω θα καταφέρει να παρέχει υποστήριξη σε διεπαφές χρήστη όπως AR (Augmented Reality) και VR (Virtual Reality) ,σε κρίσιμες εφαρμογές όπως αυτές που αφορούν δημόσια ασφάλεια ,αυτόνομα οχήματα και να υποστηρίξει το Διαδίκτυο των πραγμάτων (IoT). Όπως γίνεται αντιληπτό από τα παραπάνω, το 5G δεν θα υποστηρίζει μόνο την πρόσβαση των χρηστών στο διαδίκτυο από τα κινητά τους, αλλά και την πρόσβαση αυτόνομων συσκευών (πολλές φορές εκατοντάδων) που δουλεύουν μαζί για αυτούς. Η υποστήριξη όλων των παραπάνω δεν επιτυγχάνεται απλά με την αύξηση του εύρους ζώνης ή την μείωση της καθυστέρησης αλλά απαιτεί μια διαφορετική αρχιτεκτονική δικτύου. Το 5G αποτελεί ευκαιρία για την δημιουργία μιας πλατφόρμας που μπορεί να υποστηρίξει την καινοτομία. Σε αντίθεση με τα προηγούμενα δίκτυα που είχαν δημιουργηθεί και βελτιστοποιηθεί για συγκεκριμένες υπηρεσίες όπως κλήσεις μηνύματα κτλ. , το 5G σχεδιάστηκε σε μεγάλο βαθμό με στόχο να ενεργοποιήσει ακόμα και μελλοντικές εφαρμογές πέρα από αυτές που γνωρίζουμε σήμερα. [2]

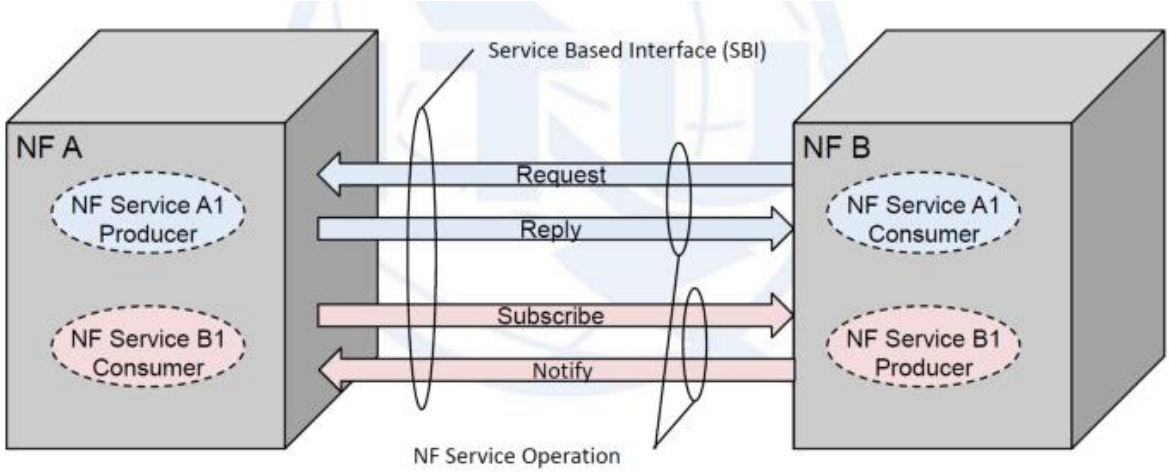
1.2 Η Αρχιτεκτονική πυρήνα του δικτύου 5G

Ο κύριος στόχος των προγενέστερων δικτύων κινητής τηλεφωνίας ήταν να προσφέρουν γρήγορες και αξιόπιστες υπηρεσίες δεδομένων κινητής τηλεφωνίας στους χρήστες. Το 5G έρχεται να διευρύνει αυτό το πεδίο και να προσφέρει ένα ευρύτερο φάσμα ασύρματων υπηρεσιών στον τελικό χρήστη που παρέχονται σε πλατφόρμες πολλαπλής πρόσβασης και δίκτυα πολλαπλών επιπέδων.

Το 5G είναι ουσιαστικά ένα δυναμικό, συνεκτικό και ευέλικτο πλαίσιο πολλαπλών προηγμένων τεχνολογιών που υποστηρίζουν μια ποικιλία εφαρμογών. Χρησιμοποιεί μια πολύ πιο έξυπνη αρχιτεκτονική, με τα Δίκτυα Πρόσβασης Ραδιοφώνου (RAN) να μην περιορίζονται από την εγγύτητα του σταθμού βάσης και την πολύπλοκη υποδομή.

Με το 5G ανοίγει ο δρόμος προς το διαχωρισμένο, ευέλικτο και εικονικό RAN μέσω νέων διεπαφών που δημιουργούν πρόσθετα σημεία πρόσβασης δεδομένων.

Το 3rd Generation Partnership Project (3GPP) καλύπτει τις τεχνολογίες τηλεπικοινωνιών, συμπεριλαμβανομένου και του RAN, βασικών δικτύων μεταφορών και δυνατοτήτων υπηρεσιών. Το 3GPP μας παράσχει τις πλήρεις προδιαγραφές του συστήματος για την αρχιτεκτονική του δικτύου 5G, η οποία είναι πιο προσανατολισμένη στις υπηρεσίες **(** service-oriented architecture,SOA) σε σχέση με τις προηγούμενες γενιές. [8]

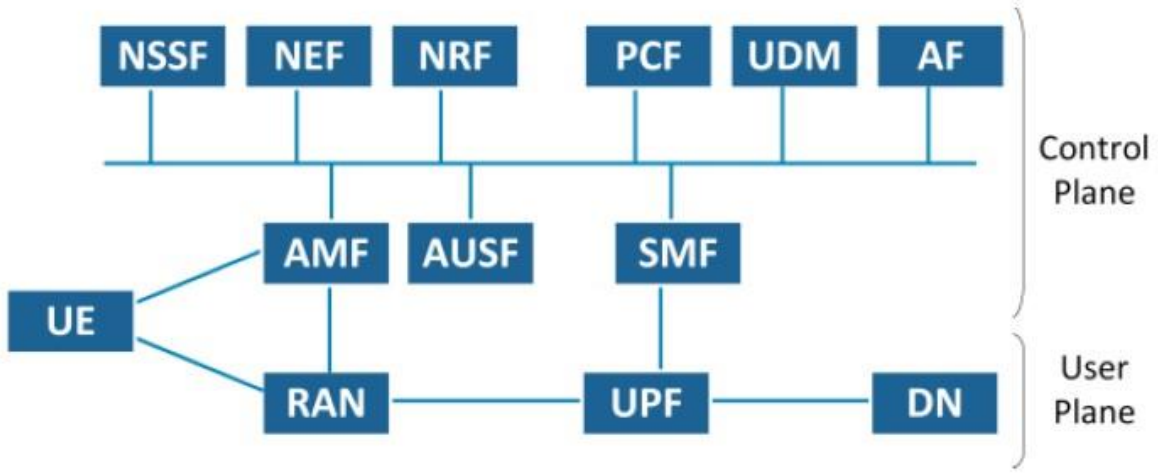


Εικόνα 1: Service-based interface [8]

Οι αρχιτεκτονικές που βασίζονται σε υπηρεσίες έχουν χρησιμοποιηθεί στη βιομηχανία λογισμικού για τη βελτίωση της σπονδυλωτότητας των προϊόντων. Ένα προϊόν λογισμικού μπορεί να αναλυθεί σε υπηρεσίες επικοινωνίας. Με αυτήν την προσέγγιση, οι προγραμματιστές μπορούν να συνδυάσουν υπηρεσίες από διαφορετικούς προμηθευτές σε ένα μόνο προϊόν. Η σπονδυλωτότητα, η επαναχρησιμοποίηση και ο αυτοπεριορισμός των λειτουργιών του δικτύου είναι πρόσθετα ζητήματα σχεδιασμού της αρχιτεκτονικής του δικτύου 5G που και αυτή περιγράφεται στις προδιαγραφές του 3GPP. [8]

Το 3GPP στη φάση 1 του 5G,παρείχε μια τεχνική προδιαγραφή για τον καθορισμό της πρώτης αρχιτεκτονικής των συστημάτων 5G και τον καθορισμό των κύριων κόμβων και των αρμοδιοτήτων τους. Σε αυτήν την αρχιτεκτονική, το επίπεδο ελέγχου (control plane) και το επίπεδο δεδομένων (data plane) διαχωρίζονται όσο το δυνατόν περισσότερο για να επιτευχθεί μια πιο ευέλικτη και κλιμακούμενη ανάπτυξη. Αντί οι οντότητες του δικτύου να ομαδοποιούν πολλές λειτουργίες, το 3GPP προσπάθησε να

ορίσει Network Functions (Λειτουργίες Δικτύου) με περισσότερους ατομικούς ρόλους ,δηλαδή, μια συγκεκριμένη ευθύνη ανά λειτουργία. Ωστόσο, οι περισσότερες από αυτές τις NF είναι κατά κάποιο τρόπο μια χαρτογράφηση των υφιστάμενων οντοτήτων του 4G. Δύο αναπαραστάσεις είναι δυνατές για αλληλεπιδράσεις NF, η μία βασίζεται στην άποψη της αρχιτεκτονικής προσανατολισμένης στην υπηρεσία (SOA) και η άλλη βασίζεται σε παραδοσιακά σημεία αναφοράς. Στην αναπαράσταση που βασίζεται σε υπηρεσίες, ένα NF εκθέτει ένα σύνολο υπηρεσιών που προσφέρει σε άλλα NF και χρησιμοποιεί τις υπηρεσίες που παρέχονται από αυτά. Όλες οι αλληλεπιδράσεις πραγματοποιούνται από το ίδιο πρωτόκολλο για τις κλήσεις των API. Κάθε φορά που χρειάζεται να συνδεθεί ένα νέο NF, μόνο το νέο του Network Functions θα πρέπει να δηλώνεται σε άλλα στοιχεία. Στην αναπαράσταση σημείων αναφοράς, διατηρούνται συγκεκριμένοι σύνδεσμοι πρωτοκόλλου μεταξύ ζευγών NF. Στην εικόνα 2 βλέπουμε την προτεινόμενη από το 3GPP αρχιτεκτονική και σημεία αναφοράς για δίκτυα 5G.[3]



Εικόνα 2: Η αρχιτεκτονική 5G και οι κύριες λειτουργίες δικτύου του. RAN είναι το Δίκτυο πρόσβασης ραδιοφώνου (Radio Access Network).[3]

AMF-Λειτουργία πρόσβασης και κινητικότητας(Access and Mobility Function):Το AMF εκτελεί τις περισσότερες από τις λειτουργίες που εκτελεί το MME σε ένα δίκτυο 4G. Έχει διαφορετικές λειτουργίες, όπως έλεγχο ταυτότητας, πρόσβασης και εξουσιοδότηση, διαχείριση εγγραφής και διαχείριση κινητικότητας. Αφού στο 5G γίνεται χρήση διαφορετικών τεχνολογιών πρόσβασης, χρειάζεται ένα

κοινό πλαίσιο διαχείρισης πρόσβασης και για τον χειρισμό της κινητικότητας μεταξύ διαφορετικών προσβάσεων. Επομένως, το AMF θα υποστηρίζει 3GPP και μη 3GPP δίκτυα πρόσβασης. Σε αντίθεση με το 4G (όπου το MME χρησιμοποιείται για πρόσβαση 3GPP και ePDG για μη 3GPP), η δομή του πυρήνα δικτύου θα είναι κοινή για πρόσβαση 3GPP και μη 3GPP πρόσβαση, στο σύστημα 5G.

SMF- Λειτουργία διαχείρισης συνεδρίας (Session Management Function): Είναι υπεύθυνη για τη διαχείριση περιόδων σύνδεσης και ορισμένες άλλες λειτουργίες, όπως η εκχώρηση διευθύνσεων IP, ο έλεγχος της επιβολής πολιτικής και το QoS (η δημιουργία μιας συνεδρίας διαχωρίζεται πλήρως από τη διαχείριση κινητικότητας). Τόσο αυτή όσο και η AMF μπορούν να θεωρηθούν ως τμήμα του 4G MME

AUSF-Λειτουργία ελέγχου ταυτότητας διακομιστή (Authentication Server Function):Παρέχει ένα ενοποιημένο πλαίσιο για ζητήματα ελέγχου ταυτότητας (για πρόσβαση 3GPP καθώς και πρόσβαση εκτός 3GPP).

UDM-Ενοποιημένη διαχείριση δεδομένων (Unified Data Management):Περιέχει δεδομένα που σχετίζονταν με το HSS (δηλαδή δεδομένα χρήστη). Το UDM αποθηκεύει μόνο ένα μέρος των δεδομένων (όπως δεδομένα συνδρομής χρηστών) και όχι όλα. Υποστηρίζει επίσης επεξεργασία διαπιστευτηρίων, ελέγχου ταυτότητας, χειρισμό ταυτότητας χρήστη και εξουσιοδότηση πρόσβασης.

Η έννοια των δεδομένων στο 5G είναι λίγο διαφορετική, με τη διαφοροποίηση μεταξύ δομημένων δεδομένων και μη δομημένων δεδομένων. Τα δομημένα δεδομένα ανταλλάσσονται μεταξύ των NF με τυποποιημένο τρόπο, για να καταστεί δυνατή η επικοινωνία μεταξύ εξοπλισμού από διαφορετικούς προμηθευτές. Τα μη δομημένα δεδομένα είναι δεδομένα ειδικά για τον προμηθευτή που μπορούν να κρυφτούν σε άλλες λειτουργίες δικτύου. Τρεις νέες λειτουργίες ορίζονται σε αυτό το πλαίσιο:

SDSF-Λειτουργία δικτύου δομημένης αποθήκευσης δεδομένων(Structured Data Storage network function)

UDSF-Λειτουργία δικτύου μη δομημένης αποθήκευσης δεδομένων(Unstructured Data Storage network function)

UDR-Ενιαίο αποθετήριο δεδομένων (Unified Data Repository): Eίναι υπεύθυνο για την αποθήκευση ή την ανάκτηση δεδομένων συνδρομής και πολιτικής.

PCF-Λειτουργία Ελέγχου Πολιτικής (Policy Control Function):Σχετίζεται με το πλαίσιο πολιτικής και παρέχει κανόνες πολιτικής στα NF στο επίπεδο ελέγχου.

Οι παρακάτω λειτουργίες είναι για τη διαχείριση της εγκατάστασης των λειτουργιών δικτύου και των αλληλεπιδράσεων μεταξύ τους, σε μια προσέγγιση NFV (Εικονικοποιημένων λειτουργιών δικτύου):

NEF-Λειτουργία έκθεσης δικτύου (Network Exposure Function): Χειρίζεται όλες τις πληροφορίες και τις υπηρεσίες που μπορούν να εκτεθούν από τα NF σε τρίτους, όπως η κυκλοφορία πληροφοριών μεταξύ διαφορετικών NF στο επίπεδο ελέγχου.

NRF-Λειτουργία αποθετηρίου (NF Repository Function):Αποθηκεύει τα διαθέσιμα NF στο σύστημα και ενημερώνει άλλα NF για νέα NF. Στην service -based αναπαράσταση, κάθε φορά που προστίθεται ένα νέο NF στο σύστημα, πρέπει να ανακαλύπτεται από όλα τα άλλα NF.

NSSF-Λειτουργία επιλογής τμήματος δικτύου (Network Slice Selection Function): Καθορίζει το AMF που εξυπηρετεί για το UE και επιλέγει στιγμιότυπα τμημάτων δικτύου για αυτό (πέρα από την έννοια του τεμαχισμού δικτύου, τα στιγμιότυπα τμημάτων δικτύου παρέχουν συγκεκριμένες υπηρεσίες σε διαφορετικές επιχειρήσεις).

Τέλος, οι γενικές λειτουργίες αντιπροσωπεύουν το επίπεδο εφαρμογής, το επίπεδο μεταφοράς και το εξωτερικό δίκτυο δεδομένων:

AF-Λειτουργία Εφαρμογής (Application Function):Παρέχει υπηρεσίες σε τρίτους.

UPF-Λειτουργία επιπέδου χρήστη (User plane Function): Είναι υπεύθυνο για οτιδήποτε σχετίζεται με τα δεδομένα χρήστη.

DN-Δίκτυο δεδομένων (Data Network) :Είναι πρόσβαση στο Διαδίκτυο ή υπηρεσίες από φορείς εκμετάλλευσης και τρίτα μέρη. [3]

1.3 Τυπικές Περιπτώσεις Χρήσης Δικτύων 5G

Γενικά οι περιπτώσεις χρήσης των δικτύων 5G είναι πολλές και προέρχονται από τις χρήσεις, τις ανάγκες και τα οράματα διάφορων έργων, οργανισμών και

βιομηχανικών τομέων. Ωστόσο, τρεις είναι οι κύριες κατηγορίες περιπτώσεων χρήσης, οι οποίες έχουν οριστεί από την Διεθνή Ένωση Τηλεπικοινωνιών (ITU) και την 3rd Generation Partnership Project (3GPP). Αυτές περιλαμβάνουν:

i)Ενισχυμένη ευρυζωνικότητα κινητής τηλεφωνίας (Enhanced mobile broadband ,eMBB),

ii)Επικοινωνίες τύπου μαζικών μηχανών (Massive Machine Type Communication, mMTC)

iii) Αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (Ultra-reliable and low latency communications, URLLC). [2]

1.3.1 Ενισχυμένη ευρυζωνικότητα κινητής τηλεφωνίας (eMBB).

Το eMBB αφορά τη βελτίωση των περιπτώσεων χρήσης ευζωνικής κινητής τηλεφωνίας όπως αυτές υποστηρίζονται από το πρότυπο 4G Long Term Evolution (LTE). Οι περιπτώσεις χρήσης eMBB οι οποίες περιλαμβάνουν βελτιωμένες υπηρεσίες ενημέρωσης και ψυχαγωγίας , Wi-Fi, ροή βίντεο υψηλής ευκρίνειας για κινητά και άλλες χρήσεις, θα ενεργοποιούνται όλες από τις ταχύτερες ταχύτητες μετάδοσης δεδομένων του 5G, τη χαμηλότερη καθυστέρηση, τη μεγαλύτερη χωρητικότητα και άλλες βελτιώσεις απόδοσης. [2]

1.3.2 Επικοινωνίες τύπου μαζικών μηχανών (mMTC).

Οι επικοινωνίες τύπου μαζικών μηχανών έχουν να κάνουν με την ανάπτυξη μεγάλου αριθμού συνδεδεμένων συσκευών που εκπέμπουν σχετικά μικρές ποσότητες δεδομένων. Τέτοιες είναι συνήθως συσκευές όπως οι αισθητήρες αλλά και οι μετρητές κοινής ωφέλειας. Από αυτές τις συσκευές απαιτείται να έχουν πολύ χαμηλό κόστος αλλά και η διάρκεια ζωής της μπαταρίας τους να είναι μεγάλη. [2]

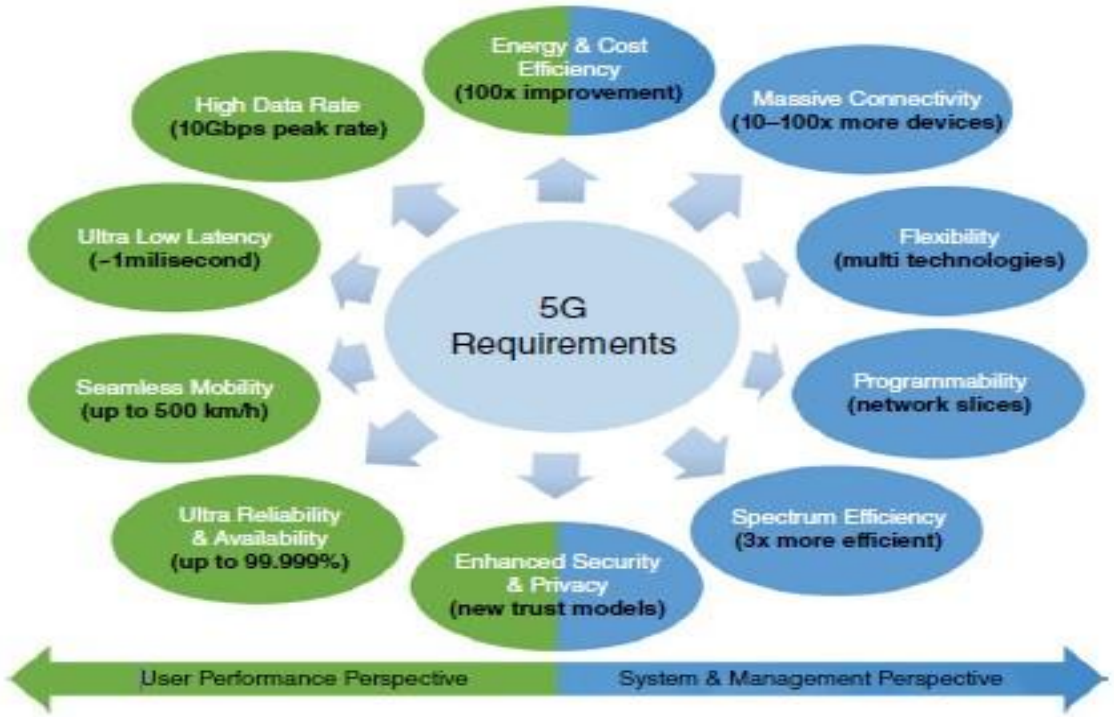
1.3.3 Αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (URLLC).

Σύμφωνα με την έκδοση 15 του 3GPP 5G-NR, το URLLC είναι ένα σύνολο χαρακτηριστικών που παρέχουν χαμηλή καθυστέρηση και εξαιρετικά υψηλή

αξιοπιστία για κρίσιμες εφαρμογές όπως το βιομηχανικό διαδίκτυο, τα έξυπνα δίκτυα, η απομακρυσμένη χειρουργική, τα αυτοκίνητα αυτόνομης οδήγησης, ο βιομηχανικός αυτοματισμός, τα έξυπνα συστήματα μεταφορών κ.α. Η 3GPP εκτός από το eMBB, έχει καθορίσει και το URLLC ως βασικό χαρακτηριστικό για την έκδοση 15 5G NR. Σύμφωνα με την Έκδοση 14 του 3GPP, η καθυστέρηση με 4G LTE είναι στην περιοχή των 4 χιλιοστών του δευτερολέπτου, αλλά με την εισαγωγή του URLLC στην έκδοση 15, ο στόχος είναι το 1 χιλιοστό του δευτερολέπτου. Το URLLC παρέχει επίσης ασφάλεια από άκρο σε άκρο και 99,999% αξιοπιστία. Ο σχεδιασμός μιας υπηρεσίας χαμηλής καθυστέρησης και υψηλής αξιοπιστίας περιλαμβάνει διάφορα στοιχεία όπως η ενσωματωμένη δομή πλαισίου ή απίστευτα γρήγορη ανάκαμψη, ο αποτελεσματικός έλεγχος και η κοινή χρήση πόρων δεδομένων. [2]

1.4 Απαιτήσεις 5G.

Σύμφωνα με διάφορους οργανισμούς, εταιρείες και ερευνητικές κοινότητες έχει εντοπιστεί ένας μεγάλος αριθμός απαιτήσεων για το 5G. Οι απαιτήσεις αυτές προέρχονται από τον τελικό χρήστη , την απόδοση του συστήματος, τις υπηρεσίες, τη λειτουργία και διαχείριση. Η εικόνα 3 συνοψίζει βασικές απαιτήσεις του 5G και μερικά παραδείγματα τιμών για κάθε απαίτηση. Κατ’ αρχάς, οι απαιτήσεις 5G μπορούν να παρουσιαστούν από την άποψη των προοπτικών απόδοσης του χρήστη, όπως ο ρυθμός δεδομένων, η καθυστέρηση, η κινητικότητα, η αξιοπιστία κ.λπ. αλλά και από την προοπτική της δικτύωσης και της διαχείρισης του συστήματος, όπως η πυκνότητα σύνδεσης, η ευελιξία του δικτύου, η ενεργειακή απόδοση και η απόδοση κόστους, κ.λπ. [4]



Εικόνα 3: Απαιτήσεις του 5G. [4]

1.4.1 Υψηλός ρυθμός δεδομένων και εξαιρετικά χαμηλή καθυστέρηση.

Μια πολύ σημαντική απαίτηση αφορά τον ρυθμό δεδομένων και την καθυστέρηση. Αυτές αποτελούν κύριες μετρήσεις αξιολόγησης για την αξιολόγηση της ποιότητας εμπειρίας των χρηστών στα ασύρματα επικοινωνιακά συστήματα. Όταν πρόκειται για την ανάπτυξη του συστήματος της γενιάς του 5G, αυτές οι δύο μετρήσεις είναι βασικές για την ικανοποίηση της ποιότητας της εμπειρίας του χρήστη. Οι απαιτήσεις που αφορούν το ρυθμό δεδομένων, μετριόνται ως ο μέγιστος ρυθμός δεδομένων ο οποίος είναι δυνατόν να επιτευχθεί για έναν χρήστη υπό ιδανικές συνθήκες και ο ρυθμός δεδομένων εμπειρίας χρήστη, ο ρυθμός δεδομένων που μπορεί να επιτευχθεί για έναν χρήστη στο πραγματικό δικτυακό περιβάλλον. Η εισαγωγή νέων εφαρμογών και υπηρεσιών που απαιτούν εύρος ζώνης, όπως η εικονική πραγματικότητα, η ροή βίντεο υψηλής ευκρίνειας ,απαιτεί μια ακραία βελτίωση των δικτύων 5G σε σύγκριση με τα δίκτυα 4G. Τα δίκτυα 5G θα φέρουν σημαντική βελτίωση στο μέγιστο ρυθμό δεδομένων. Μια βελτίωση που υπολογίζεται να φτάσει έως και τα 20 Gbps. Βελτίωση περίπου 100 φορές σε σχέση με τα δίκτυα 4G αναμένεται και στο ρυθμό δεδομένων εμπειρίας χρήστη. Η καθυστέρηση, το λεγόμενο latency αποτελεί άλλη μια πολύ

σημαντική απαίτηση. Η καθυστέρηση αυτή, ουσιαστικά αφορά την καθυστέρηση που αντιλαμβάνεται ο χρήστης με την χρήση μιας υπηρεσίας. Με την έλευση των πρόσφατων υπηρεσιών όπως το αυτοκινούμενο όχημα και ο αυτόματος έλεγχος κυκλοφορίας, που απαιτούν αποκρίσεις πραγματικού χρόνου και αλληλεπιδράσεις, η ελαχιστοποίηση της καθυστέρησης γίνεται όλο και πιο σημαντική. Σε σχέση με το 4G, το 5G , θα φέρει μεγάλη μείωση στον λανθάνοντα χρόνο τόσο στο επίπεδο του χρήστη όσο και στο επίπεδο ελέγχου. [4]

1.4.2 Τεράστια συνδεσιμότητα και απρόσκοπτη κινητικότητα

Όταν λέμε μαζική συνδεσιμότητα εννοούμε την απαίτηση για υποστήριξη μεγάλου αριθμού συνδεδεμένων συσκευών κάτι που συνεπάγεται ένα τεράστιο αριθμό συνδέσεων σε μια περιοχή . Η τεράστια αύξηση του αριθμού των συσκευών στη εποχή μας, την εποχή των 5G συστημάτων, οφείλεται εκτός από τις νέες υπηρεσίες και τους νέους τύπους συσκευών που έχουν κάνει την εμφάνιση τους και στην τεράστια αύξηση του αριθμού των συσκευών που υπήρχαν και παλαιότερα, όπως τα έξυπνα κινητά και οι φορητές ταμπλέτες. Για το λόγο αυτό το 5G θα πρέπει να παρέχει πυκνότητα σύνδεσης έως και ενός δισεκατομμυρίου συνδεδεμένων συσκευών ανά τετραγωνικό χιλιόμετρο. Ένα άλλο στοιχείο που αποτελεί σημαντική απαίτηση στο 5G είναι η παροχή απρόσκοπτης εμπειρίας εξυπηρέτησης στο χρήστη κινητού. Παρόλα αυτά η απρόσκοπτη κινητικότητα δεν αποτελεί απαραίτητη απαίτηση καθώς όλες οι συσκευές στο 5G δεν είναι κινητά και όλοι οι χρήστες δεν είναι κινητοί χρήστες, κάτι που σημαίνει ότι θα πρέπει να υποστηρίζονται λύσεις κινητικότητας κατά απαίτηση. [4]

1.4.3 Αξιοπιστία και υψηλή διαθεσιμότητα.

Σημαντικές απαιτήσεις αποτελούν ακόμα η αξιοπιστία και η υψηλή διαθεσιμότητα. Όταν λέμε αξιοπιστία ενός συστήματος εννοούμε την εγγυημένη επιτυχία στη μετάδοση δεδομένων κάτω από συγκεκριμένες καθοριζόμενες συνθήκες για συγκεκριμένο χρονικό διάστημα. Το ποσοστό αξιοπιστίας θα αλλάζει ανάλογα με τις διαφορετικές περιπτώσεις χρήσεις και τις υπηρεσίες. Διάφορες υπηρεσίες που είναι και εξαιρετικά κρίσιμες όπως το e-health , ο αυτόματος έλεγχος κυκλοφορίας κ.α. , οι οποίες πρέπει να έχουν μεγάλη αξιοπιστία στην επικοινωνία, αποτελούν το λόγο για

τον οποίο το 5G αναμένεται να εγγυάται ένα πολύ υψηλό ποσοστό αξιοπιστίας που θα φτάνει έως και 99,999%. Η διαθεσιμότητα αναφέρεται ως η δυνατότητα παροχής υπηρεσιών κάθε στιγμή και οπουδήποτε. Τα συστήματα 5G θα πρέπει να είναι ικανά να μπορούν να ανταπεξέλθουν σε όλες τις περιπτώσεις πιθανής διακοπής της λειτουργίας τους. Η διαθεσιμότητα εκφράζεται συνήθως ως ποσοστό του χρόνου λειτουργίας σε μια δεδομένη περίοδο του χρόνου (π.χ. ένα έτος. [4]

1.4.4 Ευελιξία και Προγραμματισμός.

Οι απαιτήσεις που αφορούν την ευελιξία και τον προγραμματισμό είναι απαιτήσεις που είναι βασισμένες στο δίκτυο. Το 5G λόγω των διαφορετικών τεχνολογιών που το αποτελούν και την πληθώρα των συσκευών και των υπηρεσιών που καλείτε να υποστηρίξει, θα πρέπει να έχει μια αρχιτεκτονική που θα του δίνει την ευελιξία να μπορεί να ανταπεξέρχεται στις διαφορετικές απαιτήσεις που προκύπτουν από αυτές. Το πόσο ευέλικτο είναι ένα δίκτυο φαίνεται από την ικανότητα του να υποστηρίζει διαφόρων τύπων τεχνολογίες ραδιοπρόσβασης, δυνατότητα κλιμάκωσης των πόρων του δικτύου κατόπιν απαίτησης και ανεξάρτητα μεταξύ του δικτύου ραδιοπρόσβασης και του κεντρικού δικτύου, όπως επίσης και μεταξύ του επιπέδου ελέγχου και του επιπέδου δεδομένων. Επίσης από την δυνατότητα εγκατάστασης νέων υπηρεσιών και εφαρμογών σε πολύ σύντομο χρονικό διάστημα, και τη δυνατότητα αναδιαμόρφωσης της δικτυακής υποδομής σε πραγματικό χρόνο ώστε να προσαρμοστεί σε μια αλλαγή απαιτήσεων του χρήστη/πελάτη. Επίσης η υποδομή του δικτυού στο σύστημα 5G θα πρέπει να προγραμματίζεται αλλά και να επαναδιαμορφώνεταί. Για αυτό το λόγο δικτυακή υποδομή του 5G θα αποτελείται από ένα σύνολο διαφορετικών εικονικών δίκτυών που θα βρίσκονται πάνω στην ίδια φυσική υποδομή. [4]

1.4.5 Ενέργεια, Κόστος και Απόδοση Φάσματος.

Παράλληλα με την ενίσχυση της χωρητικότητας του δικτύου και τη βελτίωση της εμπειρίας του χρήστη, η ενέργεια και η αποδοτικότητα κόστους αποτελούν μια σημαντική παράμετρο για το σχεδιασμό του 5G. Συγκεκριμένα, το σύστημα 5G αναμένεται να έχει εκατονταπλάσια βελτίωση στην ενέργεια και αποδοτικότητα σε σύγκριση με το σημερινό σύστημα 4G. Σημαντική παράμετρο για τα έσοδα των

εταιρειών κινητής, αποτελεί η αύξηση της αποδοτικότητας κόστους, που είναι μια οικονομική πτυχή του συστήματος 5G. Επιπλέον, όπως γνωρίζουμε, το 5G θα τροφοδοτείται όχι μόνο από ανθρωποκεντρικές συσκευές όπως τα smartphone, αλλά και από ένα τεράστιο αριθμό «πραγμάτων», όπως αισθητήρες, και έξυπνοι μετρητές, πράγματα που απαιτείται να έχουν πολύ μεγαλύτερη διάρκεια ζωής μπαταρίας για να λειτουργούν χωρίς περαιτέρω παροχή ρεύματος, για μεγάλα χρονικά διαστήματα. Η αύξηση της απόδοσης του φάσματος τέλος, αποτελεί άλλη μια παράμετρο η οποία θα πρέπει να βελτιωθεί σε σχέση με τα προγενέστερα συστήματα. [4]

1.4.6 Ασφάλεια και Απόρρητο.

Κλείνοντας το κομμάτι των απαιτήσεων θα αναφερθούμε σε άλλη μια σημαντική απαίτηση στα 5G συστήματα που είναι η ασφάλεια. Η ασφάλεια αποτελεί σημαντική απαίτηση γιατί η εισαγωγή διαφοροποιημένων υπηρεσιών και συσκευών θα δημιουργήσει πολλές προκλήσεις για τη διασφάλιση στο 5G. Πιο συγκεκριμένα, η ασφάλεια για το 5G θα πρέπει να είναι εγγυημένη σε διαφορετικά επίπεδα, συμπεριλαμβανομένου του επιπέδου πρόσβασης, του επιπέδου υποδομής και του επιπέδου υπηρεσιών. Η νέες τεχνολογίες που ενεργοποιούν το 5G όπως το SDN, NFV, τεμαχισμός δικτύου κ.λπ., είναι ανοιχτές και προγραμματιζόμενες πράγμα που φέρνει καινούργιες απαιτήσεις στο κομμάτι της ασφάλειας. Ακόμα νέα επίπεδα ασφαλείας απαιτούνται λόγω των νέων υπηρεσιών, όπως οι κρίσιμες υπηρεσίες (e-health, δημόσια ασφάλεια) που πρέπει να έχουν περισσότερη ασφάλεια από κάποιες άλλες. Ακόμα εφόσον θα προκύψουν νέοι εμπλεκόμενοι φορείς με διαφορετικά μοντέλα επιχειρήσεων θα έρθουν και νέα μοντέλα παροχής. Σημαντικές είναι επίσης οι ανησυχίες για το απόρρητο και πρέπει επίσης να ληφθούν υπόψη στο 5G. Τα δίκτυα 5G θα φιλοξενήσουν τεράστιο αριθμό συσκευών χρηστών, δηλαδή θα μεταφερθεί μεγάλος όγκος πληροφοριών απορρήτου χρήστη, όπως τα αναγνωριστικά χρήστη μέσω του δικτύου. Επομένως, χρειάζεται ένας αποτελεσματικός τρόπο διαχείρισης για αυτόν τον τεράστιο όγκο πληροφοριών καθώς και για την προστασία και την πρόληψη της διαρροής των προσωπικών στοιχείων χρήστη. Για το κομμάτι του απορρήτου θα αναφερθούμε και σε επόμενο κεφάλαιο αναλυτικότερα. [4]

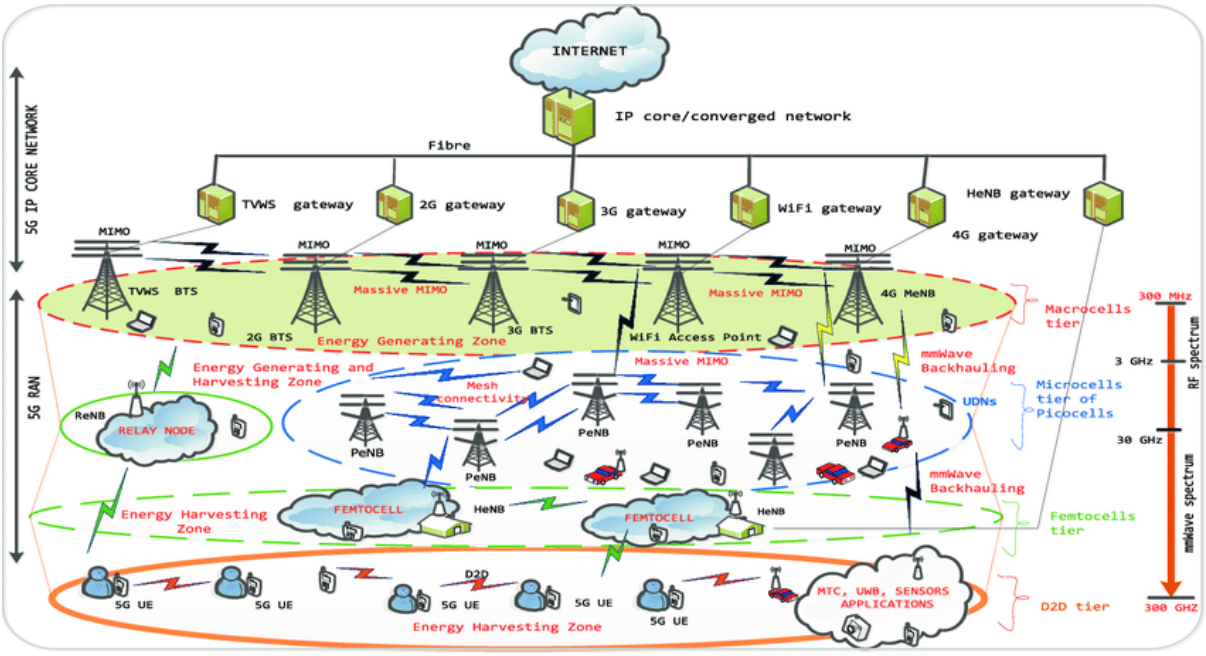
1.5 Οι τεχνολογίες που υλοποιούν το 5G.

Για την ικανοποίηση των απαιτήσεων που αναφέραμε προηγουμένως, μια σειρά από τεχνολογίες έχουν εξεταστεί. Το σύστημα από άκρο σε άκρο, το κεντρικό δίκτυο και το δίκτυο ραδιοπρόσβασης είναι τα μέρη στα οποία θα γίνει η ανάπτυξη της τεχνολογίας των συστημάτων 5G.

1.5.1 Δίκτυο ραδιοπρόσβασης 5G (RAN) .

Τα δίκτυα ραδιοπρόσβασης έχουν εξελιχθεί με την πάροδο των ετών καθώς η τεχνολογία κινητής τηλεφωνίας έφτασε στο 5G. Σήμερα, τα RAN μπορούν να υποστηρίξουν κεραίες πολλαπλής εισόδου, πολλαπλής εξόδου (MIMO), εύρη ζώνης μεγάλου φάσματος, συνάθροιση φορέα πολλαπλών ζωνών και πολλά άλλα. Αυτή η εξέλιξη του RAN για 5G θα έχει τεράστιο αντίκτυπο στις ασύρματες τεχνολογίες, συμπεριλαμβανομένης της ενεργοποίησης του Mobile Edge Computing (MEC) και του network slicing. Αυτά τα RAN του μέλλοντος θα συμβάλουν επίσης στη χαμηλότερη καθυστέρηση που κάνει το 5G πολύ ισχυρό. [14]

Οι τεχνολογίες ενεργοποίησης για το 5G RAN περιλαμβάνουν τις επικοινωνίες που θα δούμε παρακάτω.



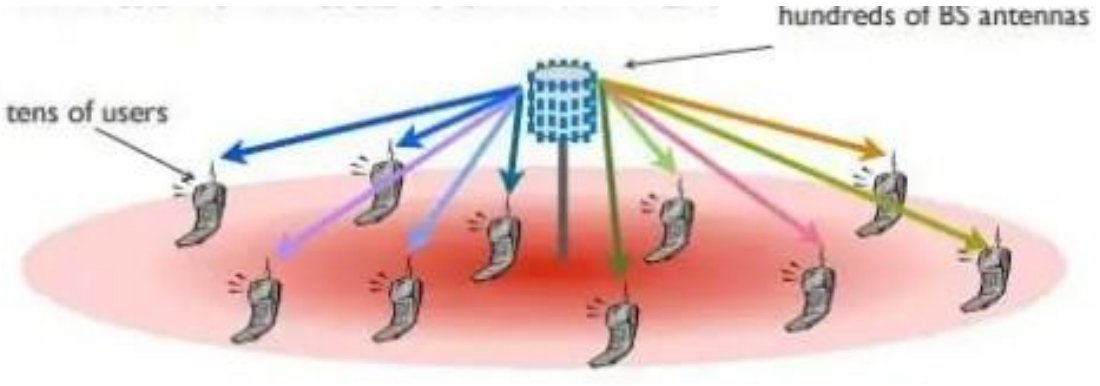
Εικόνα 4: Η Αρχιτεκτονική του 5G RAN συστήματος. [18]

1.5.1.1 mm Wave Communication.

Η χωρητικότητα έως και δεκάδες Gbps σε μέγιστο ρυθμό δεδομένων είναι ένα από σημαντικότερα χαρακτηριστικά του 5G, όμως τα υπάρχοντα ασύρματα συστήματα δεν επαρκούν στο 5G ώστε να πετύχει μεγαλύτερη διαθεσιμότητα φάσματος καθώς οι χρήσεις φάσματος τους, δεν επαρκούν για αυτό. Με την εκμετάλλευση υψηλών ζωνών φάσματος επιτυγχάνεται μια αποτελεσματική λύση για την επέκταση του εύρους ζώνης. Το mmWave με τα πλεονεκτήματα του ,τη παροχή μεγαλύτερου εύρους ζώνης και υψηλότερου ρυθμού μετάδοσης δεδομένων είναι μια πολλά υποσχόμενη τεχνολογία, ωστόσο προκλήσεις και ζητήματα όπως η παρέμβαση και η ετερογένεια θα πρέπει να επιλυθούν. [4]

1.5.1.2 Massive MIMO.

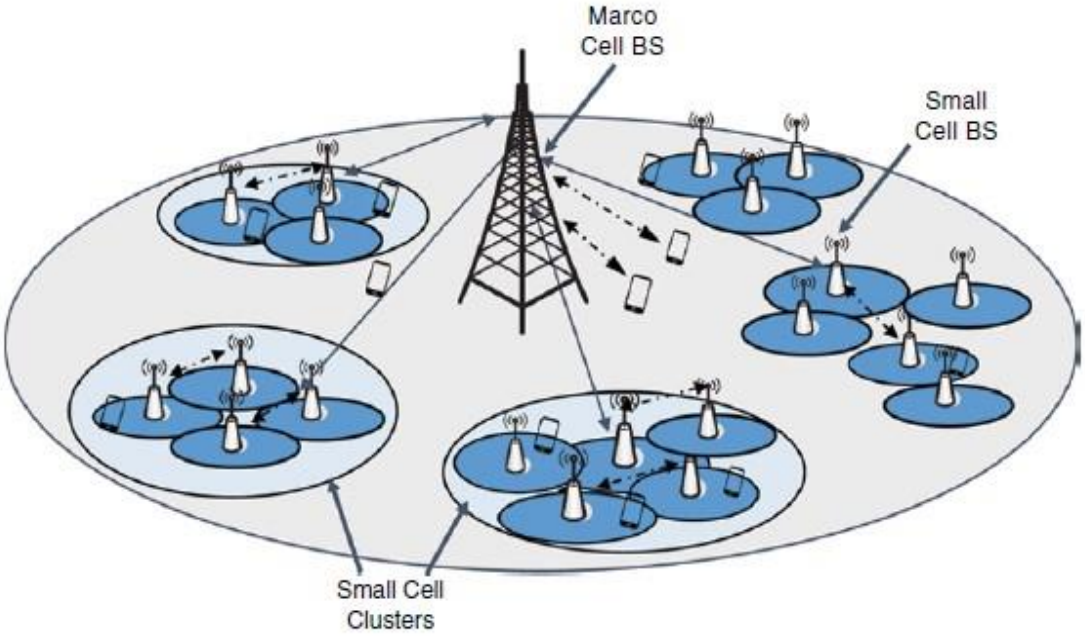
Massive MIMO είναι ουσιαστικά η τεχνική λύση που αφορά την συμπύκνωση του αριθμού των κεραιών που έχουν αναπτυχθεί. Με τον τρόπο αυτό ικανοποιούνται οι απαιτήσεις των συστημάτων του 5G ,που αφορούν την πυκνότητα και την χωρητικότητα του δικτύου. Ουσιαστικά στο MIMO γίνεται η χρήση πολλαπλών κεραιών για την μετάδοση και την λήψη δεδομένων. Είναι μια τεχνολογία κεραίας στις ασύρματες επικοινωνίες οι οποία χρησιμοποιείται και στα δίκτυα 4G και αναφέρεται στην επικοινωνία MIMO πολλών χρηστών, όπου πολλοί χρήστες εξυπηρετούνται ταυτόχρονα από μια πολλαπλή κεραία σταθμό βάσης. Το massive MIMO όμως ορίζεται ως ένα σύστημα MIMO πολλαπλών χρηστών, όπου ο αριθμός των κεραιών του σταθμού βάσης και ο αριθμός των χρηστών είναι μεγάλος. Έτσι η αύξηση της χωρητικότητας και της πυκνότητας του δικτύου θα έρθει από την ύπαρξη περισσότερων κεραιών στο σταθμό βάσης. Το massive MIMO είναι απαραίτητο για τα συστήματα 5G καθώς μέσω αυτού θα επιτευχθεί η βελτίωση στη φασματική και ενεργειακή απόδοση. [10]



Εικόνα 5: Παρουσίαση του Massive MIMO. [10]

1.5.1.3 Εξαιρετικά πυκνές μικρές κυψέλες.

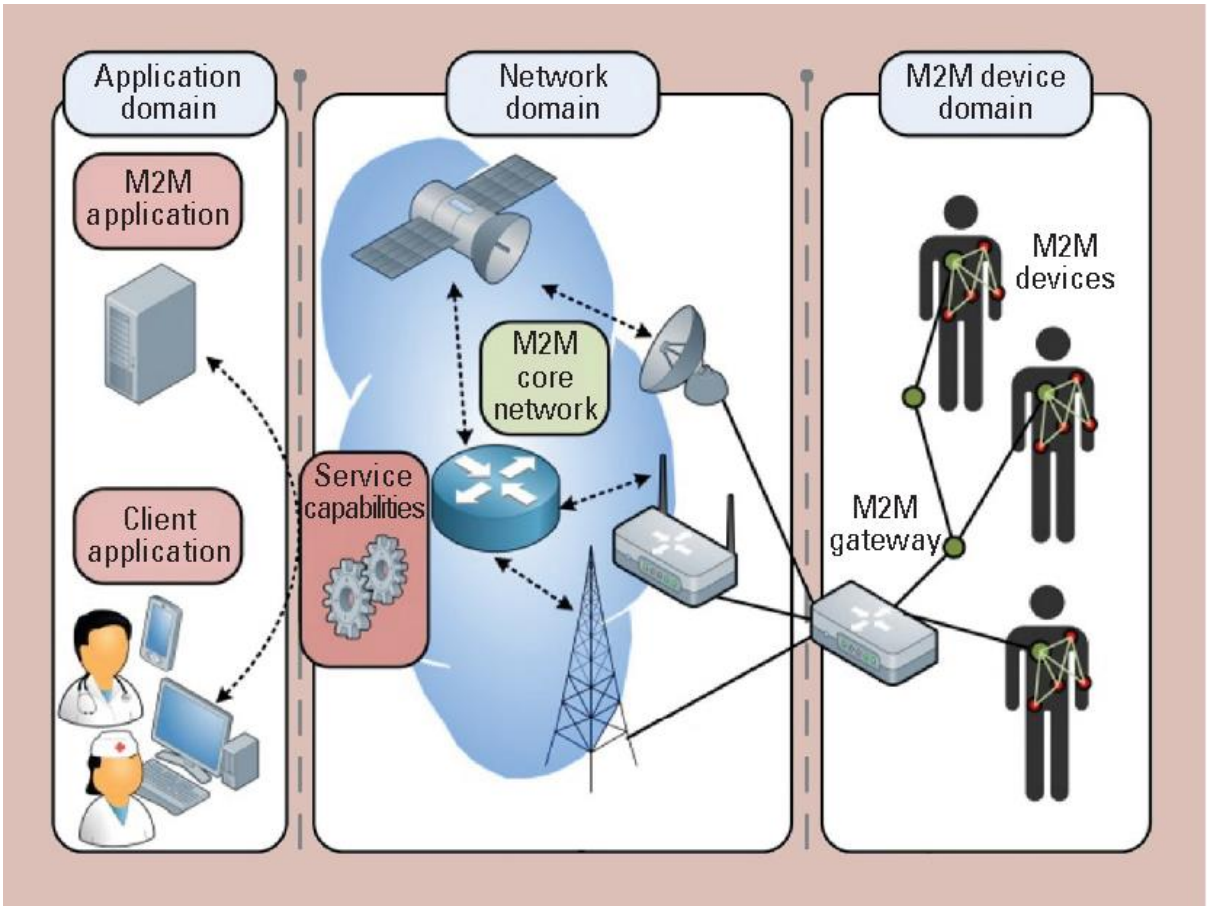
Η τεχνολογία των μικρών κυψελών αποτελεί άλλη μια τεχνική λύση για να βελτιωθεί η απόδοση και να αυξηθεί η πυκνότητα του δικτύου. Αυτό γίνεται μέσω της πύκνωσης του αριθμού των ασύρματων κόμβων, έτσι ώστε να έχουν μικρότερο εύρος κάλυψης σε σχέση με αυτούς που χρησιμοποιούνταν στα παλαιότερα συστήματα. Λέγοντας μικρές κυψέλες, μιλάμε για ραδιοφωνικούς κόμβους πρόσβασης, ελεγχόμενους από χειριστή, που έχουν χαμηλή κατανάλωση και εύρος κάλυψης που κυμαίνεται από 10 έως αρκετές εκατοντάδες μέτρα. Με την τεχνολογία των μικρών κυψελών το δίκτυο έρχεται πολύ πιο κοντά στον χρήστη, πράγμα που εξυπηρετεί καλύτερα περιοχές υψηλής κυκλοφορίας. Με τις μικρές κυψέλες επιτυγχάνεται μεγαλύτερος αριθμός σημείων μετάδοσης χαμηλής ισχύος, πράγμα που βελτιώνει τη φασματική απόδοση αφού γίνεται καλύτερη χρήσης των διαθέσιμων πόρων συχνότητας. Επιπλέον, το σύστημα 5G θα κατασκευαστεί με ετερογενή τρόπο, όπου τα μακρό και τα μικρά κελιά τοποθετούνται μαζί και ίσως συνδέονται μεταξύ τους μέσω ασύρματων συνδέσεων backhaul, παρέχοντας έτσι αυξημένα επίπεδα χωρητικότητας δικτύου μέσω εκφόρτωσης κυκλοφορίας. [4]



Εικόνα 6: Παρουσίαση ανάπτυξης μικρών κυψελών. [4]

1.5.1.4 Επικοινωνίες M2M και D2D.

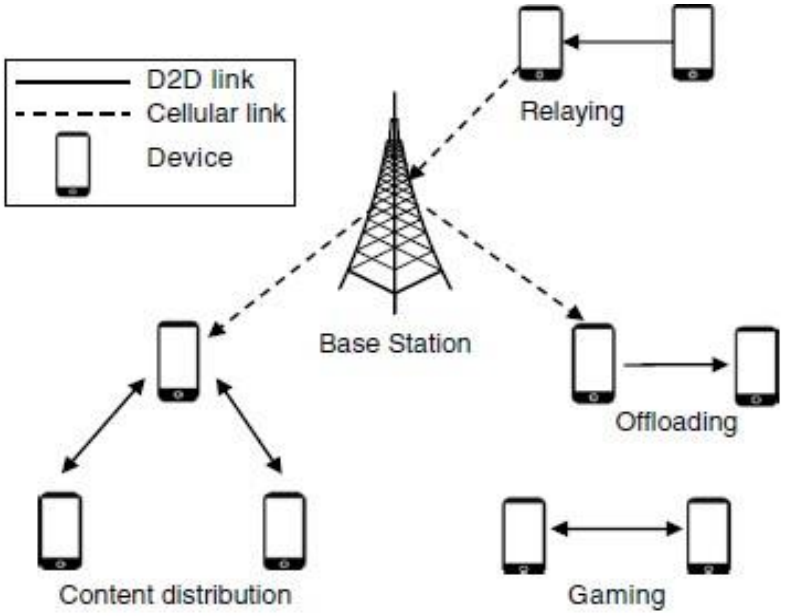
α) Επικοινωνία Machine-2-Machine (M2M).
Οι περισσότερες περίπτωσης χρήσης (τα δυο τρίτα) του 5G είναι σχετικές με το IoT και το Machine Type Communication. Οπότε οι επικοινωνίες M2M και MTC αποτελούν βασικούς παράγοντες στο σύστημα 5G παρότι έκαναν την εμφάνιση τους στα 4G συστήματα. Η M2M επικοινωνία έχει να κάνει με τις αυτοματοποιημένες επικοινωνίες δεδομένων, μεταξύ συσκευών και υποδομών μεταφοράς δεδομένων και αφορά επικοινωνίες δεδομένων τόσο μεταξύ μιας συσκευής MTC και ενός διακομιστή , αλλά και δυο συσκευών MTM απευθείας. Υπηρεσίες και εφαρμογές όπως το mobile health ενεργοποιούνται με την επικοινωνία M2M. Στην εικόνα παρακάτω φαίνεται η αρχιτεκτονική M2M για την περίπτωση του Mobile-Health. [4]



Εικόνα 7: Αρχιτεκτονική M2M για Mobile-Health. [11]

β) Device-2-Device (D2D) Επικοινωνία.

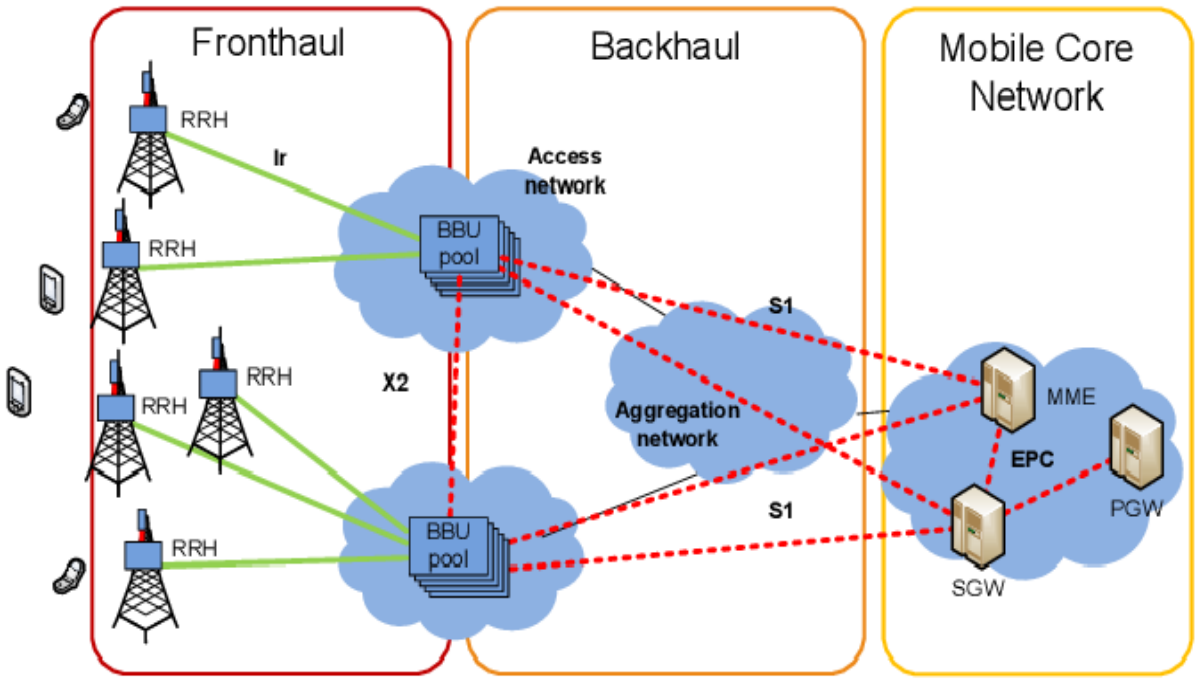
Η επικοινωνία χωρίς τη διέλευση από υποδομή δικτύου μεταξύ δύο κινητών χρηστών-συσκευών, είναι ουσιαστικά η D2D επικοινωνία. Καθορίστηκε από το 3GPP στην Έκδοση LTE 12. Αξιοποιώντας την άμεση επικοινωνία μεταξύ συσκευών, καθώς η επικοινωνία D2D μπορεί να βοηθήσει στη βελτίωση της αποδοτικότητας του φάσματος, τη βελτίωση του ρυθμού δεδομένων χρήστη, τη μείωση του λανθάνοντος χρόνου καθώς και της κατανάλωσης ενέργειας, πράγματα τα οποία θεωρούνται, βασικά στοιχεία του συστήματος 5G. Η D2D επικοινωνίας μπορεί να είναι τόσο εντός ζώνης σε αδειοδοτημένο φάσμα όπως το LTE όσο και εκτός ζώνης σε φάσμα μη αδειοδοτημένο όπως Wi-Fi. Υπάρχουν πολλές περιπτώσεις χρήσεις και σενάρια εφαρμογών για D2D, όπως υπηρεσίες εγγύτητας, παιχνίδια, δημόσια ασφάλεια, επικοινωνίες οχημάτων και εκφόρτωση, όπως φαίνεται στην εικόνα. [4]



Εικόνα 8: D2D επικοινωνία. [4]

1.5.1.5 Δίκτυο ραδιοπρόσβασης που βασίζεται σε νέφος (Cloud-based RAN).

Το δίκτυο ραδιοπρόσβασης που βασίζεται στο νέφος (Cloud-RAN) είναι η ιδανική λύση για το σχεδιασμό μέρους ραδιοπρόσβασης των δικτύων 5G, καθώς επιτρέπει την ενεργειακή απόδοση, την εξοικονόμηση κόστους πόρων βάσης ζώνης, βελτιώσεις στη χωρητικότητα του δικτύου και αυξημένη απόδοση. Το Cloud-RAN είναι ουσιαστικά η αποσύνδεση του Remote Radio Head (RRH) από τη μονάδα βάσης ζώνης (Baseband Unit,BU) ενός σταθμού βάσης και την υλοποίηση του BU σε ένα κεντρικό περιβάλλον υπολογιστικού νέφους. Η σύνδεση του Remote Radio Head με μια δεξαμενή Baseband Unit γίνεται με τη χρήση δικτύων fronthaul υψηλής ταχύτητας οπτικών ινών ή μικροκυμάτων. Εκτός από τα οφέλη που προσφέρει το Cloud-RAN στη σχεδίαση του συστήματος 5G,υπάρχουν διάφορες προκλήσεις που πρέπει να ξεπεραστούν πριν την πλήρη εκμετάλλευση των ωφελειών από αυτό, όπως οι περιορισμοί στο fronthaul και η βελτιστοποίηση της απόδοσης, η βελτιστοποιημένη τοποθέτηση των RRH, ο αποτελεσματικός προγραμματισμός και η ελαστική κλιμάκωση των BBU στη δεξαμενή των BBU. [4]

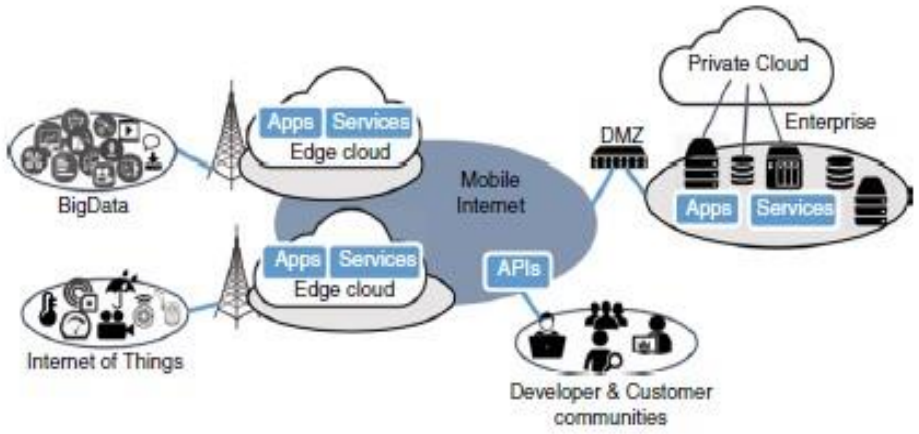


Εικόνα 9: Cloud-based RAN concept. [12]

1.5.1.6 Mobile Edge and Fog Computing.

Το Mobile Edge Computing και το Fog Computing είναι ουσιαστικά τεχνολογίες που φέρνουν τις υπηρεσίες πληροφορικής και τις δυνατότητες τις επεξεργασίας μέχρι την άκρη του δικτύου πολύ κοντά στο χρήστη, πράγμα που έχει ως αποτέλεσμα να επιτυγχάνονται πολύ μικρές καθυστερήσεις. Η τεχνολογία του MEC δεν είναι αποκλειστικά για το 5G, αλλά αποτελεί σίγουρα αναπόσπαστο στοιχείο της αποτελεσματικότητάς του . Χαρακτηριστικά του αποτελούν η χαμηλή καθυστέρηση, το υψηλό εύρος ζώνης και η πρόσβαση σε πραγματικό χρόνο στις πληροφορίες RAN που διακρίνουν την αρχιτεκτονική του 5G σε σχέση με τους προκατόχους του. Τα δίκτυα 5G όπως αυτά βασίζονται στις προδιαγραφές του 3GPP 5G,αποτελούν ιδανικό περιβάλλον για την ανάπτυξη του MEC. Οι προδιαγραφές του 5G καθορίζουν τις δυνατότητες για τους υπολογιστές αιχμής και επιτρέπουν στο MEC και το 5G να δρομολογούν μαζί την κυκλοφορία. Εκτός από τα πλεονεκτήματα του λανθάνοντος χρόνου και του εύρους ζώνης της αρχιτεκτονικής MEC, η κατανομή της υπολογιστικής ισχύος θα ευνοήσει τον μεγάλο όγκο συνδεδεμένων συσκευών που αποτελεί βασικό χαρακτηριστικό στην ανάπτυξη του 5G και την άνοδο του Διαδικτύου των Πραγμάτων

(IoT). Η εισαγωγή νέων υπηρεσιών και εφαρμογών από τους παρόχους υπηρεσιών και εκμετάλλευσης δικτύων θα επιτευχθεί μέσω των δυνατοτήτων του MEC. Παραδείγματα όπως το IoT και τα συνδεδεμένα αυτοκίνητα είναι παραδείγματα υπηρεσιών που οφείλονται στο MEC. Το Fog Computing είναι μια τεχνολογία όπου οι πόροι υπολογιστικού νέφους επεκτείνονται έως την άκρη του δικτύου για τη δημιουργία μιας πλατφόρμας που παρέχει αποθήκευση και δικτύωση υπηρεσιών, μεταξύ τελικών συσκευών και κέντρων δεδομένων. Μερικά από τα σημαντικότερα χαρακτηριστικά του FC, τα οποία το κάνουν κατάλληλο για τις 5G επικοινωνίες, είναι η χαμηλή καθυστέρηση, επίγνωση της τοποθεσίας, οι αλληλεπιδράσεις σε πραγματικό χρόνο, η υποστήριξη κινητικότητας, η γεωγραφική κατανομή και η υπεροχή της ασύρματης πρόσβασης. Η παρακάτω εικόνα απεικονίζει την έννοια του MEC και την αρχιτεκτονική του. [14]



Εικόνα 10: Αρχιτεκτονική του Mobile Edge Computing. [4]

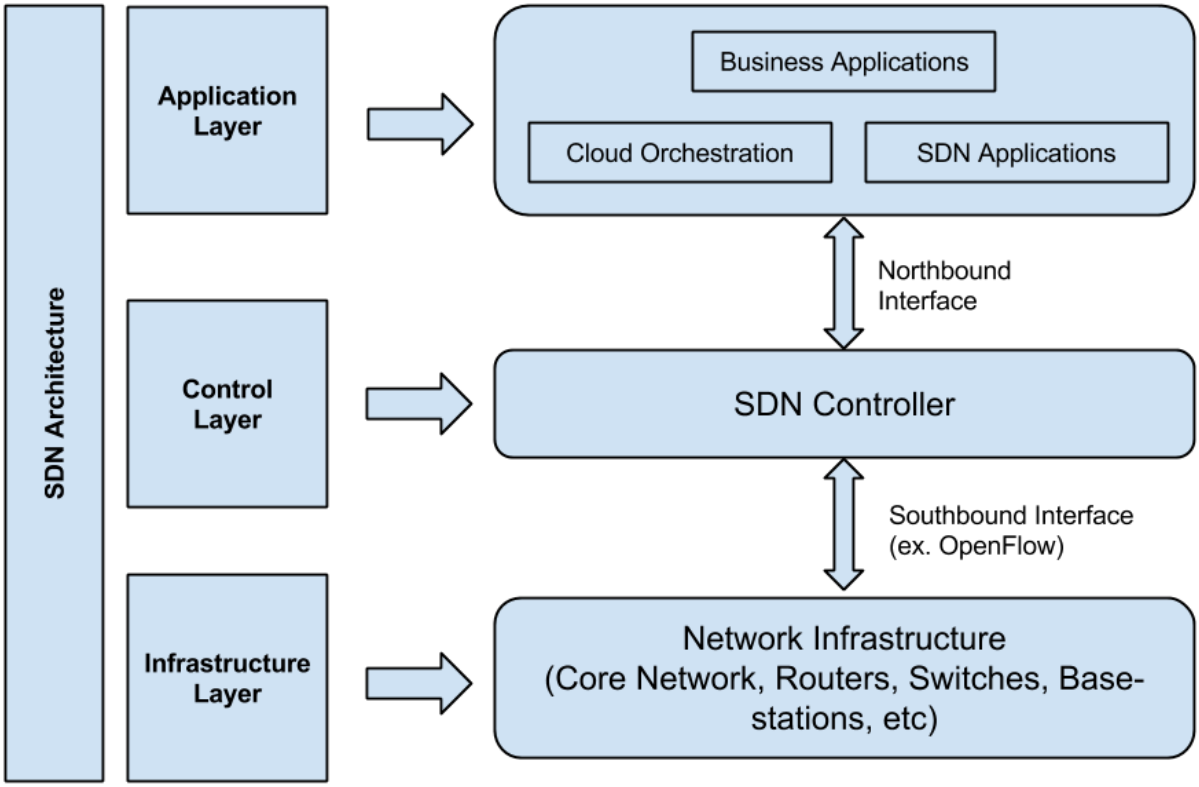
1.5.2 Δίκτυο πυρήνα κινητής τηλεφωνίας 5G.

Οι βασικές τεχνολογίες για το σχεδιασμό μέρους του πυρήνα των δικτύων 5G είναι το SDN ,το NFV και το cloud computing.

1.5.2.1 Software Defined Networking.

Το SDN θεωρείται η καλύτερη τεχνολογία για την ανάπτυξη των δικτύων 5G. Στο SDN έχουμε τον διαχωρισμό του επιπέδου προώθησης από το επίπεδο ελέγχου, πράγμα που κάνει πιο εύκολη τη διαχείριση του δικτύου. Έτσι χρησιμοποιείται στο 5G

για να είναι δυνατή μια πιο ευέλικτη αρχιτεκτονική δικτύου πυρήνων. Παρακάτω βλέπουμε την αρχιτεκτονική του SDN.

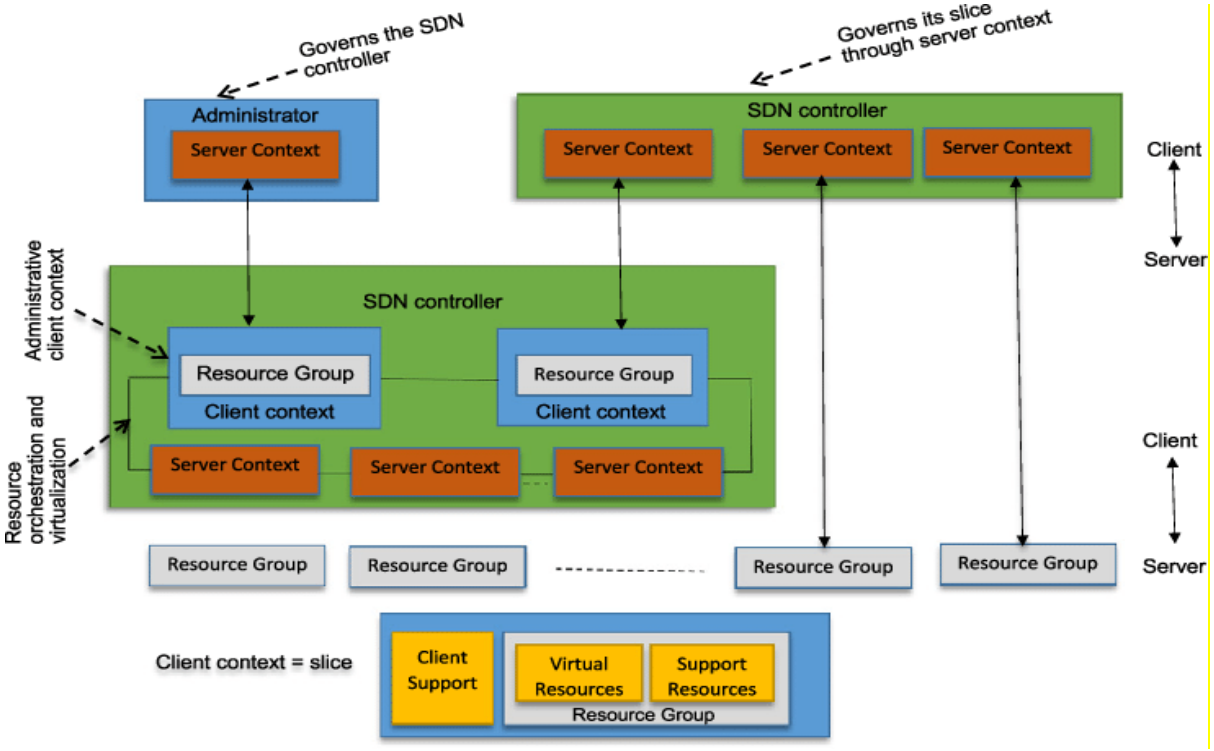


Εικόνα 11: Η αρχιτεκτονική του SDN. [9]

Το SDN είναι μια προσέγγιση που φέρνει ευφυΐα και ευέλικτα προγραμματιζόμενα δίκτυα 5G, ικανά να ενορχηστρώνουν και να ελέγχουν εφαρμογές/υπηρεσίες καθορίζοντας τις καλύτερα στο ευρύτερο δίκτυο. Το Open Network Foundation (ONF) ορίζει το SDN ως τον διαχωρισμό του επιπέδου ελέγχου δικτύου από το επίπεδο προώθησης όπου ένα επίπεδο ελέγχου ελέγχει πολλές συσκευές. Αυτός ο διαχωρισμός έχει ως αποτέλεσμα την ευελιξία και τον κεντρικό έλεγχο με συνολική άποψη ολόκληρου του δικτύου. Παρέχει επίσης δυνατότητα γρήγορης ανταπόκρισης σε γρήγορα μεταβαλλόμενες συνθήκες δικτύου, στις ανάγκες των επιχειρήσεων, της αγοράς και των τελικών χρηστών. Το SDN δημιουργεί ένα εικονικό επίπεδο ελέγχου που μπορεί να επιβάλει έξυπνες αποφάσεις διαχείρισης μεταξύ των λειτουργιών δικτύου, γεφυρώνοντας το χάσμα μεταξύ των υπηρεσιών παροχής και διαχείρισης δικτύου. Με το SDN, ο έλεγχος του δικτύου γίνεται άμεσα προγραμματιζόμενος χρησιμοποιώντας τυποποιημένες διεπαφές Southbound (SBI) όπως το OpFlex, το ForCES και το OpenFlow . Αυτά τα πρότυπα ορίζουν την επικοινωνία μεταξύ των

συσκευών προώθησης στο επίπεδο δεδομένων και των στοιχείων στο επίπεδο ελέγχου και διαχείρισης. Το επίπεδο προώθησης του SDN μπορεί να υλοποιηθεί σε έναν εξειδικευμένο εμπορικό διακομιστή όπως π.χ. η πλατφόρμα NSX της VMware που αποτελείται από έναν ελεγκτή και έναν εικονικό διακόπτη (vSwitch). Ωστόσο, τέτοιες υλοποιήσεις εξαρτώνται από την απόδοση, τις ανάγκες και απαιτήσεις χωρητικότητας των περιβαλλόντων SDN. Σε αυστηρά πλαίσια, ο ακαδημαϊκός κόσμος, η βιομηχανία και οι πρότυποι φορείς όπως το ONF, το Software Defined Networking Research Group (SDNRG) ,η Ομάδα Εργασίας Έρευνας Διαδικτύου (IRTF) και η Ειδική Ομάδα Μηχανικής Διαδικτύου (IETF) έχουν ήδη συνειδητοποιήσει τις δυνατότητες του SDN και όρισαν τα αρχιτεκτονικά στοιχεία, τις διεπαφές και τις λειτουργικές του απαιτήσεις, για τα μελλοντικά δίκτυα 5G . [9]

Το SDN έχει ρυθμιστεί να αντιμετωπίζει τους περιορισμούς των παραδοσιακών δικτύων που είναι ακατάλληλοι για τη δυναμική διαμόρφωση δικτύου, τον έλεγχο και τη διαχείριση, καθώς και τις ανάγκες αποθήκευσης για τα σημερινά κέντρα δεδομένων, τις πανεπιστημιουπόλεις και τα ετερογενή περιβάλλοντα. Το παράδειγμα SDN για 5G της ανάλυσης κοπής δικτύου (network slicing) έχει επεξεργαστεί εκτενώς από το ONF. Κάθε περιβάλλον πελάτη SDN στην αρχιτεκτονική ONF υποδεικνύει ένα δυναμικό slice όπως φαίνεται στην Εικόνα 12 . [5]

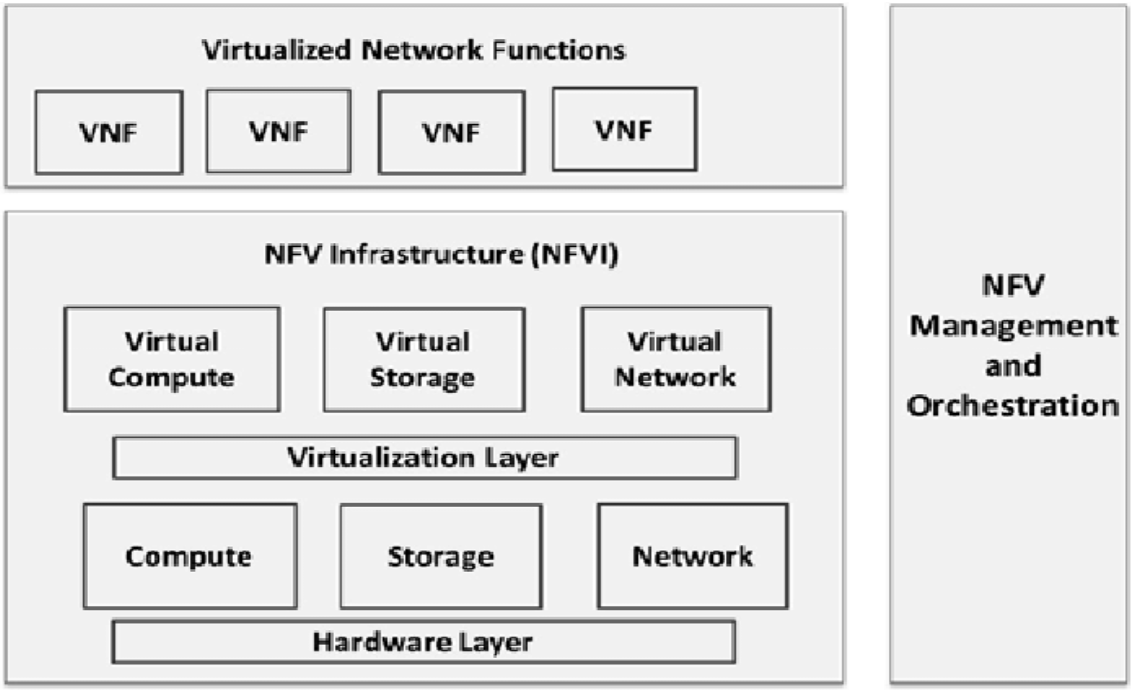


Εικόνα 12: ONF SDN network slicing architecture. [5]

Ο ελεγκτής SDN διαχειρίζεται τμήματα δικτύου χρησιμοποιώντας ένα σύνολο κανόνων ή πολιτικών. Ο ελεγκτής SDN διευκολύνει επίσης τη δημιουργία περιβάλλοντος διακομιστή και πελάτη, όπως και την εγκατάσταση των σχετικών πολιτικών τους. Συγκεκριμένα, ο ελεγκτής SDN διατηρεί ένα τμήμα δικτύου πλαισίου πελάτη. Έτσι, επιτρέπει σε έναν ελεγκτή SDN να διαχειρίζεται δυναμικά κομμάτια δικτύου, ομαδοποιώντας τα κομμάτια αυτά που ανήκουν στο ίδιο περιεχόμενο. Ο ελεγκτής SDN διαχειρίζεται τα κομμάτια του (slices) και εκτελεί ενορχήστρωση πόρων στο περιβάλλον του διακομιστή. Το πλαίσιο του πελάτη αποτελείται από υποστήριξη, πελάτη και εικονικούς πόρους για την ικανοποίηση τυχόν εισερχόμενων αιτημάτων από τελικούς χρήστες. Με το SDN μπορεί να βελτιωθεί η αποδοτικότητα αφού λόγω του διαχωρισμού των επίπεδων ελέγχου και δεδομένων, η δικτυακή υποδομή είναι δυνατόν να κατασκευαστεί κατόπιν ζήτησης και με βάση τις απαιτήσεις υπηρεσίας. Ωστόσο προβλήματα όπως, η καθυστέρηση μεταξύ των συσκευών και του ελεγκτή SDN, το πρόβλημα ασφάλειας του καναλιού επικοινωνίας μεταξύ των επιπέδων ελέγχου και δεδομένων και η έλλειψη τυποποίησης σχετικά με το σχεδιασμό του πρωτοκόλλου που επικοινωνεί μεταξύ των επιπέδων ελέγχου και δεδομένων, θα πρέπει να αντιμετωπιστούν. [5]

1.5.2.2 Network Function Virtualization (NFV).

Η αποδοτικότητα κόστους όπως έχουμε ήδη αναφέρει είναι ένας σημαντικός παράγοντας καθώς έχει να κάνει με τα έσοδα των παρόχων κινητής. Οι πάροχοι κινητής τηλεφωνίας 5G θα αναμένουν το κόστος για την ανάπτυξη, το οποίο αναφέρεται ως δαπάνη κεφαλαίου ή CAPEX, και το κόστος λειτουργίας και διαχείρισης, το οποίο αναφέρεται ως λειτουργικό κόστος ή OPEX, να είναι όσο το δυνατόν χαμηλότερο. Το NFV έρχεται να αντικαταστήσει λειτουργίες δικτύου που γίνονταν με μεγάλο κόστος. Είναι μια τεχνολογία που ουσιαστικά φέρνει τη μετεγκατάσταση των λειτουργιών δικτύου, σε πλατφόρμες με συσκευές λογισμικού που εκτελούνται σε περιβάλλον cloud ή σε γενικής χρήσης διακομιστές. Με τη λειτουργία του δικτύου ως λογισμικό, είναι ευκολότερη η εκμετάλλευση φορέων κινητής τηλεφωνίας, για δυναμική κλιμάκωση πόρων (υπολογιστές, αποθήκευση και δικτύωση) ανάλογα με τις αλλαγές στις απαιτήσεις κίνησης και με ταχύτερο χρόνο διάθεσης των νέων υπηρεσιών. Η παρακάτω εικόνα δείχνει το αρχιτεκτονικό πλαίσιο αναφοράς του NFV. [14]



Εικόνα 13: Αρχιτεκτονική NFV. [15]

1.5.2.3 Cloud Computing.

Το cloud computing αποτελεί σημαντικό παράγοντα για το σχεδιασμό του πυρήνα του 5G, λόγω του πλεονεκτήματος της ελαστικής παροχής υπηρεσιών και πόρων μέσω διαδικτύου. Έτσι οι πιο βασικές οι λειτουργίες του δικτύου 5G θα πραγματοποιούνται σαν εικονικές μηχανές που θα ελέγχονται από τον διαχειριστή του cloud. Με την παροχή πόρων σε μοντέλο πολυενοικιαστή στο cloud computing, επιτρέπετε στους φορείς εκμετάλλευσης και παρόχους κινητής τηλεφωνίας να εφαρμόσουν την έννοια των κινητών χειριστών εικονικών δικτύων-MVNO πολύ εύκολα. Επίσης με την χρήση του μοντέλο pay-as-you-use, στο cloud computing, οι εταιρείες κινητής μπορούν να μειώσουν τα κεφάλαια τους, αφού έχουν τη δυνατότητα μετακίνησης και ενοποίησης των πόρων. [4]

1.5.3 Σύστημα 5G End-to-End.

-Τεμαχισμός Δικτύου (Network Slicing)

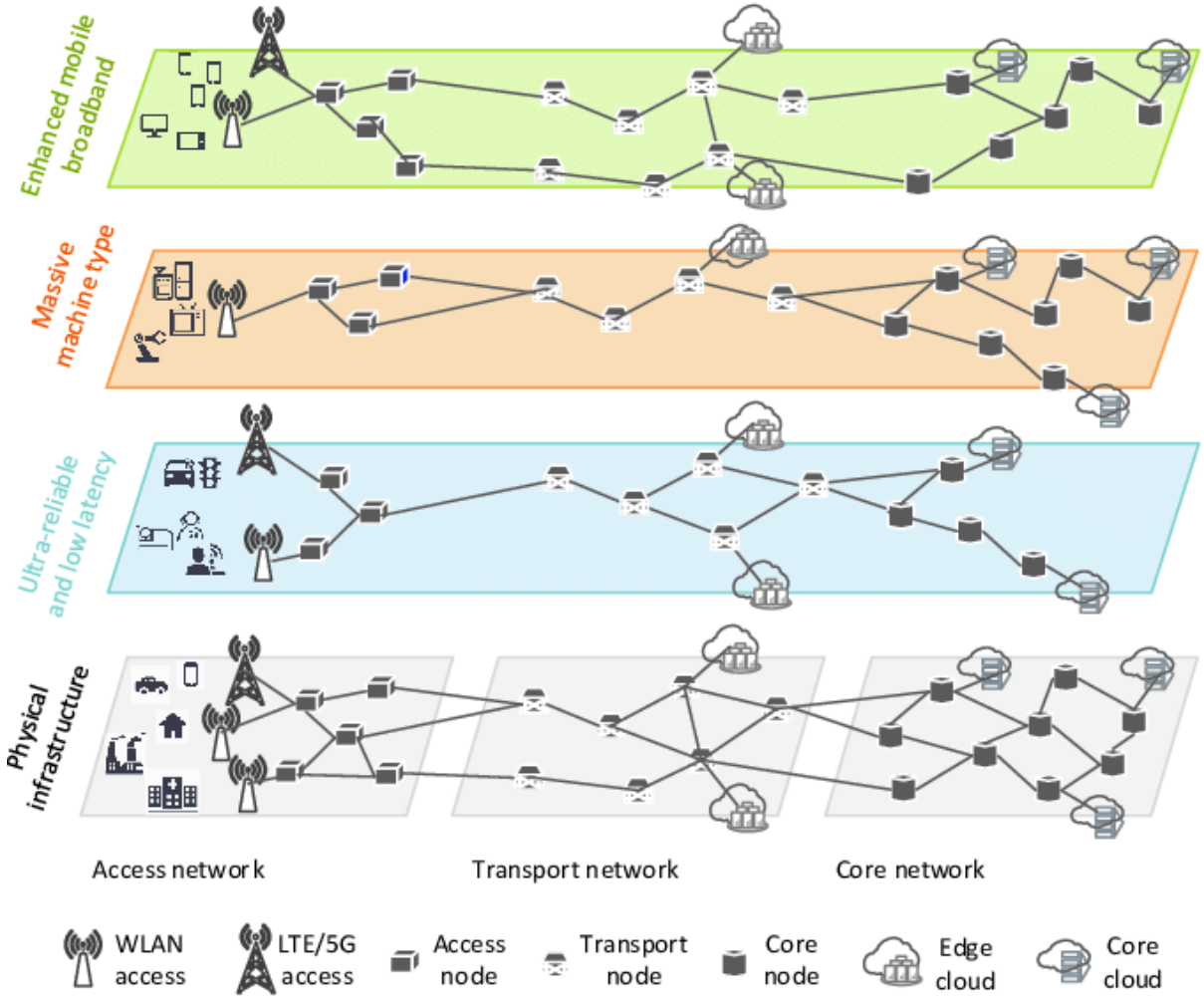
-Διαχείριση και ενορχήστρωση (MANO).

1.5.3.1 Network Slicing.

Για την ικανοποίηση των απαιτήσεων που θα προκύψουν στα συστήματα 5G λόγω της υποστήριξης συσκευών και υπηρεσιών με διαφορετικά χαρακτηριστικά και δυνατότητες δικτύου, κάθε τύπος υπηρεσίας θα πρέπει να πρέπει να παρέχεται ως από άκρο σε άκρο, ως απομονωμένη αλλά και ως λειτουργία περιβάλλοντος υποδομής. Η τεχνολογία Network Slicing αποτελεί ίσως το βασικό συστατικό για την πλήρη αξιοποίηση των δυνατοτήτων της αρχιτεκτονικής 5G δικτύου. Αυτή η τεχνολογία προσθέτει μια επιπλέον διάσταση στον τομέα NFV και επιτρέπει σε πολλαπλά λογικά δίκτυα να λειτουργούν ταυτόχρονα πάνω από μια κοινή φυσική υποδομή δικτύου. Αυτό γίνεται αναπόσπαστο κομμάτι της αρχιτεκτονικής 5G δημιουργώντας εικονικά δίκτυα από άκρο σε άκρο που περιλαμβάνουν λειτουργίες δικτύωσης και αποθήκευσης. Οι φορείς εκμετάλλευσης μπορούν να διαχειρίζονται αποτελεσματικά διάφορες περιπτώσεις χρήσης 5G, με διαφορετικές απαιτήσεις απόδοσης, καθυστέρησης και διαθεσιμότητας, μοιράζοντας τους πόρους του δικτύου σε πολλούς χρήστες. Το network slicing είναι εξαιρετικά χρήσιμο για εφαρμογές όπως

το IoT, όπου ο αριθμός των χρηστών μπορεί να είναι τεράστιος, αλλά η συνολική ζήτηση εύρους ζώνης είναι χαμηλή. Κάθε κλάδος 5G θα έχει τις δικές του απαιτήσεις, οπότε ο διαχωρισμός του δικτύου είναι σημαντικός παράγοντας σχεδιασμού για την αρχιτεκτονική του δικτύου 5G. Το κόστος, η διαχείριση των πόρων και η ευελιξία των διαμορφώσεων δικτύου μπορούν όλα να βελτιστοποιηθούν πλέον με αυτό το επίπεδο προσαρμογής. Επίσης το network slicing επιτρέπει γρήγορες δοκιμές για πιθανές νέες υπηρεσίες 5G και ταχύτερο χρόνο διάθεσης στην αγορά. [14]

Η εικόνα 14 απεικονίζει ένα παράδειγμα της έννοιας του network slicing, με τέσσερα διαφορετικά κομμάτια που αντιστοιχούν σε τέσσερις κατηγορίες περιπτώσεων χρήσης 5G.

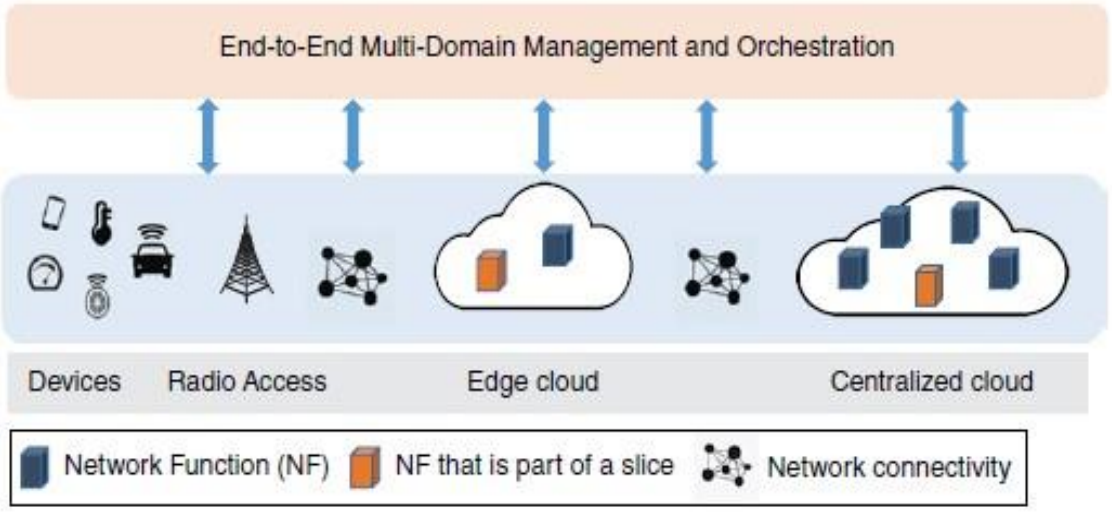


Εικόνα 14: Ένα παράδειγμα του Network Slicing. [16]

Για το σκοπό αυτό, η εφαρμογή της έννοιας του network slicing είναι από άκρο σε άκρο.

1.5.3.2 Διαχείριση και Ενορχήστρωση (MANO).

Η Διαχείριση και Ενορχήστρωση-MANO, είναι πολύ σημαντική λόγω της διαφορετικών περιπτώσεων χρήσης του 5G, των υπηρεσιών αλλά και του αριθμού των τμημάτων δικτύου που δημιουργήθηκαν με διαφορετικές απαιτήσεις πόρων. Η διαχείριση της δικτυακής υποδομής που αφορά τη διαχείριση σφαλμάτων, τη διαμόρφωση, την απόδοση και την ασφάλεια αποτελούν το ρόλο της Διαχείρισης και Ενορχήστρωσης . Το πιο σημαντικό είναι, ότι η MANO θα είναι υπεύθυνη για τη διαχείριση του κύκλου ζωής και τη παροχή των πόρων δικτύου για τη συνδεσιμότητα από άκρο σε άκρο τμημάτων δικτύου με έναν δυναμικό, αυτοματοποιημένο και αποτελεσματικό τρόπο. Όπως φαίνεται στην εικόνα, ο ρόλος της διαχείριση και η ενορχήστρωσης από άκρο σε άκρο είναι πολλαπλών τομέων, πολλαπλών χειριστών και πολλαπλών τεχνολογιών και εκτείνεται από το επίπεδο υποδομής έως το επίπεδο της εφαρμογής (υπηρεσία) και από το RAN έως τον πυρήνα του δικτύου. [4]



Εικόνα 15: Παρουσίαση του end-to-end multi domain management and orchestration. [4]

ΚΕΦΑΛΑΙΟ 2ο

2.1 Ασφάλεια στα ασύρματα δίκτυα από το 1G στο 5G

Η ασφάλεια των δικτύων επικοινωνίας ήταν δύσκολο έργο λόγω της πολυπλοκότητας στο υποκείμενο δίκτυο, των ιδιόκτητων και περιμετρικών λύσεων ασφαλείας που είναι δύσκολες στη διαχείριση και αδύναμες στη διαχείριση της ταυτότητας. Από την αρχή των δικτύων κινητής, η ασφάλεια του ασύρματου δικτύου έχει εξελιχθεί σταδιακά. Η αλλαγή σε επικοινωνία με IP στα ασύρματα δίκτυα ήταν αυτή που έφερε τις προκλήσεις ασφάλειας του διαδικτύου στα ασύρματα δίκτυα. Παρακάτω θα κάνουμε μια επισκόπηση των αλλαγών που προκύπτουν σε θέματα ασφάλειας στα ασύρματα δίκτυα από 1G έως 5G ή καλύτερα από ασύρματα δίκτυα χωρίς IP σε ασύρματα που βασίζονται σε IP. [13]

2.1.1 Ασφάλεια στο 1G.

Τα κυψελωτά συστήματα 1G χρησιμοποιούσαν αναλογική επεξεργασία σήματος και σχεδιάστηκαν κυρίως για φωνητικές υπηρεσίες. Το πιο επιτυχημένο σύστημα 1G ονομάζεται Advanced Mobile Phone Service και αναπτύχθηκε για πρώτη φορά εμπορικά από τα εργαστήρια AT&T και Bell κατά το 1983 . Οι υπηρεσίες ασφαλείας στο 1G δεν ήταν δυνατόν να παρασχεθούν λόγω της ευάλωτης φύσης του αναλογικού σήματος. Στο 1G δεν υπήρχε καμία εμπιστευτικότητα καθώς μπορούσε ο οποιοσδήποτε να υποκλέψει μια ιδιωτική επικοινωνία δύο χρηστών. Για να το κάνει αυτό το μόνο που χρειαζόταν ήταν έναν δέκτης που να λειτουργούσε σε παρόμοιες συχνότητες. Ακόμα ήταν δυνατόν να γίνει αντιγραφεί της ταυτότητα του κινητού τηλεφώνου και έτσι όλες οι χρεώσεις κλήσεων από το τηλέφωνο κλώνο θα μπορούσαν να πάνε στον κάτοχο του κανονικού τηλεφώνου. Λόγω του μεγέθους του δικτύου το οποίο ήταν μικρό στα δίκτυα πρώτης γενιάς, δεν υπήρχε ο κίνδυνος μαζικής κλωνοποίησης των κινητών συσκευών. Παρόλο που οι πληροφορίες σχετικά με τον αριθμό που καλείται θα μπορούσαν να είναι κρυπτογραφημένες, το κύριο πρόβλημα ήταν η μετάδοση μέσω του αέρα, καθώς τα σήματα μπορούσαν να ληφθούν εύκολα χρησιμοποιώντας οποιονδήποτε δέκτη FM, αφού η μετάδοση χρησιμοποιούσε διαμόρφωση συχνότητας. [13]

2.1.2 Ασφάλεια στο 2G.

Η βελτίωση των ικανοτήτων επεξεργασίας στις πλατφόρμες υλικού έκανε δυνατή την ανάπτυξη των ασύρματων συστημάτων 2G. Στο 2G έγινε η μετάβαση στα ψηφιακά σχήματα διαμόρφωσης οπότε και η συνολική απόδοση του συστήματος βελτιώθηκε όπως και η συνολική χωρητικότητα με τη χρήση ψηφιακών κωδικοποιητών ομιλίας, την εφαρμογή διαίρεσης χρόνου αλλά και της τεχνικής πολυπλεξίας διαίρεσης κώδικα. Στα 2G δίκτυα το Global System for Mobile (GSM) ήταν το πιο χρησιμοποιούμενο πρότυπο στις κυψελωτές επικοινωνίες. Η ανωνυμία, ο έλεγχος ταυτότητας, η προστασία σηματοδότησης και η προστασία δεδομένων χρήστη προσδιορίστηκαν ως οι σημαντικότερες πτυχές ασφαλείας. Η ανωνυμία παρέχεται με τη χρήση προσωρινών αναγνωριστικών ώστε να μην είναι εύκολος ο εντοπισμός του χρήστη ενός συστήματος. Κατά το άνοιγμα της συσκευής χρησιμοποιούνται τα πραγματικά αναγνωριστικά ενώ μετά εκδίδεται ένα προσωρινό αναγνωριστικό. Μέσω της εκτέλεσης μηχανισμού πρόκλησης απόκρισης γίνεται η αυθεντικοποίηση για την αναγνώριση του χρήστη από το χειριστή του δικτύου Η σηματοδότηση και η προστασία δεδομένων χρήστη πραγματοποιούταν μέσω κρυπτογράφησης στην οποία η Subscriber Identity Module (SIM) έπαιζε σημαντικό ρόλο στα κλειδιά κρυπτογράφησης. Ωστόσο, το 2G είχε αρκετούς περιορισμούς και αδυναμίες ασφάλειας. Οι χειριστές επαλήθευαν την ταυτότητα των UE μόνο σε μονομερή μηχανισμό, ενώ οι UE δεν είχαν επιλογή να πιστοποιήσουν την ταυτότητα του χειριστή. Έτσι ήταν δυνατή η εκτέλεση μιας επίθεσης man in the middle μέσω της δυνατότητας που δίνονταν σε ένα ψεύτικο χειριστή να μιμηθεί τον αρχικό. Επιπλέον, αρκετές επιθέσεις δέχονταν και οι αλγόριθμοι κρυπτογράφησης λόγω του ότι ήταν αντίστροφης μηχανική. Το GSM δεν παρείχε ακεραιότητα δεδομένων κατά της πειρατείας καναλιών, απουσία κρυπτογράφησης και ήταν επίσης ευάλωτο σε επιθέσεις DoS. Ενώ να αναφέρουμε επίσης ότι τα συστήματα 2G δεν είχαν τη δυνατότητα να αναβαθμίσουν τη λειτουργικότητα ασφαλείας τους με την πάροδο του χρόνου . Επίσης στο 2G ήρθαν και νέες εφαρμογές όπως η υπηρεσία σύντομων μηνυμάτων τα γνωστά σε όλους SMS. Επίσης τα συστήματα 2G κατάφεραν να υποστηρίξουν υπηρεσίες πακέτων δεδομένων, ενώ και το πρωτόκολλο ασύρματης πρόσβασης, το WAP μπήκε στα δίκτυα 2G για να παρέχει περιεχόμενο διαδικτύου στις φορητές συσκευές. [13]

2.1.3 Ασφάλεια στο 3G.

Τα κυψελωτά δίκτυα 3G αναπτύχθηκαν κυρίως για να παρέχουν υψηλότερους ρυθμούς δεδομένων από τα δίκτυα 2G και εισήγαγαν υπηρεσίες όπως οι εφαρμογές βίντεο, ήχου και γραφικών. Σε αυτά πρωτοείδαμε και την τηλεφωνία μέσω βίντεο αλλά και τη ροή βίντεο μέσω επικοινωνίας δικτύων κινητής τηλεφωνίας. Στο πρότυπο 3G προτάθηκε μια αρχιτεκτονική ασφαλείας αναβαθμισμένη, ώστε να αντιμετωπιστούν τα κενά ασφαλείας που προέκυψαν στα 2G δίκτυα. Το 3G παρείχε ένα ενιαίο συμβατό πρότυπο για δίκτυα κινητής τηλεφωνίας το οποίο θα μπορούσε να χρησιμοποιηθεί παγκόσμιος για όλες τις εφαρμογές σε κινητά. Η υποστήριξη που παρείχε ήταν για μεταγωγή πακέτων αλλά και για επικοινωνία δεδομένων με μεταγωγή κυκλώματος. Το Universal Mobile Telecommunications System είναι μια τεχνολογία κινητής τηλεφωνίας 3G .Η αρχιτεκτονική ασφαλείας του, αποτελείται από πέντε σετ χαρακτηριστικών ασφαλείας . Ο έλεγχος ταυτότητας του UMTS και το πρωτόκολλο συμφωνίας κλειδιού Authentication Key Agreement έχει σχεδιαστεί με τέτοιο τρόπο ώστε να επιτυγχάνεται μέγιστη συμβατότητα με το GSM. Ο αμοιβαίος έλεγχος ταυτότητας δικτύου, η συμφωνία για το κλειδί ακεραιότητας κ.α, αποτελούν στόχους που εξυπηρετεί το UMTS AKA. Για την αποφυγή της απειλής ψεύτικου σταθμού βάσης το UMTS υποστηρίζει διμερή έλεγχο ταυτότητας. Η δυνατότητα ασφάλειας πρόσβασης περιλαμβάνει το απόρρητο της ταυτότητας χρήστη που διασφαλίζει ότι ένας χρήστης δεν μπορεί να υποκλαπεί σε σύνδεση ραδιοφωνικής πρόσβασης. Το απόρρητο της ταυτότητας του χρήστη πρέπει να υποστηρίζει το απόρρητο τοποθεσίας χρήστη αλλά και τη μη ιχνηλάτηση της τοποθεσίας του χρήστη. Για όλα τα παραπάνω ,ο χρήστης αναγνωρίζεται από μια προσωρινή ταυτότητα ή μια μόνιμη κρυπτογραφημένη ταυτότητα. Επιπλέον, δεν πρέπει να γίνεται ταυτοποίηση του χρήστη για μεγάλο χρονικό διάστημα ενώ δεδομένα που μπορεί να αποκαλύψουν την ταυτότητα του, θα πρέπει να κρυπτογραφούνται. [13]

2.1.4 Ασφάλεια στο 4G.

Το LTE-Advanced (LTE-A), καθορίστηκε από το 3GPP και ικανοποιεί τις απαιτήσεις του πρότυπου για το 4G όπως αυτές είχαν καθοριστεί από τη Διεθνή Ένωση

Τηλεπικοινωνιών-Τομέας Ραδιοεπικοινωνιών. Το 3GPP όρισε χαρακτηριστικών ασφαλείας για το LTE-A. Αυτά είναι: (i) η ασφάλεια πρόσβασης, (Evolved Universal Terrestrial Radio Access Network ii) η ασφάλεια δικτύου τομέα, (iii) η ασφάλεια τομέα χρήστη, (iv) η ασφάλεια εφαρμογής τομέα και (v) η ορατότητα και δυνατότητα διαμόρφωσης της ασφάλειας. Ωστόσο, κάθε ένα από τα χαρακτηριστικά έχει βελτιωθεί σημαντικά για την ασφάλεια των συστημάτων LTE-A. Επιπλέον, καθορίστηκαν εντελώς νέοι μηχανισμοί ασφαλείας για το MTC, το home eNB και τους κόμβους αναμετάδοσης.

Το Evolved Packet System-AKA (EPS-AKA) είχε μια σημαντική βελτίωση σε σχέση με το UMTS-AKA, τον διαχωρισμό κρυπτογραφικού δικτύου. Με αυτή τη βελτίωση καταφέρνει και περιορίζει εκτός από την παραβίαση ασφάλειας σε ένα δίκτυο και την πιθανότητα εξάπλωσης της επιθέσεις σε όλο το δίκτυο. Αυτό επιτυγχάνεται με τη δέσμευση οποιουδήποτε κρυπτογραφικού κλειδιού που σχετίζεται με το EPS για την ταυτότητα της Υπηρεσίας Δικτύου (SN). Ο χρήστης και το απόρρητο των δεδομένων σηματοδότησης έχουν υποστεί επίσης αλλαγές για το EPS. Το τελικό σημείο της κρυπτογράφησης της πλευράς του δικτύου βρίσκεται στο σταθμό βάσης ενώ στο 3G βρισκόταν στον ελεγκτή ραδιοφωνικού δικτύου. Υπάρχει επίσης πρόσθετος μηχανισμός προστασίας του απορρήτου για σηματοδότηση μεταξύ του UE και του βασικού δικτύου. Υπάρχουν δύο τύποι δικτύων πρόσβασης χωρίς 3GPP,αυτά με αξιόπιστη πρόσβαση χωρίς 3GPP και αυτά μη αξιόπιστη πρόσβαση χωρίς 3GPP. Για ένα μη αξιόπιστο μη 3GPP δίκτυο πρόσβασης. Επιπλέον, για τη διασφάλιση της ασφαλούς διαδικασίας κινητικότητας στο LTE, έχει εισαχθεί μια νέα ιεραρχία κλειδιών και ένας μηχανισμός διαχείρισης κλειδιών παράδοσης. Η αδυναμία ασφάλειας του σημείου πρόωρου τερματισμού σε συνδυασμό με την αρχιτεκτονική του EPS που επιτρέπει την τοποθέτηση του eNB εκτός δικτύου ασφαλείας το καθιστούν πιο ευάλωτο σε φυσικές επιθέσεις, DoS επιθέσεις ή παθητικές επιθέσεις με την υποκλοπή μακροπρόθεσμων κλειδιών. Το 3GPP για την αντιμετώπιση όλων των τρωτών σημείων εισήγαγε αυστηρές απαιτήσεις για το eNB. [13]

Πίνακας 1: Η εξέλιξη της ασφάλειας από το 1G στο 4G. [13]

Δίκτυο	Μηχανισμός Ασφαλείας	Πρόκληση Ασφαλείας
1G	Χωρίς ουσιαστική ασφάλεια και μέτρα προστασίας της ιδιοτικότητας.	Υποκλοπή, παρακολούθηση κλήσεων, και χωρίς μηχανισμούς ασφαλείας απορρήτου.
2G	Αυθεντικοποίηση, ανωνυμία και προστασία με βάση την κρυπτογράφηση	Ψεύτικος σταθμός βάσης, ασφάλεια σύνδεσης ραδιοφώνου, μονόπλευρος έλεγχος ταυτότητας, και spamming.
3G	Υιοθέτηση της ασφάλειας του 2G. Ασφαλής πρόσβαση στο δίκτυο. Εισαγωγή του ελέγχου ταυτότητας, συμφωνίας κλειδιού (AKA) και αμφίδρομης αυθεντικοποίησης.	τρωτά σημεία ασφάλειας της κυκλοφορίας IP, ασφάλεια κλειδιών κρυπτογράφησης, ασφάλεια περιαγωγής.
4G	Παρουσίαση νέας κρυπτογράφησης (EPS-AKA) και μηχανισμών εμπιστοσύνης. Ασφάλεια κλειδιών κρυπτογράφησης. Εκτός 3GPP ασφάλεια πρόσβασης. Προστασία ακεραιότητας.	Αυξημένη κίνηση IP που προκαλεί θέματα ασφαλείας, π.χ. Επιθέσεις DoS, ακεραιότητα δεδομένων. Ασφάλεια Πομποδέκτη Σταθμού Βάσης. και υποκλοπή μακροπρόθεσμων κλειδιών. Ακατάλληλο για ασφάλεια νέων υπηρεσιών και συσκευών όπως το τεράστιο IoT που προβλέπεται στο 5G.

2.1.5 Ασφάλεια στο 5G

Το 5G θα παρέχει ευρυζωνικές υπηρεσίες πραγματικού χρόνου, θα επιτρέψει τη συνδεσιμότητα τεράστιου αριθμού συσκευών με τη μορφή IoT και θα ψυχαγωγεί τους χρήστες συσκευών, με υψηλή κινητικότητα με εξαιρετικά αξιόπιστο και προσιτό τρόπο. Το 5G θεωρείται νέο οικοσύστημα που συνδέει σχεδόν όλες τις πτυχές της κοινωνίας. Αυτό όπως γίνεται αντιληπτό, θα φέρει μια νέα σειρά απειλών και τρωτών σημείων ασφαλείας που θα πρέπει να αντιμετωπιστούν και θα αποτελέσουν σημαντική πρόκληση για τα σημερινά και τα μελλοντικά δίκτυα. Συνδέοντας για παράδειγμα το ηλεκτρικό δίκτυο, το 5G θα συνδέσει κρίσιμες υποδομές ισχύος στο δίκτυο, επομένως

η ασφάλεια και οι παραβιάσεις σε τέτοιες υποδομές είναι ζωτικής σημασίας και μπορεί να είναι καταστροφικές τόσο για τις υποδομές όσο και στην κοινωνία που το 5G εξυπηρετεί. Επομένως, η ασφάλεια του 5G και των συστημάτων που είναι συνδεδεμένα μέσω αυτού θα πρέπει να ληφθούν υπόψη ήδη από τις φάσεις σχεδιασμού. Το 5G όπως αναφέραμε θα φέρει τεράστια οφέλη απόδοσης και ποικιλία εφαρμογών μέσω της εκτεταμένης χρήσης πόρων που βασίζονται στο cloud, της εικονικοποίησης, του διαχωρισμού δικτύου και άλλων αναδυόμενων τεχνολογιών που χρησιμοποιεί. Με αυτές τις αλλαγές έρχονται όμως και νέοι κίνδυνοι ασφάλειας και πολλές νέες επιφάνειες επίθεσης που εκτίθενται στην αρχιτεκτονική ασφάλειας του. Το 5G βασίζεται στις πρακτικές ασφαλείας των προγενέστερων τεχνολογιών κινητής τηλεφωνίας, ωστόσο το μοντέλο εμπιστοσύνης έχει γίνει πολύ πιο επεκτατικό με περισσότερους παίκτες να συμμετέχουν στη διαδικασία παροχής υπηρεσιών. Το IoT και ο αριθμός των χρηστών δημιουργούν έναν εκθετικά μεγαλύτερο αριθμό τελικών σημείων με πολλές από αυτές τις εισόδους κυκλοφορίας να μην εποπτεύονται πλέον από τον άνθρωπο. Μεταξύ των βελτιωμένων χαρακτηριστικών ασφαλείας 5G που περιγράφονται λεπτομερώς από τα πρότυπα του 3GPP είναι, ο ενοποιημένος έλεγχος ταυτότητας για την αποσύνδεση του ελέγχου ταυτότητας από τα σημεία πρόσβασης, τα επεκτάσιμα πρωτόκολλα ελέγχου ταυτότητας για την υποδοχή ασφαλών συναλλαγών, οι ευέλικτες πολιτικές ασφαλείας για την αντιμετώπιση περισσότερων περιπτώσεων χρήσης και τα μόνιμα αναγνωριστικά συνδρομητών (SUPI) για τη διασφάλιση του απορρήτου στο δίκτυο .

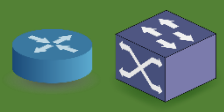
Καθώς η ανάπτυξη του 5G συνεχίζεται και οι κρίσιμοι κόμβοι απόδοσης γίνονται όλο και περισσότερο εικονικοποιημένοι, οι χειριστές θα πρέπει να παρακολουθούν και να αξιολογούν συνεχώς την απόδοση ασφάλειας. Η συμμόρφωση με τις βέλτιστες πρακτικές σημαίνει παρακολούθηση της ασφάλειας του δικτύου από άκρο σε άκρο σε όλη την αρχιτεκτονική του συστήματος, τις συσκευές και τις εφαρμογές. Αναμφίβολα, το 5G θα προσφέρει την εκθετική βελτίωση της ταχύτητας που έχουν συνηθίσει οι χρήστες με κάθε νέα γενιά δικτύων κινητής τηλεφωνίας, αλλά η ταχύτητα είναι μόνο το ένα κομμάτι. Οι αναμενόμενες αλλαγές σε κλάδους , από τις προσωπικές μεταφορές μέχρι την κατασκευή και τη γεωργία θα είναι τόσο σημαντικές που πολλοί έχουν ονομάσει το 5G ως την επόμενη βιομηχανική επανάσταση. Στο επίκεντρο αυτής της αλλαγής βρίσκεται η πολύπλευρη αρχιτεκτονική του, με το MEC, το massive MIMO το

NFV και μια βασική αρχιτεκτονική βασισμένη σε υπηρεσίες ευθυγραμμισμένη με το cloud, που συνεργάζονται για να προσφέρουν ένα νέο κύμα υπηρεσιών. [13]

2.2 Αρχές σχεδίασης για την ασφάλεια του 5G

Η ανάγκη για καινούριες αρχές σχεδίασης στο 5G παρουσιάστηκε, λόγω των νέων υπηρεσιών και συσκευών που εμφανίστηκαν και ως εκ τούτου, των απαιτήσεων που προκύπτουν από αυτές και έχουν να κάνουν με την χαμηλή καθυστέρηση και την κάλυψη υπηρεσιών σε πραγματικό χρόνο. Οι αρχές σχεδιασμού 5G που περιγράφονται από το NGMN και παρουσιάζονται στο παρακάτω πίνακα, τονίζουν την ανάγκη για υψηλή ελαστικότητα και στιβαρά συστήματα. Για το radio είναι απαραίτητη μια οικονομικά αποδοτική και πυκνή ανάπτυξη, η ακύρωση των παρεμβολών και η χρήση δυναμικών ραδιοτοπολογιών. Οι απαιτήσεις που προκύπτουν για το δίκτυο είναι διαφορετικές και αφορούν κυρίως της νέες τεχνολογίες και την ενσωμάτωσή τους. Η ενεργοποίηση της δυναμικής τοποθέτησης των λειτουργιών του δικτύου θα γίνει με την χρήση των τεχνολογιών του SDN και του NFV. Αυτό αποτελεί στόχο για την ελαχιστοποίηση των δικτύων παλαιού τύπου και την εισαγωγή νέων διεπαφών μεταξύ του πυρήνα και των τεχνολογιών ραδιοπρόσβασης (RATs). Επίσης η ανάπτυξη μηχανισμών και λειτουργιών ασφαλείας θα πρέπει να υποστηρίζονται από την αρχιτεκτονική του δικτύου όποτε αυτή απαιτείται. Η ανάγκη για απλοποίηση της λειτουργίας και της διαχείρισης θα γίνεται μέσω του SDN και της δυνατότητας που αυτό δίνει για διαχωρισμό του επιπέδου ελέγχου από το επίπεδο προώθησης δεδομένων. Με την χρήση διασυνδεμένων εφαρμογών το επίπεδο ελέγχου επιβλέπει ολόκληρο το δίκτυο κάνοντας παράλληλα και τον έλεγχο των πόρων του δικτύου. Η χρήση όμως αυτών των διασυνδεμένων εφαρμογών στο δίκτυο αλλά και ο συγκεντρωτικός έλεγχος του, δημιουργούν κάποια σημαντικά θέματα ασφαλείας. Θέματα ασφαλείας εκτός από το SDN προκύπτουν και από τις άλλες τεχνολογίες που θα χρησιμοποιηθούν στο 5G , όπως το NFV και ο τεμαχισμός του δικτύου, πράγμα που είναι πολύ σημαντικό και θα πρέπει να ληφθεί υπόψιν και στις αρχές σχεδίασης των συστημάτων. [4]

Πίνακας 2: Αρχές σχεδίασης [4]

 Radio	 Δίκτυο	 Λειτουργία & Διαχείρηση
-Αποδοτικότητα φάσματος -Οικονομική πυκνή ανάπτυξη -Συντονισμός & ακύρωση παρεμβολών -Υποστήριξη δυναμικής ραδιοτοπολογίας	-Δημιουργία κοινού συνθετικού πυρήνα -Ελαχιστοποίηση οντοτήτων και λειτουργιών -C/U- διαχωρισμός λειτουργίας -RAT -αγνωστικός πυρήνας -Ελαχιστοποίηση δικτύωσης παλαιού τύπου	-Απλοποίηση των λειτουργιών και της διαχείρισης: -Αυτοματισμός και αυτοθεραπεία -Ανίχνευση παρακολούθησης -Συνεργατική διαχείριση -Ενσωματωμένη λειτουργικότητα OAM -Ενορχήστρωση cloud δικτύου

Ευέλικτες λειτουργίες και δυνατότητες	Υποστήριξη δημιουργίας νέας σταθεράς
• Τεμαχισμός δικτύου • Διακύμανση συνάρτησης • Ευέλικτη κατανομή λειτουργίας/υπηρεσιών/εφαρμογών • Συνδυασμός NFV/SDN • Ανεξάρτητες λειτουργίες • Ομαλή υποβάθμιση	• Εκμετάλλευση των μεγάλων δεδομένων και της επίγνωση του περιβάλλοντος • Έκθεση των API ραδιοφώνου και δικτύου • Διευκόλυνση του XaaS • Ενισχύστε την ασφάλεια και την ιδιωτικότητα • Επέκταση της ασφάλειας του C-plane (π.χ. HetNets) • Διασφαλίστε το απόρρητο της τοποθεσίας και της προστασία της ταυτότητας από (παράνομη) αποκάλυψη

2.3 Η ασφάλεια στις βασικές τεχνολογίες του 5G.

Οι προκλήσεις ασφαλείας στο 5G είναι δυνατόν να περιγράφουν κατάλληλα εξετάζοντας τις κύριες τεχνολογίες ενεργοποίησης του 5G, οι κεραίες MIMO, το SDN, το NFV και οι έννοιες του cloud computing όπως το Multi-access Edge Computing (MEC).

2.3.1 Ασφάλεια στο Massive MIMO.

Αρχικά θα αναφερθούμε στις προκλήσεις ασφαλείας στο massive MIMO. Το massive MIMO είναι μια από τις σημαντικότερες τεχνολογίες για το 5G. Σε αυτό ο σταθμός βάσης αποτελείται από μεγάλο αριθμό κεραιών έτσι ώστε να υποστηρίζεται μεγάλος αριθμός τελικών χρηστών με την ίδια ζώνη συχνοτήτων. Με τον μεγάλο αριθμό κεραιών επιτυγχάνονται πολλά πλεονεκτήματα όπως η αύξηση της κάλυψης και της ενεργειακής απόδοσης αλλά και η χρήση τους για διάφορες άλλες λειτουργίες. Τα τρωτά σημεία ασφαλείας στο massive MIMO είναι η παθητική υποκλοπή και η ενεργητική υποκλοπή. Ο εισβολέας κατά την παθητική υποκλοπή έχει ως σκοπό να διακόψει τα μεταδιδόμενα σήματα. Ο παθητικός εισβολέας δεν μεταδίδει οποιοδήποτε σήμα από μόνος του. Στην ενεργητική υποκλοπή, ο εισβολέας μεταδίδει σήματα για να διαταράξει τη λειτουργία της μετάδοσης του νόμιμου χρήστη. Εάν ο μόνος στόχος της ενεργητικής επίθεσης είναι να διαταραχθεί η νόμιμη μετάδοση, μπορεί να ονομαστεί jamming επίθεση. Μια ακόμα ενεργητική επίθεση είναι το pilot spoofing , στην οποία ο εισβολέας προσποιείται τον νόμιμο χρήστη. Το Channel State Information χρησιμοποιείται στο σταθμό βάσης για προκωδικοποίηση της μετάδοσης και λαμβάνεται μέσω της διαδικασίας εκτίμησης καναλιού με βάση τα πιλοτικά σήματα που αποστέλλονται από τους νόμιμους χρήστες. Σε μια επίθεση σε αυτό, ο εισβολέας προσπαθεί να δημιουργήσει σύγχυση στο σταθμό βάσης στέλνοντας το ίδιο σήμα πιλότο. Οπότε ο σταθμός βάσης μπερδεύεται και σχεδιάζει εσφαλμένα την προκωδικοποίηση της μετάδοσης, ο εισβολέας ωφελείται και το κανάλι μεταξύ σταθμού βάσης και νόμιμου χρήστη καθίσταται ανακριβής.

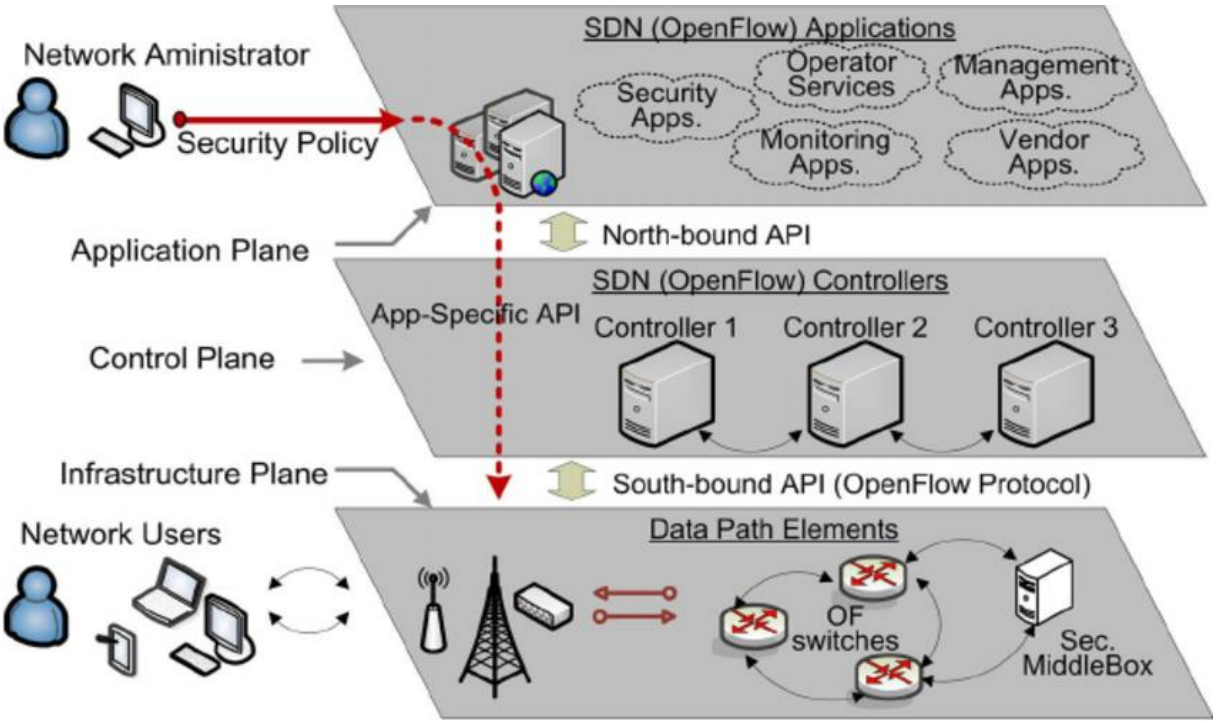
Για ένα δέκτη massive MIMO, οι επιθέσεις παρεμβολής είναι δυσκολότερο να αντιμετωπιστούν σε σχέση τις επιθέσεις πλαστογράφησης. Ο εισβολέας προσπαθεί να δημιουργήσει τη μέγιστη δυνατή εμπλοκή σε αντίθεση με την επίθεση

πλαστογράφησης. Τα συστήματα massive MIMO είναι γενικά ανθεκτικά σε παθητικές επιθέσεις υποκλοπής λόγω του ότι σε αυτά πολλές κεραίες εξυπηρετούν ένα συγκεκριμένο χρήστη. Παρόλα αυτά ο εισβολέας μπορεί να πάρει αντίμετρα, αξιοποιώντας την υψηλή συσχέτιση καναλιών, την εγγύτητα του χρήστη ή την αδυναμία της εκτίμησης καναλιού. Η διαδικασία εκτίμησης καναλιών στο MIMO υπήρξε ένας από τους εύκολους στόχους για επιθέσεις ασφαλείας. Πληροφορίες κατάστασης λανθασμένου καναλιού μπορούν επίσης να χρησιμοποιηθούν για επιθέσεις παρεμβολής. Κάποιες από τις λύσεις ασφαλείας που προτείνονται για massive MIMO αναφέρονται παρακάτω. Για να αξιοποιηθούν πλήρως τα οφέλη του MIMO, το σύστημα πρέπει να ασφαλιστεί απέναντι στις σημαντικές προκλήσεις ασφαλείας που προκύπτουν. Η μετάδοση τυχαίων πιλοτικών σημάτων έτσι ώστε να γίνει εντοπισμός ενεργών υποκλοπών , αποτελεί μια μέθοδο ανίχνευσης. Σε αυτήν ο νόμιμος χρήστης μεταδίδει μια ακολουθία τυχαίων συμβόλων που επιτρέπει στο σταθμό βάσης να ανιχνεύσει τον εισβολέα. Το μειονέκτημα αυτής της μεθόδου είναι ότι επιβαρύνει τα γενικά έξοδα μετάδοσης πρόσθετων τυχαίων ακολουθιών. Μια άλλη μέθοδο για την ανίχνευση ενεργής υποκλοπής, είναι ο διαμορφωτής δέσμης να είναι κατασκευασμένος με τέτοιο τρόπο ώστε το λαμβανόμενο δείγμα από τον νόμιμο χρήστη να ισούται με μία συμφωνημένη αξία. Όταν θα υπάρχει εισβολέας ο νόμιμος χρήστης θα το καταλάβει καθώς θα δει μια μικρότερη τιμή. Σταθμοί βάσης που συνεργάζονται μεταξύ τους μπορούν να ανιχνεύσουν ενεργές υποκλοπές. Σε τέτοια σενάρια, διαφορετικοί σταθμοί βάσης μπορούν να ανταλλάσσουν πληροφορίες και έτσι παρουσιάζετε μια ευκαιρία για από κοινού εκτίμηση του επίπεδο νόμιμης μόλυνσης που προκαλείται από τους πιλότους. Μηχανισμοί μηχανών μάθησης (Machine-Learning) μπορούν επίσης να χρησιμοποιηθούν για την ανίχνευση ενεργών επιθέσεων υποκλοπής. Στο massive MIMO ο σταθμός βάσης είναι δυνατόν να εξυπηρετήσει μεγάλο αριθμό χρηστών την ίδια στιγμή. Μια περίπτωση επίθεσης μπορεί να συμβεί ακόμα, όταν ένας εισβολέας κάνει χρήση ισχυρών συστοιχιών κεραιών για την παρακολούθηση πληροφοριών. Η προσέγγιση ασφαλείας επιπέδου που ονομάζεται, αρχική φάση συμβόλου περιστρεφόμενου συστήματος ασφαλούς μετάδοσης προτείνεται για την άμυνα έναντι αυτού ένα σενάριο. Η βασική ιδέα αυτής είναι να περιστρέψουμε τη φάση του αρχικού σήματος τυχαία για να μπερδέψει τον εισβολέα, ενώ στην άλλη πλευρά, οι νόμιμοι χρήστες μπορούν να βρουν σωστά την περιστροφή φάσης με τις απαραίτητες κατάλληλες αντίστροφες λειτουργίες για να

ανακτήσουν την αρχική μετάδοση. Ένας δέκτης ανθεκτικός στην εμπλοκή προτείνεται για να αντιμετωπιστούν οι επιθέσεις παρεμβολής σε μαζική ανοδική σύνδεση MIMO. [13]

2.3.2 Ασφάλεια στο SDN.

Το SDN όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο διαχωρίζει το επίπεδο ελέγχου δικτύου από το επίπεδο προώθησης και συγκεντρώνει τον έλεγχο του δικτύου σε πλατφόρμες λογισμικού ελέγχου δικτύου. Στη δικτύωση μέσω λογισμικού, η αλληλεπίδραση μεταξύ των συναρτήσεων ελέγχου με τις συσκευές προώθησης γίνεται μέσω εφαρμογών (application). Αυτό επιτυγχάνει απλότητα στον έλεγχο, τη διαχείριση, τη λειτουργία του δικτύου, και επιταχύνει την καινοτομία στην ανάπτυξη των χαρακτηριστικών δικτύου. Τρία λειτουργικά επίπεδα με διεπαφές μεταξύ τους, αποτελούν την αρχιτεκτονική του SDN. Το OpenFlow που είναι μια εφαρμογή του SDN έχει ακριβώς αυτή την αρχιτεκτονική των τριών επιπέδων , έτσι έχει τις εφαρμογές, τον ελεγκτή και τους διακόπτες OpenFlow. Η αρχιτεκτονική του SDN φαίνεται στην παρακάτω εικόνα. [17]



Εικόνα 16: SDN Architecture. [17]

Παρακάτω θα αναφερθούμε στις προκλήσεις ασφαλείας στο SDN. Οι λειτουργίες δικτύου μπορούν να υλοποιηθούν σαν εφαρμογές που αναπτύσσονται στο επίπεδο εφαρμογής του. Οι εφαρμογές SDN μπορούν να χειρίζονται το δίκτυο σύμφωνα με τις απαιτήσεις της εφαρμογής. Ωστόσο, το SDN έχει πολλές προκλήσεις ασφαλείας, οι περισσότερες εκ των οποίων έχουν αποδειχθεί σχετικά με το OpenFlow του SDN. Για παράδειγμα, ο κεντρικός έλεγχος του δικτύου κάνει την πλατφόρμα ελέγχου ευνοϊκή για επιθέσεις Denial-of-Service (DoS). Επίσης το δίκτυο μπορεί να δεχθεί απειλές ασφαλείας όταν κρίσιμες εφαρμογές εκτεθούν σε κακόβουλο λογισμικό.

Μετά την αναφορά σε κάθε πρόκληση ασφαλείας στο SDN,θα παρουσιάζουμε και τις λύσεις ασφαλείας που προτείνονται για κάθε μια από αυτές . Η ασφάλεια του SDN είναι ένα πολυδιάστατο θέμα που αφορά τόσο την ασφάλεια του SDN λόγω της εγγενούς φύσης του, που το κάνει ευάλωτο σε απειλές ασφαλείας, όσο και στο πώς το SDN με τον κεντρικοποιημένο έλεγχο δικτύου και τον μεγαλύτερο έλεγχο και ορατότητα των κυκλοφοριακών ροών, μπορεί χρησιμοποιείται για την αύξηση της ασφάλειας του δικτύου. Θα εστιάσουμε κυρίως, στους προτεινόμενους μηχανισμούς ασφαλείας για την αύξηση της ασφάλειας εντός του SDN και των επιμέρους επιπέδων του. [13]

2.3.2.1 Προκλήσεις ασφάλειας και λύσεις στις εφαρμογές του SDN.

Προκλήσεις σχετικά με εφαρμογές του SDN: Το SDN φέρνει καινοτομία στα δίκτυα επικοινωνίας αλλά μαζί με αυτήν φέρνει και πολλές ευπάθειες ασφαλείας. Ο έλεγχος του δικτύου με λογισμικό, και το συγκεντρωτικό έξυπνο δίκτυο αποτελούν τις δυο βασικές ιδιότητες του SDN. Οι περισσότερες λειτουργίες του δικτύου στο SDN υλοποιούνται σαν εφαρμογές, οπότε αυτό σημαίνει ότι μπορεί να γίνει μια σημαντική ζημιά στο δίκτυο, αν μια κακόβουλη εφαρμογή αποκτήσει πρόσβαση. Τα open APIs , η έλλειψη σωστού ελέγχου ταυτότητας , η έλλειψη μηχανισμών εμπιστοσύνης και τεχνικών αδειοδότησης αιτήσεων μπορεί να αποτελούν παράγοντες για προκλήσεις ασφαλείας που εισάγονται από εφαρμογές. Όπως γίνεται κατανοητό θα πρέπει να βρεθούν λύσεις στις παραπάνω προκλήσεις ασφαλείας πριν ενεργοποιηθούν οι εφαρμογές SDN που θα λειτουργούν το δίκτυο.

Λύσεις ασφαλείας για το επίπεδο εφαρμογών του SDN: Στο SDN δεν πρέπει να παραχωρείτε πρόσβαση σε κακόβουλο λογισμικό, στο δίκτυο ή το επίπεδο ελέγχου δικτύου. Υπάρχουν διάφορες προτάσεις για το πως πρέπει να γίνεται αυστηρή επαλήθευση στις εφαρμογές του SDN, προτού τους παραχωρηθεί πρόσβαση για διαμορφώσεις δικτύου μέσω του επιπέδου ελέγχου. Το PermOF είναι ένα λεπτομερές σύστημα αδειών που θέτει όρια στις εφαρμογές ώστε να λειτουργούν εντός των καθορισμένων προνομίων του. Το PermOF είναι σχεδιασμένο έτσι ώστε να παρέχει σε διαφορετική εφαρμογή τον έλεγχο αδείας που αφορά την ανάγνωση, την εγγραφή, την ειδοποίηση και το σύστημα δικαιωμάτων. Έτσι, προστατεύει τις πλατφόρμες ελέγχου από κακόβουλες εφαρμογές. Άλλα συστήματα αδειών για εφαρμογές SDN που υπάρχουν διασφαλίζουν ότι οι λειτουργίες στο επίπεδο ελέγχου είναι διαθέσιμες μόνο σε αξιόπιστες εφαρμογές. Ομοίως, το FortNOX είναι ένας πυρήνας επιβολής ασφάλειας που προτείνεται ως μια λύση για κακόβουλες εφαρμογές το οποίο υλοποιεί εξουσιοδότηση βάση ρόλων για κάθε εφαρμογή του OpenFlow. Τέλος, ένα σύστημα αδειών που αφορά εφαρμογές και ουσιαστικά διασφαλίζει την προστασία της λειτουργίας του ελεγκτή από κακόβουλα προγράμματα προτείνεται από τον ελεγκτή Rose-Mary. [13]

2.3.2.2 Προκλήσεις ασφάλειας και λύσεις στους ελεγκτές του SDN.

Προκλήσεις ασφάλειας στους ελεγκτές του SDN: Το κεντρικοποιημένο επίπεδο ελέγχου (control plane) του SDN (π.χ. ελεγκτής OpenFlow) το κάνει ένα εξαιρετικό στόχο για την παραβίαση του δικτύου ή τη διεξαγωγή κακόβουλων δραστηριοτήτων στο δίκτυο, λόγω του κεντρικού ρόλο στη λήψη αποφάσεων. Οι κύριοι τύποι απειλών αποτελούν οι επιθέσεις DoS και DistributedDoS. Ωστόσο, ο συγκεντρωτικός έλεγχος επιπέδου, όπως υλοποιείται στο OpenFlow έχει ακόμα περισσότερες συνέπειες στην ασφάλεια. Για παράδειγμα, η ορατότητα ελεγκτή, οι εφαρμογές ελέγχου, η επεκτασιμότητα του ελεγκτή μπορεί να χρησιμοποιείται αντίστροφα για να πλήξει την ασφάλεια ολόκληρου του δικτύου.

Λύσεις ασφαλείας για το επίπεδο ελέγχου (control plane) του SDN: Λόγω του κεντρικού ρόλου του επιπέδου ελέγχου, υπάρχουν πολλές προτάσεις και προσεγγίσεις για την ενίσχυση της ασφάλειάς του. Η Ενισχυμένη Ασφάλεια (Security-

Enhanced) του ελεγκτή Floodlight επεκτείνει την ασφάλεια του αρχικού ελεγκτή Floodlight. Για να ασφαλίσει το επίπεδο ελέγχου SDN, ο ελεγκτής SE-Floodlight παρέχει μηχανισμούς για διαχωρισμό των προνομίων, με την προσθήκη ενός ασφαλούς προγραμματιζόμενου north-bound API στον ελεγκτή SDN. Λειτουργεί ως διαμεσολαβητής μεταξύ της εφαρμογής και των επιπέδων δεδομένων επαληθεύοντας κανόνες ροής που δημιουργούνται από εφαρμογές. Ο ελεγκτής ROSEMARY είναι ένα ισχυρό λειτουργικό σύστημα δικτύου για τον SDN ελεγκτή και την ασφάλειά του από κακόβουλες εφαρμογές. Για την προστασία από τις επιθέσεις Dos, αλλά των προβλημάτων επεκτασιμότητας του ελεγκτή, το AVANT-GUARD έχει την δυνατότητα να βάζει όρια στα αιτήματα ροής στο επίπεδο ελέγχου. Υπάρχουν επίσης διάφορές προσεγγίσεις όπως οι αυτοοργανωμένοι χάρτες, για τη βελτίωση της ασφάλειας στο επιπέδου ελέγχου έναντι των επιθέσεων DoS και Distributed DoS (DDoS). Περαιτέρω προσεγγίσεις για την αύξηση της ανθεκτικότητας του ελεγκτή κατά των ελλείψεων ασφαλείας περιλαμβάνουν, το κατανεμημένο επίπεδο ελέγχου, τοποθέτηση ελεγκτή, πλεονασμό επιπέδου και αντιδραστικό έναντι προληπτικού ελέγχου κανόνων ροής και ενημερώσεων. [13]

2.3.2.3 Προκλήσεις ασφάλειας και λύσεις στο επίπεδο δεδομένων (data plane).

Προκλήσεις ασφαλείας στο επίπεδο δεδομένων: Το επίπεδο δεδομένων του SDN, περιλαμβάνει απλές συσκευές προώθησης με πίνακες ροής, που χρησιμοποιούνται από ελεγκτές SDN για την εγκατάσταση κανόνων προώθησης ροής . Οι επιθέσεις κορεσμού γνωστές ως saturation attacks, εκμεταλλεύονται το ότι οι πίνακες ροής δεν έχουν απεριόριστη χωρητικότητα και είναι δυνατόν να εξαντληθούν διατηρώντας έναν μεγάλο αριθμό αυτόκλητων ροών. Έτσι με κακόβουλες ροές με διαφορετικές κεφαλίδες πεδίων καταφέρνουν να εξαντλούν τους πίνακες ροής . Κατά τη διάρκεια τέτοιων επιθέσεων, θα υπάρχουν νόμιμες ροές που θα απορρίπτονται λόγω της περιορισμένης ικανότητας του μεταγωγέα να ρυθμίσει ροές TCP/UDP. Λόγω του ότι η διακόπτες του SDN δεν έχουν τη δυνατότητα να ξεχωρίζουν ποιες ροές είναι νόμιμες και ποιες κακόβουλες υπάρχει περίπτωση να χρησιμοποιηθούν για επιθέσεις σε άλλους διακόπτες ή και ελεγκτές.

Λύσεις ασφαλείας για το επίπεδο δεδομένων: Το επίπεδο δεδομένων μεταφέρει τα πραγματικά πακέτα και χρειάζεται τους κατάλληλους μηχανισμούς ασφαλείας. Λόγω της ικανότητας των εφαρμογών να αλλάζουν την διαμόρφωση στο επίπεδο προώθησης δεδομένων, θα πρέπει να υπάρχει προστασία από εφαρμογές μη εξουσιοδοτημένες. Για το λόγο αυτό πρέπει να υπάρχουν κάποιοι μηχανισμοί ασφαλείας, σε εφαρμογές που μπορούν να κάνουν αλλαγές σε κανόνες ροής στα στοιχεία του επιπέδου προώθησης δεδομένων. Έναν τέτοιο μηχανισμό μας δίνει το FortNox, το οποίο δίνει τη δυνατότητα στον ελεγκτή να μπορεί να τσεκάρει αν προκύπτουν αντιφάσεις σε κανόνες ροής που προέκυψαν από εφαρμογές. Το FlowChecker μπορεί να ελέγξει και να εντοπίσει ασυνέπειες στους κανόνες ροής σε διακόπτες OpenFlow, όπως επίσης να εντοπίσει εσφαλμένες διαμορφώσεις εντός του διακόπτη μέσω δυαδικών διαγραμμάτων απόφασης. [13]

2.3.2.4 Προκλήσεις ασφάλειας και λύσεις στις διεπαφές (interfaces) του SDN.

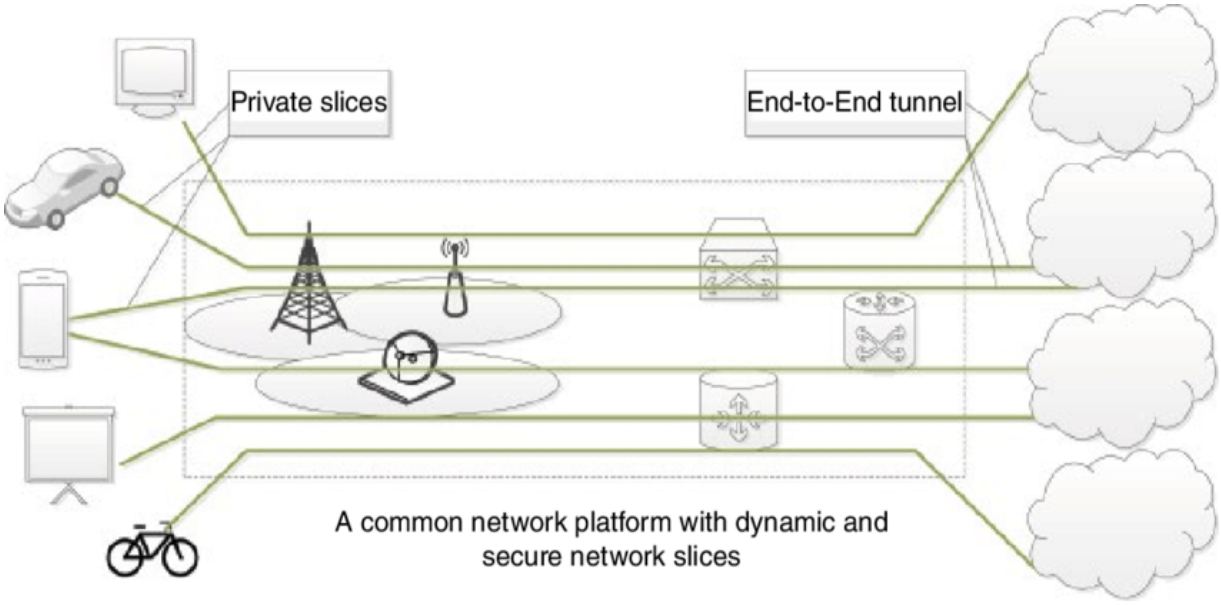
Προκλήσεις ασφαλείας στις διεπαφές του SDN: Η north-bound και η south-bound αποτελούν τις κύριες διεπαφές του SDN. Η πρώτη αποτελεί τη διεπαφή μεταξύ ελεγκτών και εφαρμογών και η δεύτερη μεταξύ ελεγκτών και των διακοπτών του. Η south-bound διεπαφή λόγω της χρήσης του TLS και του DTLS είναι ανοιχτή σε πολλές επιθέσεις μεταξύ των οποίων οι υποκλοπές και οι επιθέσεις στο επίπεδο ελέγχου, ενώ η north-bound διεπαφή είναι πρόκληση ασφαλείας για απομακρυσμένες εφαρμογές λόγω της μη διαθεσιμότητας τυποποιημένων διεπαφών.

Λύσεις ασφαλείας για τις διεπαφές SDN: Η north-bound διεπαφή στο SDN εξακολουθεί να είναι μια ανοιχτή πρόκληση ασφαλείας αν και υπάρχουν πολλές προτάσεις για την ασφάλεια της διεπαφής του ελεγκτή από κακόβουλες εφαρμογές. Η κύρια πρόκληση που χρειάζεται περαιτέρω έρευνα είναι η ασφάλεια της διεπαφής όταν οι απομακρυσμένες εφαρμογές θέλουν να έχουν πρόσβαση στο επίπεδο ελέγχου ή να διαμορφώσουν το επίπεδο δεδομένων. Όσον αφορά τις south-bound διεπαφές, που κάνουν χρήση του TLS, ακόμα δεν υπάρχουν κάποιοι μηχανισμοί ασφαλείας, ωστόσο το πρωτόκολλο OpenFlow υποστηρίζει TLS και DTLS για TCP και UDP αντίστοιχα. Το TLS που παρέχει απόρρητο και ακεραιότητα δεδομένων για την επικοινωνία του χρήστη, χρησιμοποιεί συμμετρική κρυπτογραφία για την

κρυπτογράφηση δεδομένων, ενώ το DTLS διασφαλίζει την κυκλοφορία UDP μεταξύ των εφαρμογών. [13]

2.3.3 Ασφάλεια στο NFV.

Το NFV βασιζόμενο στην ιδέα της εικονικοποίησης κάνει το διαχωρισμό των λειτουργιών του δικτύου από το υποκείμενο ιδιόκτητο υλικό, μεταφέροντας τις λειτουργίες του δικτύου σε εφαρμογές λογισμικού. Καταφέρνει να παρέχει λειτουργίες δικτύου που βασίζονται στη ζήτηση σε κάθε μέρος του δικτύου, χωρίς την ανάγκη για εξοπλισμό λειτουργίας. Παρόλα αυτά με την χρήση του, έχουν προκύψει προκλήσεις ασφαλείας που αφορούν την ασφάλεια των πληροφοριών των χρηστών, τις υπηρεσίες και το ίδιο το δίκτυο. Παρακάτω θα αναφερθούμε στις προκλήσεις ασφαλείας στο NFV. Με την ανάπτυξη του NFV, μια σειρά από προκλήσεις ασφαλείας θα εμφανιστούν κυρίως λόγω της δυνατότητας μετεγκατάστασης λειτουργιών ή υπηρεσιών από το ένα σημείο στο άλλο ή από τον έναν πόρο στον άλλο. Δεδομένου ότι ο αριθμός των υπηρεσιών ή των εικονικών λειτουργιών θα αυξηθεί, μια ανησυχία σχετίζεται με τις χειροκίνητες διαμορφώσεις των εικονικών συστημάτων ή των VNF που μπορούν να οδηγήσουν σε δυναμικές παραβιάσεις ασφαλείας λόγω της αυξημένης πολυπλοκότητας με την ανάπτυξη των συστημάτων. Επίσης, ο αυξημένος αριθμός των VNF αποτελεί σημαντική ανησυχία για μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, υποκλοπές κυκλοφορίας και κλοπή υπηρεσιών. Εξάλλου, υπάρχουν προκλήσεις ασφαλείας που κληρονομούνται στα εικονικά ή NFV συστήματα. Μετά την αναφορά σε κάθε πρόκληση ασφαλείας θα αναφερόμαστε στις προτεινόμενες λύσεις ασφαλείας για αυτή την πρόκληση. Η εικονικοποίηση μέσω του μηχανισμού του network slicing (τεμαχισμού δικτύου) μπορεί να αυξήσει εξαιρετικά την ασφάλεια του χρήστη. Με το network slicing γίνεται ο διαχωρισμός της κυκλοφορίας διαφορετικών υπηρεσιών ή τμημάτων δικτύου, οι οποίες βασίζονται σε προτεραιότητες ασφαλείας της υπηρεσίας και του δικτύου. Επίσης για την αύξηση της διαθεσιμότητας και της επεκτασιμότητας αλλά και της αντιμετώπισης επιθέσεων DoS και DDoS μπορούν να αναπτυχθούν κατανεμημένα VNF. Τα VNF μπορούν να βελτιώσουν την ασφάλεια στα 5G δίκτυα, μέσω της προσθήκης περισσότερης νοημοσύνη για αυτοπροστασία. Το network slicing αποτελεί βασικό πλεονέκτημα του 5G σε σύγκριση με τα δίκτυα προηγούμενης γενιάς. [13]



Εικόνα 17: Ασφαλείς end-to-end tunnels για διαφορετικές υπηρεσίες. [19]

2.3.3.1 Προκλήσεις ασφαλείας και λύσεις σε εικονικά συστήματα.

Προκλήσεις σε εικονικά συστήματα: Εικονικά συστήματα τα οποία εκτελούνται στο ίδιο στοιχείο δικτύου, είναι πιθανόν να μην χρειάζονται την ίδια ασφάλεια. Οπότε όπως γίνεται κατανοητό δεν γίνεται να εφαρμοστούν οι ίδιες πολιτικές ασφαλείας σε όλο το μηχάνημα. Ένα σενάριο που υπάρχει, είναι ένας διακομιστής να φιλοξενεί μια εικονική μηχανή που χωρίζεται σε πολλές ζώνες καθεμία από τις οποίες έχει διαφορετικά επίπεδα ασφάλειας. Η κάθε ζώνη που έχει ένα συγκεκριμένο επίπεδο ασφαλείας δεν μπορεί να μετακινηθεί σε άλλο φυσικό διακομιστή, γιατί αυτός μπορεί να έχει ένα άλλο επίπεδο ασφαλείας που δεν μπορεί να την υποστηρίξει. Ακόμα η υπηρεσία αλυσίδας διαφόρων του NFV θα κάνει την ανάλυση αιτιών των απειλών ασφαλείας ακόμη πιο περίπλοκη.

Λύσεις ασφαλείας για εικονικά συστήματα: Τα εικονικά συστήματα παρόλη την δυσκολία στην παρακολούθηση, έχουν πολλά πλεονεκτήματα στην ασφάλεια. Παραδείγματος χάριν ένα εικονικό σύστημα εύκολα μεταφέρεται όταν δεχθεί κάποια επίθεση για να ελαχιστοποιηθούν οι επιπτώσεις της. Για τις προκλήσεις που προκύπτουν για την διασφάλιση της σταθερότητας των πολιτικών ασφαλείας σε εικονικά δίκτυα, προτείνεται η χρήση ενός διαχειριστή πολιτικής, που επιβάλλει μια πολιτική ασφάλειας σε δυναμικά περιβάλλοντα VNF .Το προτεινόμενο στοιχείο

λογισμικού για το NFV δίνει στους χρήστες ένα τρόπο να προσδιορίσουν και να επιβάλλουν τις δικές τους απαιτήσεις εντός του δικτύου, αποφεύγοντας τις πολύπλοκες διαδικασίες ασφαλείας. [13]

2.3.3.2 Προκλήσεις ασφαλείας και λύσεις σε hypervisors.

Προκλήσεις σε hypervisors: Οι hypervisors χρησιμοποιούνται στην εικονικοποίηση για να αντιστοιχούν σε λογικά στιγμιότυπα δικτύου ή φυσικό υλικό στοιχείων δικτύου διάφορες λειτουργίες δικτύου Ο hypervisor αποτελεί την κύρια οντότητα του εικονικού συστήματος που βασίζεται σε hypervisor και μπορεί να ελέγχει τον προγραμματισμό της CPU και να εκτελεί πολλαπλές λειτουργίες συστημάτων. Αυτό σημαίνει ότι εάν παραβιαστεί ένας hypervisor, ολόκληρο το σύστημα μπορεί να τεθεί σε κίνδυνο. Ο hypervisor μπορεί να γίνει στόχος μίας σειράς επιθέσεων. Επιθέσεις DoS σε VM, οι VM hopping επιθέσεις και επιθέσεις για την εκμετάλλευση του λειτουργικού συστήματος του κεντρικού υπολογιστή με σκοπό να πληγεί η απομόνωση ενός τμήματος, είναι τέτοιες επιθέσεις.

Λύσεις ασφαλείας για hypervisors: Λόγω του κεντρικού ρόλου του hypervisor, η βασική επιλογή για την ενίσχυση της ασφάλειάς του, είναι η ελάχιστη ή περιορισμένη έκθεση σε VM ή άλλα συστήματα. Ενεργώντας για αυτούς τους λόγους, η τροποποιημένη έκδοση του Xen που ονομάζεται Xoar αυξάνει την ασφάλειά του. Η πλατφόρμα σπάει το VM ελέγχου σε πολλαπλά VM ενός σκοπού, για να κάνει σαφή την έκθεση στον κίνδυνο ,ενώ διατηρεί τα ελάχιστα προνόμια πρόσβασης και έτσι αυξάνει την ασφάλεια του συνολικού συστήματος. Το OpenVirteX παρουσιάζει μια νέα ενδιαφέρουσα πλατφόρμα εικονικοποίησης δικτύου που παρέχει στους πελάτες εικονικά SDN. Ο hypervisor λειτουργεί όπως ο ελεγκτής στο OpenFlow όπου τα slices των χρηστών έχουν τα δικά τους επίπεδα ελέγχου και δεδομένων. Εδώ ο ελεγκτής SDN μπορεί να παρακολουθεί τα κενά ασφαλείας καθώς έχει τη δυνατότητα να προσπερνά τις δραστηριότητες του hypervisor. [13]

2.3.3.3 Προκλήσεις ασφαλείας και λύσεις που προκύπτουν λόγω δυναμικότητας.

Προκλήσεις λόγω δυναμικότητας: Λόγω της φύσης των εικονικών μηχανών και την δυνατότητα τους να δημιουργούνται να διαγράφονται και να μετακινούνται πολύ εύκολα σε ένα δίκτυο, γίνεται εύκολα το πόσο δύσκολη πρόκληση θα αποτελέσει η παρακολούθηση μιας εικονικής κακόβουλης μηχανής. Αυτό θα ισχύει και στα 5G δίκτυα. Μια σημαντική πρόκληση θα αφορά το VNF που θα είναι πιο επιρρεπείς σε σφάλματα διαμόρφωσης λόγω της δυναμικής φύσης του. Πολλές προκλήσεις της εικονικοποίησης όπως η απώλεια της μοναδικότητας συσκευών και των δεδομένων , στο 5G θα είναι ακόμα πιο έντονη, λόγω του IoT. Επίσης θα είναι δυσκολότερη η παρακολούθηση των κακόβουλων συσκευών και η ανάπτυξη συστήματος εμπιστοσύνης μεταξύ hypervisors και VM.

Λύσεις ασφαλείας για το dynamicity: Η δυναμική φύση των VNF και οι εικονικοί πόροι μπορούν να χρησιμοποιηθούν ως δύναμη από άποψη ασφάλειας. Για παράδειγμα, η ευελιξία του NFV επιτρέπει την απομόνωση παραβιασμένων στοιχείων δικτύου ή ακόμη και ολόκληρων τμημάτων δικτύου μέσω του καθορισμού ζωνών ασφαλείας και της χρήσης του συστήματος διεύθυνσης κυκλοφορίας. Τέλος για τη δυναμική διαχείριση των λειτουργιών ασφαλείας και την διασφάλιση των υποδομών και των πλατφορμών που βασίζονται σε NFV, έχει προταθεί ένα διαχειριζόμενο πλαίσιο ενορχήστρωσης προσανατολισμένο στην ασφάλεια. [13]

2.3.3.4 Προκλήσεις ασφαλείας και λύσεις για : Mobile Virtual Network Operators (MVNOs).

Προκλήσεις για MVNO: Τα MVNOs κάνουν το NFV να λειτουργεί το δίκτυο με τέτοιο τρόπο, ώστε να αντιμετωπίζονται οι προκλήσεις ασφαλείας που οφείλονται κυρίως στους περιορισμούς που προκύπτουν στα τρέχοντα συστήματα NFV . Για την ανάπτυξη των υπηρεσιών τους, οι κάτοχοι υποδομής δικτύου θα εκθέσουν τα API τους σε πλατφόρμες δικτύου τρίτων. Δεδομένου ότι το 5G θα έχει πολύ διαφορετικούς φορείς, γίνεται κατανοητό ότι στις υπηρεσίες τους μπορεί να είναι πολλοί παρόχοι υπηρεσίας. Δηλαδή μπορεί την ίδια υποδομή δικτύου να την μοιράζονται, πολλαπλά MVNO , πάροχοι υπηρεσιών επικοινωνίας και άλλοι πάροχοι υπηρεσιών. Όλοι αυτοί οι πάροχοι υπηρεσίας θα έχουν διαφορετικές πολιτικές ασφαλείας και απορρήτου. Οι

διαφορετικές πολιτικές ασφαλείας και απορρήτου που έχουν όλοι αυτοί οι πάροχοι αποτελεί μια ακόμα πρόκληση.

Λύσεις ασφαλείας για MVNO: Η ασφάλεια των MVNO εξαρτάται πολύ από την ασφάλεια των συστημάτων που χρησιμοποιούν τα MVNO. Ωστόσο, αυτό δεν είναι αρκετό από μόνο του. Προτείνεται ένα πλαίσιο ασφάλειας και εμπιστοσύνης για VNF σε βασισμένα σε SDN κινητά δίκτυα Το προτεινόμενο πλαίσιο εφαρμόζει προσαρμοστικές τεχνολογίες αξιολόγησης εμπιστοσύνης, διαχείρισης και βιώσιμες αξιόπιστες τεχνολογίες υπολογιστών, για διασφάλιση της εμπιστοσύνης της υπολογιστικής πλατφόρμας και επιτυγχάνει καθορισμένη από το λογισμικό ασφάλεια δικτύου. Ομοίως, προτείνεται, ένα πλαίσιο διαχείρισης ασφάλειας και ενορχήστρωσης βασισμένο στο NFV ,το οποίο προστατεύει τους πόρους ή άλλα VNF από απειλές ασφαλείας που προέρχονται από το διαδίκτυο ή άλλα VNF, επικυρώνοντας τα χαρακτηριστικά ασφαλείας τους. Ωστόσο, η περιορισμένη ανάπτυξη τέτοιων χειριστών σε πραγματικό χρόνο καθιστά δύσκολη την κατανόηση του πλήρους φάσματος των πιθανών απειλών ασφαλείας. [13]

2.3.4 Ασφάλεια στο Cloud.

Το cloud computing παρέχει υπολογιστικούς πόρους και υπηρεσίες κατ' απαίτηση, τόσο σε μικρές όσο και σε μεγάλες επιχειρήσεις, βελτιστοποιώντας τους διαθέσιμους πόρους και επιτρέποντας μεγαλύτερη αφαίρεση των υποκείμενων μηχανισμών από την πλευρά του πελάτη. Στην εποχή μας τεχνολογικοί κολοσσοί έχουν υιοθετήσει, χρησιμοποιούν το cloud και αναπτύσσονται μέσω των δυνατότητων του. Οι μαζικές επικοινωνίες τύπου μηχανής αποτελούν μια από τις κύριες περιπτώσεις χρήσης του cloud computing στο 5G. Στις μαζικές επικοινωνίες τύπου μηχανής ένας μεγάλος αριθμός συνδεδεμένων μηχανών που αποτελούν ένα δίκτυο αισθητήρων και ενεργοποιητών υποστηρίζουν ένα μεγάλο αριθμό συσκευών χαμηλού κόστους και μικρής ενέργειας. Εδώ φαίνεται να υπάρχει η ανάγκη για cloud computing με κοινή χρήση δεδομένων σε πραγματικό χρόνο μεταξύ των συσκευών και για cloud computing συσκευών χαμηλής αποθήκευσης που θα παρέχονται με εικονική χωρητικότητα αποθήκευσης στο cloud. Το MEC (Multi-Access Edge Computing) είναι μια άλλη βασική περίπτωση χρήσης του cloud computing και έχει μεγάλη σημασία για

τα δίκτυα κινητής τηλεφωνίας 5G και όχι μόνο. Μέσω του MEC γίνεται επέκταση των δυνατοτήτων της πληροφορικής και του cloud computing εντός του RAN στην άκρη των δικτύων κινητής τηλεφωνίας. Έτσι δίνεται η δυνατότητα άμεσης πρόσβασης στους παρόχους περιεχομένου σε πληροφορίες ραδιοφώνου σε πραγματικό χρόνο, πετυχαίνοντας μικρή καθυστέρηση και υψηλό εύρος ζώνης. Όλες αυτές οι τεχνολογίες ωστόσο, φέρνουν μαζί τους μεγάλες προκλήσεις ασφαλείας.

Οι προκλήσεις ασφαλείας στο cloud computing συνδέονται σε μεγάλο βαθμό με τις τεχνολογίες που εμπλέκονται σε αυτό ,όπως η δικτύωση, εικονικοποίηση και οι υπηρεσίες που αναπτύσσονται σε αυτό. Όπως είναι εύκολα κατανοητό, λόγω των εικονικών και εξαιρετικά κατανεμημένων πόρων αλλά και των διαφορετικών τύπων υπηρεσιών στο cloud, δεν επαρκούν για την προστασία του οι παραδοσιακές μέθοδοι ασφαλείας. Υπάρχουν ποικίλες τεχνολογίες που εμπλέκονται στο cloud computing, και ως εκ τούτου, υπάρχουν ποικίλες προκλήσεις ασφάλειας που απαιτούν συγκεκριμένες λύσεις προσαρμοσμένες σε αυτές. Οι λύσεις για τις απειλές ασφάλεια στο cloud είναι πολύπλευρες. Για παράδειγμα, η ασφάλεια εικονικοποίησης και η ασφάλεια των VNF που υπάρχουν στο cloud, έχει άμεσες επιπτώσεις στην ασφάλεια του cloud. Παρακάτω θα μιλήσουμε και για τις λύσεις ασφαλείας για κάθε απειλή που θα αναφερθεί. [13]

2.3.4.1 Απειλές και λύσεις ασφαλείας στην εικονικοποίηση.

Απειλές εικονικοποίησης: Εφόσον η εικονικοποίηση θα παίζει ζωτικό ρόλο στο σχεδιασμό και την εφαρμογή των cloud-based δικτύων για την υλοποίηση του 5G, το πεδίο απειλών σε εικονικές πλατφόρμες, είναι εξίσου ανησυχητικό τόσο για τους παρόχους υπηρεσιών όσο και για τους χρήστες και προγραμματιστές των εφαρμογών. Επιθέσεις DoS αλλά και χειραγώγησης, μπορεί να θέτουν σε κίνδυνο την ασφάλεια του συστήματος, καθώς κακόβουλες οντότητες είναι δυνατόν να εκμεταλλεύονται διαρροές δεδομένων αλλά και να στοχεύουν συστήματα edge computing και hypervisors στις εικονικοποιημένες πλατφόρμες και υποδομές τους

Λύσεις Ασφαλείας για την εικονικοποίηση: Οι απειλές εδώ αφορούν κυρίως τις εικονικές μηχανές. Η ασφάλεια της εικονικής μηχανής, ήταν ένα μεγάλο και ενδιαφέρον έργο για εταιρείες όπως η IBM και η XEN. Τα μέτρα ασφαλείας που εφαρμόζονται στα

λειτουργικά συστήματα των φυσικών μηχανών είναι απαραίτητο να εφαρμόζονται και στα λειτουργικά συστήματα των εικονικών μηχανών, ούτως ώστε η στρατηγική ασφαλείας να είναι αποτελεσματική. Πριν η IBM αναπτύξει το TVDc που αποτελούσε μια προσπάθεια της για την αντιμετώπιση των προβλημάτων ασφαλείας στα εικονικά συστήματα, η XEN με το sHype δημιούργησε μια ασφαλή αρχιτεκτονική hypervisor για απομόνωση εικονικών συστημάτων με ασφάλεια ελέγχου πρόσβασης. Αυτά τα συστήματα μπορούν να κάνουν έλεγχο της ροής των πληροφοριών και τις επικοινωνίας μεταξύ πολλών VM σε διαφορετικά μηχανήματα. Επιθέσεις DoS σε εικονικά συστήματα μπορούν να αντιμετωπιστούν με τη χρήση firewall proxies. [13]

2.3.4.2 Απειλές και λύσεις για την ασφάλεια του Cyber Physical System που βασίζεται σε cloud.

Απειλές για την ασφάλεια του CPS που βασίζεται σε cloud: Τα Cyber-Physical Systems (CPS) που βασίζονται σε σύννεφο κάνουν εικονικοποίηση στοιχείων δικτύου με τη χρήση cyber-physical clouds και είναι εικονικά στοιχεία που παρέχονται σαν συμβατικοί πόροι cloud που χρησιμοποιούνται για την παροχή υπηρεσιών cloud. Επιθέσεις σε CPS περιλαμβάνουν HyperText Tranfer Protocol (HTTP) και Extensible Markup Language (XML), DoS (HX-DoS) attack. Οι επιθέσεις αυτές λειτουργούν ουσιαστικά γεμίζοντας τις υποδομές CPS cloud, συνδυάζοντας με καθορισμένους ρυθμούς μηνύματα HTTP και XML. Τέτοια επίθεση θα μπορεί να συμβεί σε υποδομές cloud, λογισμικού ή πλατφορμών όπως η Υποδομή ως υπηρεσία (Infrastracture as a Service,IaaS), η Υπηρεσία ως Υπηρεσία (Software as a Service,SaaS) και η Πλατφόρμα ως υπηρεσία (Platform as a Service,PaaS). Άλλη απειλή σε αυτό το πεδίο αποτελεί η Slowly-increasing Polymorphic DDoS Attack Strategy (SIPDAS), που αποτελεί ένα είδος DoS επίθεσης και λειτουργεί συμπεριφερόμενη δυναμικά ώστε να μην γίνεται αντιληπτή από τον αλγόριθμο ανίχνευσης.

Ασφάλεια σε Cyber-Physical σύστημα που βασίζεται σε cloud: Ένα τρόπος αντιμετώπισης για τις επιθέσεις CPS με τις προαναφερθέντες μορφές (HX-DoS, DDoS ή SIPDAS), είναι ο έλεγχος της κατανάλωσης των υπολογιστικών πόρων αλλά και ο έλεγχος του αριθμού των εισερχομένων αιτημάτων. Η ανίχνευση κάποιων ανωμαλιών θα ενεργοποιήσει ένα πιο προηγμένο μέτρο ελέγχου. Για τον μετριασμό των επιθέσεων CCPS με τη μορφή HX-DoS, προτείνετε η χρήση του λεγόμενου ENDER

(pre-dEcisioN, advaNce Decision, lEaRning) για τον εντοπισμό και το διαχωρισμό ενός νόμιμο CCPS από ένα παράνομο. Για να επιτύχει αυτό, το σύστημα ENDER χρησιμοποιεί δύο μεθόδους αποφάσεως, για την ανίχνευση κίνησης επιθέσεων και στη συνέχεια τη χρήση παρόμοιας τεχνική όπως στα παραδοσιακά συστήματα ανίχνευσης εισβολής (IDSs), Έτσι είναι στη συνέχεια σε θέση να αναγνωρίσει και να επισημάνει ένα μήνυμα επίθεσης. Όταν ανιχνευτεί ένα τέτοιο μήνυμα ,το σύστημα με τη χρήση ενός RAD αλγορίθμου μπορεί να το αφαιρέσει πριν αυτό του προκαλέσει ζημιά. [13]

2.3.4.3 Απειλές και λύσεις ασφαλείας για Cloud Intrusion.

Cloud intrusion: Η απειλή του cloud intrusion είναι μια απειλή στους πόρους και τις υπηρεσίες του cloud που αφορά την ακεραιότητα αλλά και την διαθεσιμότητα και εμπιστευτικότητα τους. Το πόσο σοβαρή μπορεί να είναι η απειλή έχει να κάνει με τις αδυναμίες του cloud αλλά και την εμπειρία του εκάστοτε εισβολέα. Πολλά διαφορετικά μοντέλα cloud μπορούν να επηρεαστούν από την απειλή του cloud intrusion.

Λύσεις ασφαλείας για εισβολή σύννεφων (Cloud Intrusion): Ο μετριασμός κατά της εισβολής σύννεφων επιτυγχάνεται κυρίως με τη δημιουργία Intrusion Detection System (IDS), ώστε να δουλέψει σε συνεργασία με άλλους μηχανισμούς ελέγχου στο περιβάλλον του cloud computing. Τα συστήματα αυτά έχουν ως σκοπό να βρίσκουν οποιαδήποτε απειλή και προσπάθεια για παραβίαση στο cloud και στις πολιτικές του ,παρακολουθώντας συνεχώς τις δραστηριότητες του. Συστήματα IDS υπάρχουν για τα διαφορετικά μοντέλα υπηρεσιών cloud IaaS, SaaS, PaaS, αλλά και για κεντρικούς υπολογιστές και hypervisors. Μεταξύ αυτών των IDS υπάρχουν τα βασισμένα σε hypervisor IDS, τα παραδοσιακά Host-IDS (HIDS) και τα network- IDS (NIDS). Τα HIDS αναπτύσσονται κατά προτίμηση στα εμπρός και πίσω άκρα της πλατφόρμας cloud, ενώ τα NIDS και τα IDS που βασίζονται σε hypervisor, είναι καλύτερα τοποθετημένα στο back-end όπου λειτουργούν τα CSP. Ένας άλλος τρόπος αντιμετώπισης του cloud intrusion είναι η δημιουργία cloud εφαρμογών που θα έχουν τη δυνατότητα να αναγνωρίζουν και να αγνοούν τα αιτήματα των εισβολέων. Ωστόσο αυτός ο τρόπος αντιμετώπισης για να είναι αποτελεσματικός θα πρέπει να είναι πάντα προσαρμοσμένος άρα και ενημερωμένος με τα συνεχώς εξελισσόμενα μοντέλα

επίθεσης, αλλιώς οι εισβολείς με την πάροδο του χρόνου θα βρουν κάποιο τρόπο να τον παρακάμψουν. [13]

2.3.4.4 Απειλές και λύσεις ασφαλείας από Insiders.

Επιθέσεις εκ των έσω (Insider attacks): Ουσιαστικά η επιθέσεις εκ των έσω, αφορούν επιθέσεις που προκαλούνται από το προσωπικό του παρόχου υπηρεσιών και αποτελούν μια πολύ σημαντική απειλή για το σύνολο του cloud. Το προσωπικό αυτό έχει πρόσβαση στους φυσικούς διακομιστές οπού και γίνεται η αποθήκευση των δεδομένων των χρηστών. Όπως γίνεται ευκολά αντιληπτό η κακή διαχείριση και χρήση των δεδομένων αυτών από αυτό το θεωρούμενο ως έμπιστο προσωπικό, αποτελεί μια σημαντική απειλή για όλο το cloud..

Λύσεις ασφαλείας για την επίθεση εκ των έσω (Insider attack): Ο μετριασμός τρωτών σημείων επίθεσης από insiders στα 5G δίκτυα που βασίζονται σε cloud,αποτελεί μια πρόκληση τόσο από κοινωνική όσο και από τεχνική πλευρά. Ενώ το CPS δουλεύουν για να παρέχουν χρήστες με ασφαλείς διεπαφές και API, η δυνατότητα κατάχρησης και η κακή χρήση των δεδομένων στο cloud από εξουσιοδοτημένο προσωπικό του παρόχου υπηρεσιών, αποτελεί μεγάλη ανησυχία. Αυτή η πρόκληση συγχέεται περαιτέρω από άλλα φυσικά συμβάντα όπως διαρροές και απώλειες δεδομένων. Από αυτή την άποψη, η ανάγκη για περισσότερα ισχυρές δυνατότητες δημιουργίας αντιγράφων ασφαλείας και πολλαπλών αντιγράφων ασφαλείας σε διαφορετικές τοποθεσίες και πλατφόρμες, έρχεται ως μια στρατηγική για μετριασμό. Για άλλες σκόπιμες επιθέσεις εκ των έσω, η υλοποίηση κατάλληλου ελέγχου και οι τακτικοί έλεγχοι ιστορικού σε συνδυασμό με την ψηφιακή σφράγιση χρόνου και τις υπογραφές σε δεδομένα cloud, θα μπορούσαν να βοηθήσουν για να μετριαστεί η πιθανότητα κατάχρησης και κακής χρήσης των δεδομένων του cloud από εξουσιοδοτημένους εμπιστευτικούς παράγοντες. [13]

Πίνακας 3: Προκλήσεις και λύσεις ασφαλείας στις βασικές τεχνολογίες του 5G. [13]

Τεχνολογία	Προκλήσεις Ασφαλείας	Λύσεις Ασφαλείας
MIMO	Μέθοδοι ανίχνευσης ενεργητικών επιθέσεων	Ασφάλεια mMimo
	Ανίχνευση ενεργής υποκλοπής	Original Symbol Phase Rotated Secure Transmission
	Ανίχνευση παθητικής υποκλοπής	Physical layer security
SDN	Εξουσιοδότηση εφαρμογής	PermOF
	Εξουσιοδότηση πρόσβασης επιπέδου ελέγχου	SE-Floodlight
	Επαλήθευση κανόνων ροής σε διακόπτες SDN	FlowChecker
	Παροχή ασφαλείας στα κανάλια ελέγχου	TLS Protocol
	Έλεγχος πρόσβασης βάσει ροής	Εισαγωγή ροής
	Ασφάλεια ελέγχου πρόσβασης βάσει υπηρεσιών	Χρήση Ασφαλούς πρωτοκόλλου
NFV	Διαμορφώσεις ασφαλείας NFV	Διαχειριστής πολιτικής
	Πλατφόρμα ασφαλείας NFV και VM	Xoar
	Ασφάλεια NFV Hypervisor	OpenVirteX
	Εξασφάλιση απομόνωσης κυκλοφορίας για VNF και εικονικά slices	Ικανότητα απομόνωσης
	Ενορχήστρωση NFV και ασφάλεια MVNO	Security and trust framework
Cloud	Μετριασμός HX-DoS για υπηρεσίες web cloud	ENDER
	Τεχνικές ανίχνευσης DoS και DDoS	Ανίχνευση DoS
	Επαλήθευση ακεραιότητας, ασφάλεια δεδομένων και συστήματα αποθήκευσης	Προτάσεις ασφάλειας
	Ασφάλεια ελέγχου πρόσβασης βάσει υπηρεσιών	Χρήση Ασφαλούς πρωτοκόλλου

ΚΕΦΑΛΑΙΟ 3ο

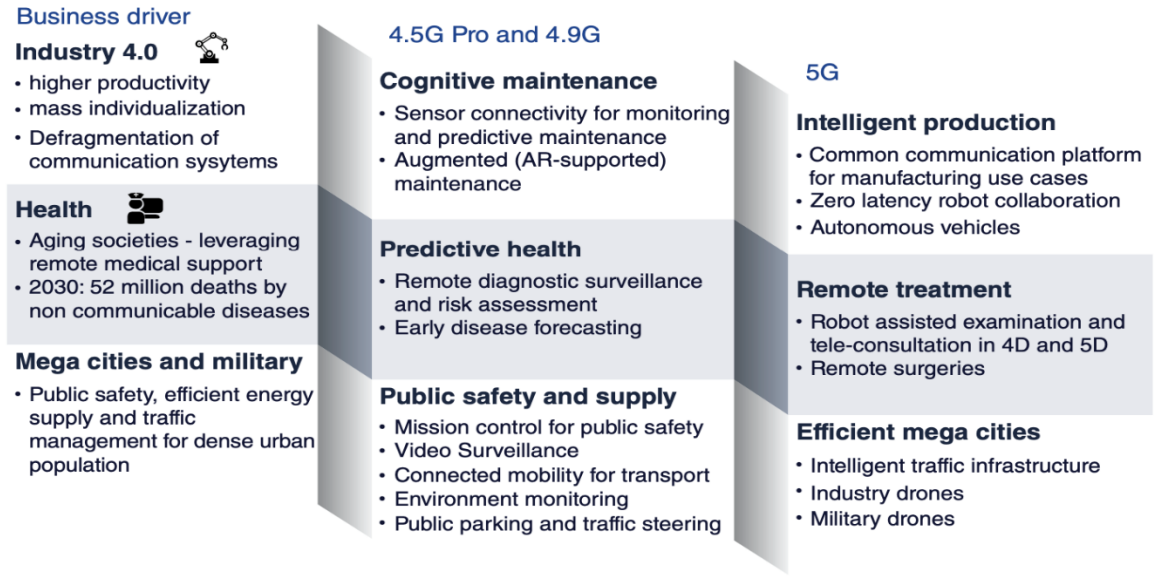
3.1 Ασφάλεια Συσκευών και Χρήστη

3.1.1 IOT συσκευές, υπηρεσίες και επιθέσεις.

Αν αναλογιστούμε το ποσοστό διείσδυσης των τεχνολογιών IoT στην αγορά των καταναλωτικών προϊόντων τα τελευταία χρόνια και το ότι αυτά τα προϊόντα αυξάνονται σε πλήθος, τότε καταλαβαίνουμε ότι έχουμε ένα νέο σύνολο υπολογιστικών συστημάτων που χρήζουν διασφάλισης. Κάθε νέος υπολογιστής, κάθε νέα εφαρμογή που συνδέεται δικτυακά (και ιντερνετικά) με άλλους υπολογιστές και εφαρμογές, τότε είναι εν δυνάμει στόχος κακόβουλων επιθέσεων. Αυτοί οι υπολογιστές και οι εφαρμογές χρειάζεται να προστατευτούν και να διασφαλιστούν βάσει των αρχών της Ασφάλειας: Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα, Ιδιωτικότητα, Αξιοπιστία. Αντίστοιχα λοιπόν με τους υπολογιστές και τις εφαρμογές τους, προστασίας χρήζουν και τα συστήματα IoT μιας και αυτά συνδέονται μεταξύ τους και με αλλά, όπως επίσης χρησιμοποιούν εφαρμογές που πρέπει να σχεδιάζονται και αυτές με βάση τις βασικές αρχές Ασφάλειας. Έτσι θα πρέπει να δούμε για κάθε μια τεχνολογία IoT που μας ενδιαφέρει κατά ποσό μπορεί να καλύψει αυτές τις βασικές αρχές ασφάλειας και με ποιο τρόπο.

Το Internet of Things ενέχει σημαντικούς κινδύνους για το σύνολο του ψηφιακού οικοσυστήματος. Αυτό οφείλεται στο γεγονός ότι πάρα πολλές τέτοιες συσκευές έχουν σχεδιαστεί χωρίς ενσωματωμένο σύστημα ασφάλειας για προστασία από τους χάκερ. Όσες περισσότερες συσκευές συνδέουμε και δημιουργείται περισσότερη αξία από τα δεδομένα που δημιουργούνται, ο κίνδυνος για παραβιάσεις και κατάχρηση ασφάλειας μεγαλώνει. Το IoHT (Internet of Hacked Things) αρχίζει να αυξάνεται ανησυχητικά. [20]

Μερικές από τις περιπτώσεις χρήσης 5G IoT απεικονίζονται στην παρακάτω εικόνα:



Εικόνα 18: Περιπτώσεις χρήσης 5G IoT. [20]

3.1.1.1 5G IoT use case evolution.

Οι υπηρεσίες IoT που παρέχονται σε διαφορετικούς τομείς, οι συσκευές IoT που χρησιμοποιούνται και οι επιθέσεις σε τέτοιες υπηρεσίες περιγράφονται περιληπτικά στη συνέχεια :

Δημόσια ασφάλεια: Υπηρεσίες όπως η παρακολούθηση και η διαχείριση έκτακτων αναγκών θα διαχειρίζονται από τις αρχές επιβολής του νόμου. Επομένως οι επιθέσεις σε κάμερες κλειστού κυκλώματος τηλεόρασης CCTV και ανιχνευτές ταχύτητας θα θέσουν σε κίνδυνο τη δημόσια ασφάλεια.

Ψηφιακή υγεία: Στις υπηρεσίες περιλαμβάνεται η προληπτική υγεία, περίθαλψη ασθενών, χειρουργική εξ αποστάσεως όπως και συνδεδεμένα νοσοκομεία και εργαζόμενοι στον τομέα της υγείας. Ο ασθενής θα έχει φορητές και έξυπνες συσκευές IoT, όπως ρολόι καρπού και αισθητήρα που θα παρακολουθεί τις παραμέτρους της υγείας του και θα τις στέλνει στο νοσοκομείο εάν χρειαστεί. Το πληροφοριακό σύστημα στο νοσοκομείο θα παρακολουθεί, θα βρίσκει προβλήματα υγείας σε πρώτο στάδιο και θα ειδοποιεί το νοσοκομείο για να κάνει τις επόμενες ενέργειες. Μια επίθεση σε τέτοιες συσκευές και υπηρεσίες θα μπορούσε να είναι η κλοπή πληροφοριών υγείας των ασθενών που παραβιάζουν το απόρρητο και τροποποίηση δεδομένων αισθητήρων που θα θέσουν σε κίνδυνο την υγεία του ασθενούς. Για παράδειγμα οι

δείκτες για έναν υγιή ασθενή μπορεί να αλλάξουν ως μη κανονικές παράμετροι ή και αντιστρόφως. [20]

Κινητικότητα: Οι υπηρεσίες θα προσφέρουν συνδεσιμότητα μεταξύ μέσων μεταφοράς, συμπεριλαμβανομένων συνδεδεμένων αυτοκινήτων, τρένων, πλοίων και αεροπλάνων. Τα αυτόνομα αυτοκίνητα ανήκουν επίσης σε αυτόν τον τομέα. Οι συσκευές IoT θα τοποθετηθούν σε οχήματα που θα αλληλοεπιδρούν με άλλα οχήματα και οι υπηρεσίες θα μειώσουν τα ατυχήματα. Μια επίθεση σε τέτοιες υπηρεσίες μπορεί να προκαλέσει καθυστερήσεις ή και αποτυχία μεταφοράς. Δηλαδή εάν οι εισβολείς εκμεταλλευτούν ένα από τα οχήματα ή την πλατφόρμα και δώσουν ψευδείς οδηγίες, αλλοιωμένες εντολές ή παράγουν παραπλανητικά προειδοποιητικά μηνύματα. Επιπλέων, εάν τα αυτοκίνητα βρίσκονται υπό τον έλεγχο ενός κακόβουλου εισβολέα, τότε αυτός μπορεί να κατασκοπεύσει τον ιδιοκτήτη του και το όχημα μπορεί επίσης να χρησιμοποιηθεί για παράνομες ενέργειες.

Βιομηχανικός κλάδος: Οι υπηρεσίες περιλαμβάνουν έξυπνη παραγωγή, γεωργία και κτίρια. Οι βιομηχανίες διαθέτουν πολύ αυτοματισμό και οι αισθητήρες χρησιμοποιούνται για την ενίσχυση της παραγωγής. Στην έξυπνη γεωργία, οι αισθητήρες μπορούν να χρησιμοποιηθούν για τη διάγνωση των επιπέδων του νερού, της υγρασίας, της ανάγκης για φυτοφάρμακα, των χρόνων συγκομιδής κ.λπ. Μια επίθεση σε αυτές τις υπηρεσίες θα επηρεάσει την παραγωγή τους.

Έξυπνο δίκτυο: Οι υπηρεσίες περιλαμβάνουν έξυπνο δίκτυο (smart grid), έξυπνη μέτρηση (smart metering), διαχείριση νερού και απορριμμάτων. Μια επίθεση στο έξυπνο δίκτυο μπορεί να επηρεάσει τη διανομή ηλεκτρικής ενέργειας και οι συγκεκριμένες περιοχές μπορεί να παρουσιάσουν διακοπές. Μια επίθεση στην έξυπνη μέτρηση επίσης μπορεί να έχει σημαντικό αντίκτυπο στα έσοδα και την εξυπηρέτηση πελατών, καθώς ένας εισβολέας μπορεί να θέσει σε κίνδυνο τον έξυπνο μετρητή για να πιστώσει λιγότερη ή υπερβολική κατανάλωση στους παρόχους ενέργειας.

Έξυπνες πόλεις: Οι υπηρεσίες περιλαμβάνουν έξυπνες υποδομές, κυκλοφορία, στάθμευση, διόδια, παρακολούθηση ποιότητας αέρα, τουρισμό, εικονική πραγματικότητα και διαφήμιση. Οι υπηρεσίες έξυπνης στάθμευσης θα βοηθήσουν τον οδηγό να βρει μια δωρεάν θέση στάθμευσης πιο κοντά και τα διόδια θα χρεώνουν

αυτόματα, με σάρωση πινακίδων αυτοκινήτου ή έξυπνους μηχανισμούς πληρωμής για παράδειγμα. Ο τουρισμός θα μπορέσει να βελτιωθεί μέσω της εικονικής πραγματικότητας (VR), η οποία θα βελτιώσει την εμπειρία των πελατών (customer experience). Μια επίθεση στην υποδομή των έξυπνων πόλεων μπορεί να έχει δυσάρεστες επιπτώσεις, καθώς τα διόδια δεν θα είναι λειτουργικά, η ποιότητα του αέρα δεν θα παρακολουθείται σωστά και τα τουριστικά έσοδα θα επηρεαστούν λόγω αποτυχίας της εικονικής πραγματικότητας και της σωστής διαφήμισης.

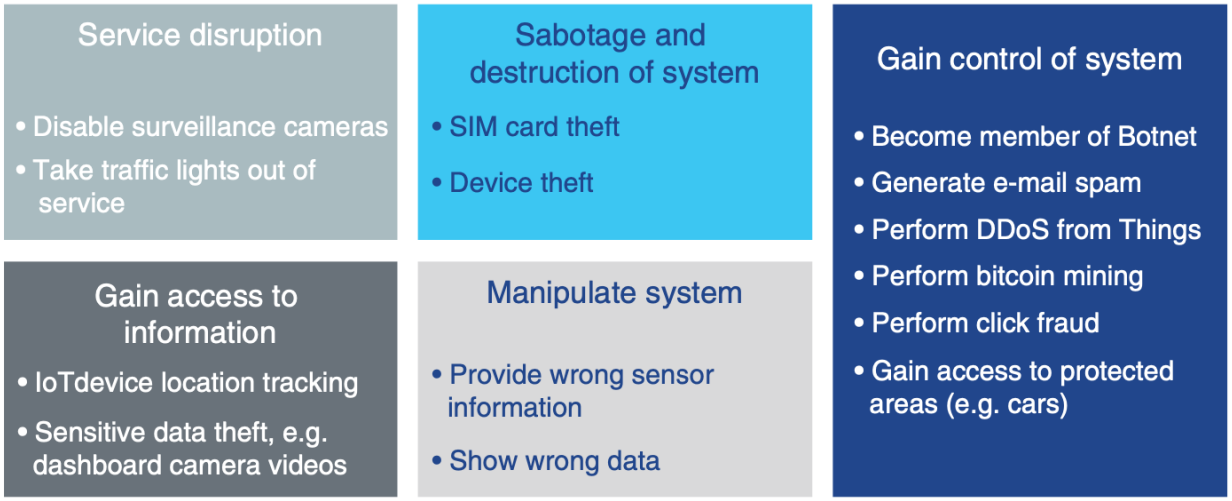
Έξυπνα σπίτια: οι υπηρεσίες περιλαμβάνουν έξυπνο καταναλωτή, φωτισμό, θερμοκρασία, μουσική και βίντεο. Οι συσκευές IoT θα αποτελούνται από διάφορους αισθητήρες και ηλεκτρικές συσκευές, όπως αισθητήρα θερμοκρασίας, αισθητήρα φωτιάς, αισθητήρα υγρασίας, ψυγείο, καφετιέρα, τοστιέρα κ.λπ. Οι συσκευές IoT θα αναφέρουν τη δραστηριότητά τους και θα μπορούν να διαμορφωθούν ως προς το πότε να εκτελούν μια ενέργεια όπως έναρξη, διακοπή, παραγγελία, ενημέρωση κατάστασης κ.λπ. Ένας εισβολέας μπορεί να εκμεταλλευτεί τις συσκευές IoT και να δώσει παραγγελίες, να τροποποιήσει τις λειτουργίες τους ή να εισαγάγει κακόβουλο κώδικα και να τις μετατρέψει σε συσκευές που μπορούν να λειτουργήσουν ως bot και να συμμετάσχουν στη διεξαγωγή μιας κατανεμημένης επίθεσης DoS (DDoS). [21]

Τομέας λιανικής: Οι υπηρεσίες στον τομέα της λιανικής είναι οι έξυπνες πληρωμές και τα έξυπνα καταστήματα. Τα καταστήματα θα είναι αυτοματοποιημένα και προσαρμοσμένα έτσι ώστε να καλύπτουν τη ζήτηση των πελατών με βάση την κατανάλωση και θα προσφέρουν έξυπνα συστήματα πληρωμών. Ο πιθανός στόχος για τον εισβολέα θα είναι τα έξυπνα συστήματα πληρωμών για να αποκομίσουν οικονομικά κέρδη. Η επίθεση στα έξυπνα καταστήματα θα επηρεάσει τη διαθεσιμότητα των προϊόντων, καθώς είτε δεν θα υπάρχουν προϊόντα είτε θα υπάρχουν περισσότερα προϊόντα από τη ζήτηση των πελατών.

Συμπερασματικά οι συσκευές IoT θα αναπτυχθούν τόσο σε εφαρμογές χαμηλής προτεραιότητας όσο και σε κρίσιμες εφαρμογές, όπως ο στρατός, οι υπηρεσίες έκτακτης ανάγκης, η εξ αποστάσεως χειρουργική στην υγειονομική περίθαλψη, τα αυτοκινούμενα οχήματα και πολλές άλλες. Οι συσκευές IoT μπορεί να βρίσκονται σε απομακρυσμένες περιοχές χωρίς ανθρώπινη επιτήρηση και μπορεί να κλαπούν για να τροποποιήσουν τις λειτουργίες τους ή να κλέψουν τις πληροφορίες τους για να μάθουν τα αδύναμα σημεία τους. Ο εισβολέας μπορεί να εκμεταλλευτεί ευπάθειες, να

εισαγάγει κακόβουλο κώδικα ή να κλέψει δεδομένα, τα οποία θα οδηγήσουν σε πλήρη ή μερική απώλεια υπηρεσιών ή εσόδων για τους τελικούς χρήστες ή τα δίκτυα. Εάν ένας εισβολέας κάνει πολλές συσκευές IoT ευάλωτες, μπορούν να χρησιμοποιηθούν για την εκκίνηση μιας επίθεσης DDoS, όπως η πρόσφατη επίθεση του botnet Mirai. Η ευαισθητοποίηση των χρηστών είναι ένα άλλο σημαντικό στοιχείο. Συνήθως οι default κωδικοί πρόσβασης δεν αλλάζουν και ο εισβολέας μπορεί εύκολα να εισέλθει σε συσκευές IoT με default κωδικούς πρόσβασης. Επομένως, οι συσκευές IoT πρέπει να διαθέτουν ισχυρούς μηχανισμούς αυθεντικοποίησης για την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Οι απειλές του IoT, όπως αναφέρεται στο ακόλουθο σχήμα, περιλαμβάνουν διακοπή υπηρεσίας, κλοπή πληροφοριών, κλοπή συσκευής, χειρισμό συστήματος και απόκτηση ελέγχου του συστήματος. Η υπηρεσία μπορεί να διακοπεί με την απενεργοποίηση συσκευών IoT ή την πραγματοποίηση επίθεσης DDoS στην υποδομή υπηρεσιών. Η απόσπαση και κλοπή πληροφοριών συμβαίνει μέσω ευάλωτων συσκευών IoT ή κλεμμένων συσκευών IoT. Εάν γίνει παραβίαση του συστήματος IoT, ενδέχεται να αποκαλυφθούν εσφαλμένες πληροφορίες αισθητήρα και δεδομένα. Εάν ένας εισβολέας αποκτήσει τον έλεγχο ενός συστήματος, οι συσκευές IoT που λειτουργούν σε αυτό το σύστημα ενδέχεται να γίνουν μέλη ενός botnet και να εκτελούν λειτουργίες όπως ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, να πραγματοποιήσουν επίθεση DDoS, εξόρυξη bitcoin, απάτη κλικ ή να αποκτήσουν πρόσβαση σε πληροφορίες και να εκδώσουν παραπλανητικές εντολές. [20]



Εικόνα 19: Πιθανές απειλές στο IoT. [20]

3.2 Απόρρητο χρήστη, ταυτότητα και εμπιστευτικότητα στο 5G.

Τα συστήματα 5G είναι η επόμενη σημαντική μετάβαση στις μελλοντικές κινητές επικοινωνίες. Η τεχνολογία 5G υπόσχεται να παρέχει υψηλότερο εύρος ζώνης και χαμηλότερο χρόνο απόκρισης. Σε αντίθεση με τις παραδοσιακές τεχνολογίες κινητής τηλεφωνίας, οι οποίες προορίζονται κυρίως για επικοινωνίες φωνής και δεδομένων, το 5G διασφαλίζει ότι παρέχει πολύ περισσότερα. Η τεχνολογία 5G έχει τη μεγάλη δυνατότητα να επιτρέψει υπηρεσίες για περιπτώσεις νέας χρήσης, για παράδειγμα, στην υγειονομική περίθαλψη, τις μεταφορές και τα έξυπνα σπίτια. Παρέχει ευκαιρίες στις εταιρείες να δημιουργήσουν νέα επιχειρηματικά μοντέλα για να προσφέρουν νέες υπηρεσίες στους καταναλωτές με πιο βελτιωμένους και αποτελεσματικούς τρόπους, καθώς και να αυξήσουν τα έσοδά τους. Αυτή η αύξηση των νέων επιχειρηματικών μοντέλων, της αρχιτεκτονικής και των τεχνολογικών αλλαγών στο 5G θα φέρει νέες προκλήσεις στο απόρρητο του χρήστη. Οι απαιτήσεις στο απόρρητο είναι ένα από τα κρίσιμα στοιχεία που πρέπει να ληφθούν υπόψη στη μελέτη της τεχνολογίας 5G, καθώς είναι υψίστης σημασίας η εξασφάλιση του απορρήτου των χρηστών σε σχέση με τις προσφερόμενες υπηρεσίες.

Τα συνεχώς εξελισσόμενα δίκτυα κινητής τηλεφωνίας εξετάζουν κυρίως τέσσερεις τομείς ασφάλειας, που είναι: ακεραιότητα, εμπιστευτικότητα, έλεγχος ταυτότητας και διαθεσιμότητα. Ωστόσο, οι απαιτήσεις απορρήτου δεν λαμβάνονται καθόλου υπόψη τόσο από την πλευρά των υποδομών όσο και από την αρχιτεκτονική. Καθώς το 5G θα

παράγει νέες και κρίσιμες εφαρμογές, είναι ζωτικής σημασίας να ληφθούν υπόψη τα χαρακτηριστικά απορρήτου από την άποψη της αρχιτεκτονικής, όπως η ανωνυμία και η μη σύνδεση. Αυτό θα εξασφαλίσει επίσης μια ισχυρότερη σχέση εμπιστοσύνης του καταναλωτή με τους παρόχους κινητής τηλεφωνίας και με τα τρίτα μέρη που παρέχουν τις διάφορες υπηρεσίες. [20]

Η τεχνολογία 5G προάγει το όραμα του «πάντα διαθέσιμου», όπου οι υπηρεσίες είναι διαθέσιμες στους χρήστες οποτεδήποτε και οπουδήποτε. Αυτή η συνδεσιμότητα 24/7 με άλλες συσκευές μπορεί να προκαλέσει μια σειρά από επιθέσεις όπως πλαστοπροσωπία, Άρνηση Υπηρεσιών (DoS) και επιθέσεις επανάληψης (replay attacks) μεταξύ άλλων. Η τεχνολογία 5G θεωρείται επίσης η βασική τεχνολογία για την παροχή απρόσκοπτης συνδεσιμότητας για έξυπνα αντικείμενα. Οι πρωτόγνωρες εμπειρίες, όπως οι υπηρεσίες με επίγνωση του περιβάλλοντος, η επαυξημένη πραγματικότητα και οι έννοιες του οτιδήποτε ως υπηρεσία και η εξατομίκευση των χρηστών θα είναι μια σημαντική ζωτική δύναμη πίσω από τη μαζική υιοθέτηση της τεχνολογίας 5G. Το 5G είναι επίσης ο κύριος μοχλός για εφαρμογές που βασίζονται στο Internet of Things (IoT), όπου τα πράγματα συνδέονται μέσω αυτής της τεχνολογίας και οι υπηρεσίες θα παρέχονται με πιο αποτελεσματικά και ταχύτερα μέσα. Αυτό σημαίνει ότι το 5G απαιτεί ιδιαίτερη προσοχή στις απαιτήσεις απορρήτου από διάφορες προοπτικές τεχνολογιών και υπηρεσιών.

Επιπλέον, λόγω των πρόσφατων εξελίξεων στις τεχνολογίες ανίχνευσης και επικοινωνίας, όπως smartphones, wearables, activity trackers, η γενική επίγνωση του απορρήτου στην σημερινή κοινωνία έχει αυξηθεί, και έτσι αυτό ενθαρρύνει την υψηλότερη προστασία των μεταδεδόμενων - metadata και των επικοινωνιών του χρήστη. Με το είδος των δυνατοτήτων που θα διαθέτει το 5G, αναμένεται ότι νέες περιπτώσεις χρήσης και εφαρμογές θα μπουν σε λειτουργία σε πραγματικό χρόνο. Στην περίπτωση του 5G, οι λύσεις που βασίζονται στην ασφάλεια και το απόρρητο πρέπει να αναθεωρηθούν από την αρχή. Επομένως, πρέπει να προσθέσει τα χαρακτηριστικά ασφάλειας και απορρήτου που είναι ενσωματωμένα στη σχεδίαση του συστήματος από την αρχή.

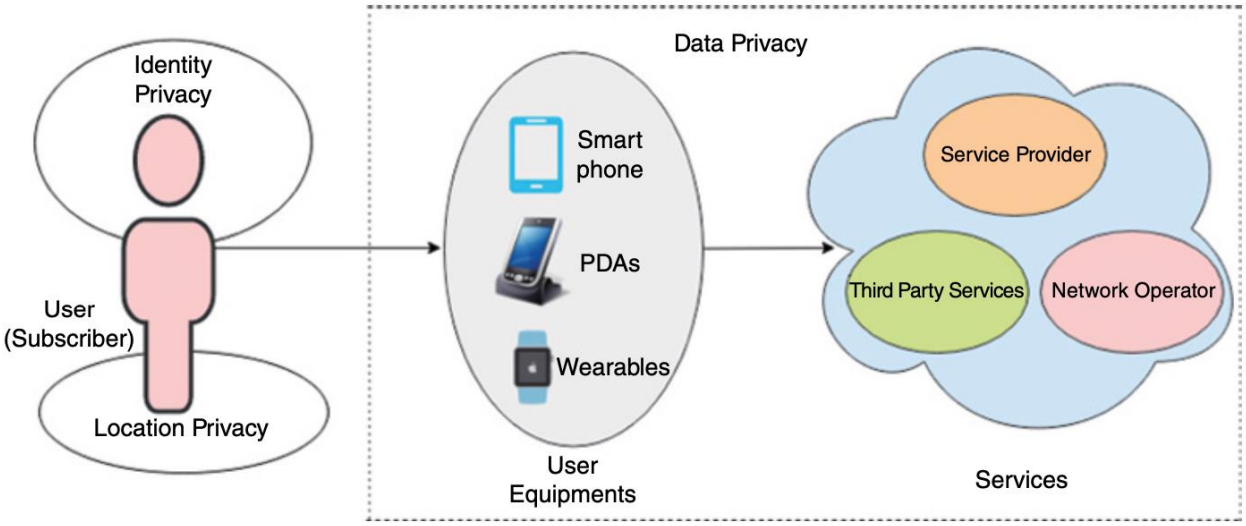
Οι συνεχείς βελτιώσεις στις τεχνολογίες κινητών επικοινωνιών απαιτούν επίσης βελτίωση των τεχνικών διαχείρισης ταυτότητας. Η τεχνολογία 5G θα φέρει μαζί έναν τεράστιο αριθμό νέων χρηστών και συσκευών και θα συνδέονται με real time τρόπο,

επομένως είναι ζωτικής σημασίας να προστατεύονται οι ταυτότητες των συνδρομητών καθώς και των συσκευών. Είναι σημαντικό να εξασφαλισθεί ότι κανένας αντίπαλος ή τρίτος δεν μπορεί να κλέψει την πραγματική ταυτότητα του συνδρομητή χωρίς τη συγκατάθεσή του. Παρόμοια είδη ασφαλών προσεγγίσεων απαιτούνται για την οικοδόμηση και τη διατήρηση της ισχυρής σχέσης εμπιστοσύνης μεταξύ των συνδρομητών και των διαφόρων ενδιαφερόμενων μερών, όπως ο πάροχος υπηρεσιών, οι επιχειρήσεις, ο ISP κ.λπ.[21]

3.2.1 Απόρρητο χρήστη στο 5G (5G User Privacy).

Η τεχνολογία πέμπτης γενιάς 5G θα επιτρέψει σε πολλές νέες εφαρμογές να ανοίξουν τις πόρτες τους για ένα μεγάλο αριθμό χρήσεων και εφαρμογών. Αυτό μας οδηγεί στο γεγονός ότι μεγάλος όγκος προσωπικών πληροφοριών θα διακινηθεί μέσω των δικτύων 5G. Με την εισαγωγή των τεχνικών εξόρυξης δεδομένων (data mining), είναι ευκολότερο να ανακτηθούν οι πληροφορίες απορρήτου δεδομένων και επομένως τα δεδομένα διατρέχουν μεγάλο κίνδυνο. Το σύστημα 5G θα πρέπει να παρέχει μηχανισμούς ασφαλείας για την προστασία μιας ποικιλίας αξιόπιστων πληροφοριών, τόσο για ανθρώπους όσο και για χειριστές μηχανών.

Η τεχνολογία 5G θα προσφέρει επίσης εξατομικευμένες υπηρεσίες δικτύου για τους καταναλωτές πραγματοποιώντας τα χαρακτηριστικά συγκεκριμένων υπηρεσιών. Έτσι, οι απαιτήσεις απορρήτου στο δίκτυο 5G ενδέχεται να διαφέρουν από υπηρεσία σε υπηρεσία. Η τεχνολογία 5G θα επιτρέψει επίσης απαιτήσεις απορρήτου προσανατολισμένες στις υπηρεσίες. Για παράδειγμα, οι πληροφορίες υγείας των χρηστών σε ορισμένες εφαρμογές υγειονομικής περίθαλψης θα απαιτούν υψηλότερο βαθμό απορρήτου. Επίσης, στην περίπτωση ορισμένων κρίσιμων βιομηχανικών εργασιών, απαιτείται εξίσου υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής. Ωστόσο, εφαρμογές όπως η αναζήτηση για κάποιο είδος πληροφοριών τοποθεσίας μπορεί να απαιτούν μικρότερο βαθμό απορρήτου. Για πιο εστιασμένη κατανόηση, χωρίσαμε τις έννοιες του απορρήτου των χρηστών σε τρία μέρη, που είναι: απόρρητο δεδομένων, τοποθεσίας και ταυτότητας, όπως φαίνεται στην κάτω εικόνα. [20]



Εικόνα 20: Various elements in user privacy. [20]

3.2.2 Ιδιωτικότητα δεδομένων (Data Privacy).

Υπάρχουν δεκάδες από έξυπνες και διαφορετικές συσκευές συνδεδεμένες μέσω της τεχνολογίας 5G και επομένως οι πιθανότητες διαρροής των προσωπικών δεδομένων του χρήστη είναι αρκετά υψηλές. Οι πάροχοι υπηρεσιών αποθηκεύουν και χρησιμοποιούν τα προσωπικά δεδομένα των πελατών τους χωρίς την άδειά τους. Σε ορισμένες περιπτώσεις, ο πάροχος υπηρεσιών αποθηκεύει τα δεδομένα χρήστη για το δικό του προϊόν και στη συνέχεια τα μοιράζεται με άλλες εταιρείες, ώστε να μπορούν να αναλύσουν τα δεδομένα και να βρουν κάποιες τάσεις, όπως για παράδειγμα ποιο από τα προϊόντα του είναι πιο κατάλληλο για τον συγκεκριμένο χρήστη. Σε ορισμένες περιπτώσεις, είναι ακόμη χρήσιμο να λαμβάνονται ορισμένα από τα προσωπικά δεδομένα του χρήστη και βάσει αυτών, η εταιρεία μπορεί να δημιουργήσει νέα προϊόντα και υπηρεσίες. Ωστόσο, οι πάροχοι υπηρεσιών πρέπει να παρέχουν μια σαφέστερη εξήγηση σχετικά με το σκοπό που έχουν χρησιμοποιηθεί τα δεδομένα τους. Πρέπει επίσης να απαντούν σε ερωτήσεις όπως ποια δεδομένα έχουν ληφθεί και πώς και πού τα έχουν αποθηκευμένα.

Αρκετά smart phone applications για παράδειγμα στο android, ζητούν ορισμένες πληροφορίες πριν την εγκατάσταση. Κυρίως, οι πληροφορίες για τις οποίες η εφαρμογή θέλει άδεια δεν έχουν άμεση σχέση με την υπηρεσία της συγκεκριμένης εφαρμογής. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν και για άλλους σκοπούς,

οι οποίοι δεν έχουν καθοριστεί από τους προγραμματιστές εφαρμογών. Στις μέρες μας, οι σελίδες μέσων κοινωνικής δικτύωσης είναι οι πιο συνηθισμένοι τρόποι κοινής χρήσης δημόσιων και ιδιωτικών πληροφοριών μεταξύ διαφόρων χρηστών. Αυτοί είναι οι συχνοί τρόποι ενημέρωσης άλλων σχετικά με τις τρέχουσες ενεργοποιήσεις σας, να μοιράζεστε ή να ανεβάζετε προσωπικές φωτογραφίες και ακόμη και να έχετε live συνομιλίες κειμένου, ήχου και βίντεο. Το 5G υποτίθεται ότι επιτρέπει αυτό το είδος επικοινωνίας απρόσκοπτα και συνεχώς.

Τα συστήματα IoT που βασίζονται στο 5G είναι το κρίσιμο μέρος των μελλοντικών τεχνολογιών για την παροχή πολυάριθμων ψηφιακών υπηρεσιών. Αυτό τελικά θα δημιουργήσει συνεχώς τεράστιες ποσότητες δεδομένων. Δεδομένου ότι το IoT γίνεται πανταχού παρόν, μεγάλος όγκος δεδομένων θα τεθεί σε δράση. Το 5G θα διασφαλίσει την αύξηση των ταχυτήτων μεταφοράς δεδομένων και έτσι θα έχει μεγαλύτερο κίνδυνο κακόβουλων επιθέσεων. Με παρόμοιο τρόπο, οι φορητές συσκευές παράγουν τεράστια ποσότητα δεδομένων, επειδή οι αισθητήρες που συνδέονται με τα wearables παρακολουθούν και συλλέγουν διαρκώς προσωπικές πληροφορίες του χρήστη όπως φυσική κατάσταση, συχνότητα σφυγμού, βάρος, ύψος κ.λπ. Αυτά τα δεδομένα μπορούν να αναλυθούν από τρίτα πρόσωπα, οι οποίοι μπορούν να εξάγουν άλλες δυνατότητες από αυτά χωρίς να ζητήσουν την άδεια του χρήστη.

Κίνδυνοι απορρήτου δεδομένων προκύπτουν όταν το τρίτο μέρος ή πάροχος υπηρεσιών ή οποιοσδήποτε κακόβουλος εισβολέας θέλει να αποκτήσει πρόσβαση στα προσωπικά δεδομένα του χρήστη χωρίς τη συγκατάθεσή του. Για παράδειγμα, παρακολουθώντας τις δραστηριότητες κάποιου που χρησιμοποιεί τα προσωπικά του δεδομένα, μπορεί κανείς εύκολα να προβλέψει την καθημερινή ρουτίνα του συγκεκριμένου καταναλωτή. Αυτό μπορεί να είναι επιβλαβές σε ορισμένες περιπτώσεις, γιατί αν κάποιος θέλει να παρακολουθήσει τις δραστηριότητες ενός ατόμου, μπορεί εύκολα να το κάνει.

Το άλλο κρίσιμο παράδειγμα μπορεί να είναι αυτό της υγειονομικής περίθαλψης, όπου τα ιατρικά δεδομένα είναι πολύ ευαίσθητα. Σε πολλές περιπτώσεις, ο ασθενής θέλει να περιορίσει ορισμένες συγκεκριμένες πληροφορίες σε συγκεκριμένα άτομα, όπως γιατρούς, συγκεκριμένα μέλη της οικογένειας ή φίλους. Ωστόσο, κακόβουλοι χρήστες ή μη εξουσιοδοτημένα άτομα ενδέχεται να έχουν πρόσβαση στις πληροφορίες και να τις χρησιμοποιήσουν για ανήθικους σκοπούς.

Στα δίκτυα 5G, σε πολλές περιπτώσεις, οι απαιτήσεις προστασίας της ιδιωτικής ζωής εξαρτώνται επίσης από τη χρήση της συγκεκριμένης τεχνολογίας πρόσβασης. Τα δεδομένα χρήστη θα μοιράζονται σε διάφορα δίκτυα πρόσβασης στο 5G και διαφορετικοί προμηθευτές θα παρέχουν τις λειτουργικές πληροφορίες για το δίκτυο. Ένα τρίτο μέρος χρησιμοποιώντας μεθοδολογίες εξόρυξης δεδομένων (data mining), μπορεί να αντλήσει προσωπικές πληροφορίες, αναλύοντας τα δεδομένα διασποράς του χρήστη, τα οποία μπορεί να είναι διαθέσιμα σε οποιοδήποτε μέρος του δικτύου. Λόγω του κινδύνου τέτοιων σεναρίων, απαιτούνται πιο αυστηρά συστήματα προστασίας της ιδιωτικής ζωής δεδομένων για δίκτυα 5G.

Είναι σημαντικό να διαμορφωθούν ισχυροί μηχανισμοί προστασίας δεδομένων ενώ συζητείται η τυποποίηση και η χάραξη πολιτικής για την τεχνολογία 5G. Οι πάροχοι υπηρεσιών πρέπει επίσης να εξηγήσουν τους τρόπους συλλογής δεδομένων και τη χρήση τους για διάφορες υπηρεσίες. Θα πρέπει να υπάρχει ισορροπία μεταξύ του απορρήτου των χρηστών και των δεδομένων που χρησιμοποιούνται από τους παρόχους υπηρεσιών, έτσι ώστε οι εταιρείες να μπορούν να δημιουργούν νέες και χρήσιμες εφαρμογές για τον χρήστη και ταυτόχρονα να μην επηρεάζεται το απόρρητο των χρηστών. Θα πρέπει να εμπλακούν μηχανισμοί ελέγχου, έτσι ώστε η παρακολούθηση κάθε δράσης από διάφορες οντότητες να είναι πιο εύκολη. Οι τεχνικές ελαχιστοποίησης δεδομένων θα πρέπει επίσης να λαμβάνουν υπόψη, έτσι ώστε οι πάροχοι υπηρεσιών ή τρίτα μέρη να περιορίζουν τα δεδομένα που συλλέγουν και διατηρούν και να τα διαγράφουν όταν δεν τα χρειάζονται πλέον. [20]

3.2.3 Απόρρητο τοποθεσίας (Location Privacy) .

Σήμερα, πολλές έξυπνες συσκευές, όπως smartphones, tablet και wearables, που διαθέτουν ισχυρές υπολογιστικές και αποθηκευτικές δυνατότητες μαζί με τεχνολογία εντοπισμού θέσης, μπορούν να ζητήσουν υπηρεσίες ανά πάσα στιγμή και οπουδήποτε. Οι Υπηρεσίες βάσει τοποθεσίας (Location Based Services) χρησιμοποιούνται ευρέως σε σχέση με την ανάπτυξη μελλοντικής ασύρματης τεχνολογίας. Με την εισαγωγή του 5G, το οποίο θα επιτρέπει την απρόσκοπτη και συνεχή διαθεσιμότητα των υπηρεσιών, η τοποθεσία του χρήστη παρακολουθείται επίσης συνεχώς σε τέτοιες περιπτώσεις. Προκειμένου να παρέχουν βελτιωμένες υπηρεσίες, διάφορες εταιρείες έχουν αρχίσει επίσης να παρακολουθούν την τρέχουσα

τοποθεσία του χρήστη. Από αυτές τις πληροφορίες, παρακολουθούν συνεχώς τις συνήθειες και τη ρουτίνα του χρήστη. Από τη μια πλευρά, αυτού του είδους η υπηρεσία παρακολούθησης βοηθά τις εταιρείες να βελτιώσουν τις υπηρεσίες τους και να δημιουργήσουν νέες φιλικές προς το χρήστη υπηρεσίες, αλλά από την άλλη πλευρά, προκαλεί σοβαρές ανησυχίες σχετικά με το απόρρητο των χρηστών.

Επίσης, πολλές διαδικτυακές εφαρμογές σε κινητές συσκευές απαιτούν πληροφορίες τοποθεσίας μαζί με τα προσωπικά τους στοιχεία. Σε ορισμένες περιπτώσεις, λαμβάνονται πληροφορίες τοποθεσίας του χρήστη, ανεξάρτητα από το αν πρόκειται να χρησιμοποιηθούν ή όχι. Αυτές οι διαδικτυακές εφαρμογές θέλουν όλο και περισσότερες πληροφορίες σε κάθε ένα από τα updates τους. Σήμερα, οι εφαρμογές κοινωνικών μέσων όπως το Facebook έχουν επίσης την επιλογή «check-in», όπου οι χρήστες μοιράζονται τις τρέχουσες τοποθεσίες τους. Αυτό θα προκαλεσει ανησυχίες σχετικά με την παρακολούθηση των κινήσεων των χρηστών παρατηρώντας συνεχώς τις πληροφορίες τοποθεσίας. Πρόσφατα, οι φορητές συσκευές χρησιμοποιούνται επίσης ενεργά για σκοπούς παρακολούθησης, όπως η παρακολούθηση παιδιών και κατοικίδιων ζώων. Αυτές οι φορητές συσκευές παρακολουθούν τον αντίστοιχο χρήστη κάθε δευτερόλεπτο και αυτό προκαλεί επίσης τεράστιες ανησυχίες για το απόρρητο.

Υπάρχουν λίγες διαθέσιμες τεχνικές για τη διατήρηση του απορρήτου της τοποθεσίας που μπορεί επίσης να είναι χρήσιμες στο πλαίσιο της προστασίας του απορρήτου τοποθεσίας σε εφαρμογές/τεχνολογία 5G. Οι συνήθεις μέθοδοι που χρησιμοποιούνται για την διαφύλαξη του απορρήτου της τοποθεσίας του χρήστη μπορεί να περιλαμβάνουν την ανωνυμία, την αλλαγή ψευδωνύμου και την παραποίηση της διαδρομής. Επίσης απαιτούνται ρυθμιστικές ενέργειες, ώστε να μπορούν να σχεδιαστούν ισχυροί κανόνες, κανονισμοί και νομοθεσία για τη σωστή χρήση του δικτύου. Οι τεχνικές που βασίζονται στην κρυπτογράφηση είναι μεταξύ άλλων διαθέσιμων τρόπων ο σημαντικότερος για την προστασία του απορρήτου της τοποθεσίας του χρήστη. Το μήνυμα κρυπτογραφείται από τον χρήστη πριν σταλεί στον τοπικό πάροχο (Local Base Station). Μόλις ληφθεί το μήνυμα από τον LBS, θα αποκρυπτογραφηθεί. Αυτή η προσέγγιση περιλαμβάνει σχετικά ισχυρότερη ανωνυμία, αλλά έχει υψηλό κόστος υπολογισμού και επικοινωνίας, το οποίο είναι ένα από τα μειονεκτήματα της χρήσης αυτής της προσέγγισης.

Οι λύσεις που βασίζονται στην ανωνυμία αποκρύπτουν την πραγματική ταυτότητα του χρήστη και την αντικαθιστούν με τυχαία ψευδώνυμα. Σε αυτήν την περίπτωση, χρησιμοποιείται ένα αξιόπιστο ενδιάμεσο λογισμικό για τη δημιουργία πλαστών πληροφοριών, το οποίο στη συνέχεια αποστέλλεται στον τοπικό πάροχο (Local Base Station) για συγκεκριμένη υπηρεσία τοποθεσίας. [20]

3.2.4 Απόρρητο ταυτότητας (Identity Privacy).

Κατά την απόκτηση και χρήση ψηφιακών υπηρεσιών σε ορισμένες περιπτώσεις, οι καταναλωτές δεν θέλουν να αποκαλύψουν την αρχική τους ταυτότητα σε άλλους χρήστες ή σε παρόχους υπηρεσιών. Για παράδειγμα, όταν ζητείται feedback στο διαδίκτυο ή δίνουν σχόλια στις ιστοσελίδες των εταιρειών, οι χρήστες προτιμούν να παραμένουν ανώνυμοι. Σε ορισμένες περιπτώσεις, οι χρήστες ενδέχεται να χρησιμοποιήσουν προσωρινές ή πλαστές ταυτότητες και να τις απορρίψουν όταν ολοκληρωθεί η απαιτούμενη εργασία. Η γνώση της μόνιμης ταυτότητας ενός χρήστη μπορεί να επιτρέψει σε έναν αντίπαλο να παρακολουθεί και να συγκεντρώνει ολοκληρωμένα προφίλ για άτομα. Η τάση της κλοπής διαδικτυακών ταυτοτήτων είναι πιο διαδεδομένη στις μέρες μας. Υπάρχουν πολυάριθμες διαδικτυακές εφαρμογές, όπως αγορές και τραπεζικές συναλλαγές, που απαιτούν διαδικτυακές πληρωμές με διάφορους τρόπους μέσω πιστωτικών καρτών. Αυτές οι πληροφορίες μπορεί να οδηγήσουν στην αποκάλυψη της πραγματικής ταυτότητας και μπορεί να προκαλέσουν πιθανούς κινδύνους για το απόρρητο του χρήστη. Συνήθως, προσεγγίσεις που βασίζονται στην ανωνυμία χρησιμοποιούνται για την απόκρυψη της πραγματικής ταυτότητας. Το απόρρητο ταυτότητας μπορεί περαιτέρω να χωριστεί σε απόρρητο ταυτότητας συνδρομητή και συσκευής:

Απόρρητο ταυτότητας συνδρομητή (Subscriber Identity Privacy): Σε αυτήν την περίπτωση, μπορεί να προκύψουν απειλές όταν οι χρήστες παρακολουθούνται από το αναγνωριστικό του συνδρομητή ή μέσω ενός προσωρινού αναγνωριστικού. Επίσης, οι χρήστες γενικά δεν επιθυμούν κανενός είδους σύνδεση μεταξύ της ταυτότητας του συνδρομητή τους και της ταυτότητας της συσκευής. Η πιθανή λύση για την προστασία του απορρήτου της ταυτότητας του συνδρομητή θα ήταν μέσω της κρυπτογράφησης του IMSI (International Mobile Subscriber Identity). Προκειμένου να διασφαλιστεί η αποσύνδεση του συνδρομητή και του αναγνωριστικού συσκευής, ένα

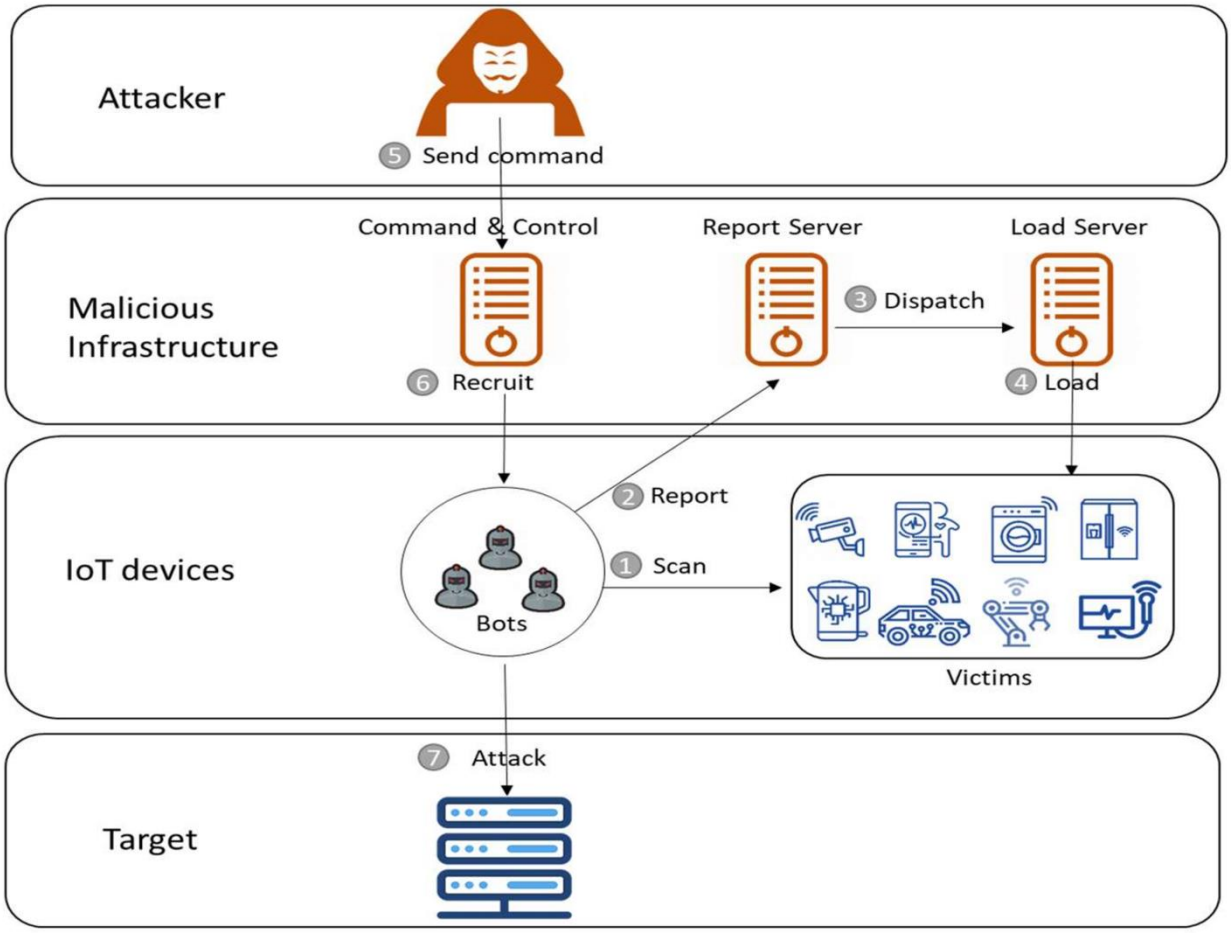
σύστημα ανωνυμοποίησης μπορεί να είναι μία από τις πιθανές προσεγγίσεις που πρέπει να ληφθούν υπόψη.

Απόρρητο ταυτότητας συσκευής (Device Identity Privacy): Τα ευπαθή σημεία που θα μπορούσαν να υπάρχουν σχετικά με το απόρρητο της ταυτότητας συσκευής είναι ότι οι συνδρομητές δεν επιθυμούν να παρακολουθούνται από τα αναγνωριστικά τους. Ομοίως, όπως και με το απόρρητο της ταυτότητας συνδρομητή, οι χρήστες δεν θέλουν επίσης σύνδεση μεταξύ των αναγνωριστικών των συνδρομητών τους με τα αναγνωριστικά συσκευής. Αυτό μπορεί να επιλυθεί μελετώντας τις πιθανές προσεγγίσεις κρυπτογράφησης και ανωνυμίας από άκρο σε άκρο που παρέχουν προστασία έναντι της μη εξουσιοδοτημένης παρακολούθησης συσκευών και διατηρούν την απόκρυψη της ταυτότητας της συσκευής. Το 5G διασφαλίζει επίσης ότι μόνο μέσω ενός εμπιστευτικού προστατευμένου μηνύματος, θα πρέπει να αποστέλλεται η Διεθνής Ταυτότητα Κινητού Εξοπλισμού (International Mobile Equipment Identity). [20]

3.3 Επιθέσεις DDoS σε 5G IoT δίκτυα και λύσεις προστασίας.

Οι εισβολείς μπορούν να εκμεταλλευτούν τις προκλήσεις των νέων τεχνολογιών του IoT και του 5G για κακόβουλους σκοπούς αφού θα συνδέσουν πολλές από τις συνήθειες της καθημερινής ανθρώπινης ζωής με τα δίκτυα επικοινωνιών και θα επιταχύνουν την ψηφιοποίηση του κόσμου. Σημαντικές θα είναι οι προκλήσεις στον τομέα της ασφάλειας. Τα δίκτυα κινητής τηλεφωνίας πάντα είχαν τα δικά τους προβλήματα από την πρώτη τους γενιά μέχρι και σήμερα. Όταν πρόκειται για την τεχνολογία του 5G που θα παρέχει νέες υπηρεσίες και θα είναι η κύρια πλατφόρμα επικοινωνίας για το IoT, οι προκλήσεις θα είναι πιο δύσκολες και πέρα από αυτές των προηγούμενων γενεών. Αρκετές συσκευές IoT έχουν αδυναμίες στο hardware, το software, το λειτουργικό σύστημα και το σχεδιασμό τους. Μία από τις πιο κοινές παραβιάσεις του εξοπλισμού IoT είναι ο σχηματισμός επιθέσεων Denial of Service (DoS) και Distributed Denial of Service (DDoS), οι οποίες συμβαίνουν με παραβιασμένο εξοπλισμό IoT. Οι επιθέσεις άρνησης υπηρεσίας διακόπτουν την πρόσβαση των εξουσιοδοτημένων χρηστών σε μια συγκεκριμένη υπηρεσία. Μια επίθεση DoS προέρχεται από μια πηγή που είναι συνήθως ένας server ή ένα σύστημα

υπολογιστή, αλλά στην επίθεση DDoS, οι πόροι είναι περισσότεροι από ένα σύστημα και μπορούν να είναι ακόμη και παγκόσμια διάσπαρτα και αποκεντρωμένα. [21]



Εικόνα 21: Sample IoT botnet network. [21]

Σαν επακόλουθο, η πιθανότητα να γίνει hack ή botnet μέσω rootkit ο εξοπλισμός του IoT γίνεται ολοένα και μεγαλύτερη κάθε μέρα. Τα ακόλουθα στοιχεία μπορούν να χαρακτηριστούν ότι έχουν τον μεγαλύτερο αντίκτυπο στην ευπάθεια του εξοπλισμού IoT:

- ***Κακός κωδικός πρόσβασης ή προεπιλεγμένος κωδικός πρόσβασης:*** ο περιορισμός του hardware στη μνήμη Ram και Rom μας οδηγεί στο να μην χρησιμοποιούνται μεγάλοι και πολύπλοκοι κωδικοί πρόσβασης σε αυτήν τη συσκευή.

- Προσαρμοσμένα λειτουργικά συστήματα: το λειτουργικό σύστημα είναι πρόχειρα σχεδιασμένο με περιορισμούς στις λειτουργίες και την παραμετροποίησή του ανάλογα με την ανάγκη και τη χρήση αυτού του εξοπλισμού.

- Κακή υποστήριξη: αρκετός από αυτόν τον εξοπλισμό δεν έχει πλήρη υποστήριξη, όπως έλλειψη παραγωγής, έλλειψη βασικών updates και αντικατάσταση με νέο εξοπλισμό.

- Έλλειψη κρυπτογράφησης ή αδύναμη κρυπτογράφηση: Λόγω της χρήσης φθηνού υλικού και περιορισμένων πόρων, δεν χρησιμοποιούνται ισχυρά κρυπτογραφικά πρωτόκολλα. [21]

3.4 Τρόποι επιθέσεων σε 5G enabled IOT συσκευές.

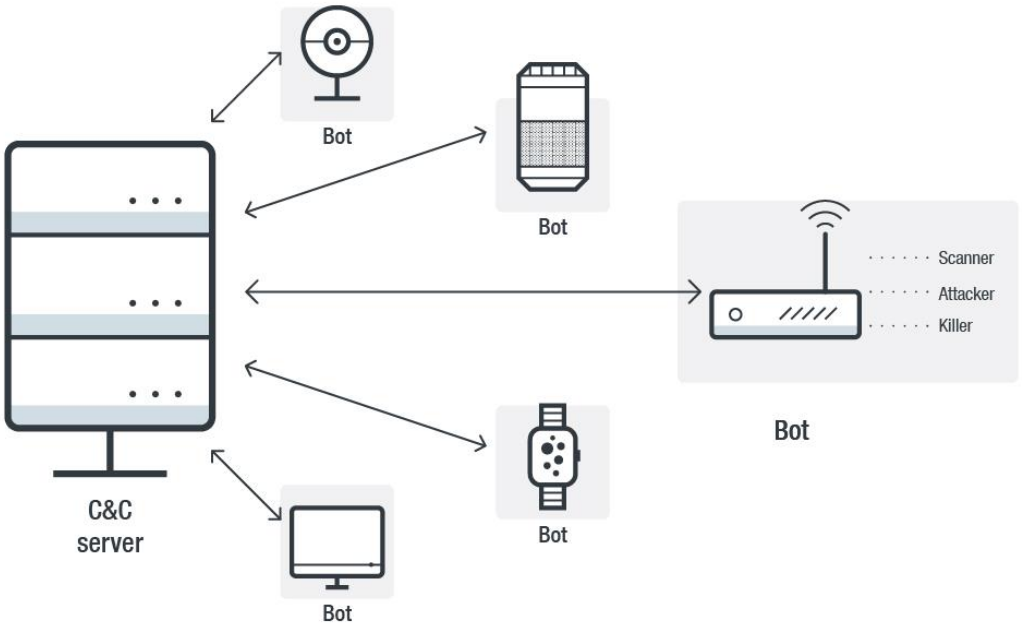
Ο μεγάλος αριθμός IoT συσκευών, η απομακρυσμένη προσβασιμότητα και η τεράστια γεωγραφική έκταση είναι παράγοντες που αθροίζονται στον αυξανόμενο αριθμό των μολυσμένων IoT συσκευών. Στο IoT, κάθε τύπος συσκευής μπορεί να μετατραπεί σε bot και να αξιοποιηθεί απομακρυσμένα.

Με βάση την απομακρυσμένη πρόσβαση, οι υπηρεσίες Telnet, SSH και Web είναι συνήθως ενεργές σε αυτές τις συσκευές IoT και αυτές οι υπηρεσίες προστατεύονται μόνο με όνομα χρήστη και κωδικό πρόσβασης, το οποίο έχει μειονεκτήματα και μπορεί εύκολα να παραβιαστεί. Επίσης, πολλές από αυτές τις συσκευές βρίσκονται επίσης στην άκρη ενός τοπικού ιδιωτικού δικτύου LAN. Σε περίπτωση εισβολής και υπό έλεγχο από τον hacker, ουσιαστικά το ιδιωτικό τοπικό δίκτυο έχει επίσης μολυνθεί και μπορεί να γίνει αντικείμενο εκμετάλλευσης.

Επίσης η δυνατότητα της κινητικότητας του εξοπλισμού IoT μπορεί να αξιοποιηθεί ακόμα πιο εύκολα σε επιθέσεις DDoS. Στην περίπτωση αυτή ο εισβολέας μπορεί εύκολα να αλλάξει τη γεωγραφική του θέση και να καθυστερήσει την αναγνώριση και ιχνηλάτηση της επίθεσης (forensics investigation). Βάσει αυτής της δυνατότητας, ένας εισβολέας μπορεί αντί να χρησιμοποιήσει έναν διακομιστή C&C (Command & Control Server) για τον έλεγχο του δικτύου botnet, να αναπτύξει έναν αριθμό Command & Control Servers που έχουν δυνατότητα κινητικότητας. Επίσης, αυτοί οι διακομιστές μπορούν να έχουν πολλές κάρτες δικτύου NIC, οι οποίες επιτρέπουν στον εισβολέα

να δημιουργήσει νέες συνδέσεις σε δίκτυα 4G και 5G. Ως αποτέλεσμα, ο εισβολέας μπορεί να χρησιμοποιήσει ένα δίκτυο κινητών C&C servers με μεγάλο αριθμό διευθύνσεων IP για τον έλεγχο του δικτύου του botnet. Έτσι, η φυσική τοποθεσία, καθώς και η διεύθυνση πηγής του Command & Control Server, θα ποικίλλουν.

Στο κάτω σχήμα, βλέπουμε ότι ένας hacker μπόρεσε να διεισδύσει στο δίκτυο IoT και κατέχει πολλά bots. Στη συνέχεια, σύμφωνα με εικονικά αιτήματα που μπορεί να περιλαμβάνουν κίνηση HTTP, TCP SYN, αίτημα DNS, αίτημα ICMP, αίτημα SIP (Session Initiation Protocol) και ούτω καθεξής, θα επιτεθεί στο θύμα και θα διακόψει την υπηρεσία. Αυτά τα bots μπορούν να βρίσκονται στο dark web market για διαφορετικούς σκοπούς με πολύ χαμηλές τιμές. [21]



Εικόνα 22: Επίθεση στο δίκτυο IoT από hacker που κατέχει πολλά bots. [21]

Σε αυτό το σενάριο, ο εισβολέας μπορεί επίσης να χρησιμοποιήσει ένα απομακρυσμένο πρόγραμμα για τον έλεγχο των C&C server του. Με αυτόν τον τρόπο, μπορεί να προγραμματίσει κάθε διακομιστή C&C για να ελέγχει το δίκτυο botnet του. Αυτή η μέθοδος μπορεί να είναι πολύ επικίνδυνη εάν ο εισβολέας τοποθετήσει τους

server του πίσω από ένα δίκτυο TOR (The Onion Router) και επίσης αποκρύψει τις διευθύνσεις IP των C&C server του. [21]

3.5 Λύσεις για την ασφάλεια σε 5G υποστηριζόμενο IOT.

Όσον αφορά τις λύσεις στην ασφάλεια, το ίδιο το 5G περιέχει κάποιους μηχανισμούς προστασίας της υποδομής του. Εισάγει την έννοια που ονομάζεται «Network Slicing», όπου το δίκτυο είναι τεμαχισμένο για γρήγορη αντιμετώπιση των επιθέσεων. Επίσης, παρέχει στοιχεία ελέγχου που δείχνουν ξεκάθαρα στους administrators του δικτύου πώς συμπεριφέρεται η εφαρμογή για να αναλάβει τον έλεγχο για την προστασία του δικτύου. Μερικές από τις λύσεις που προτείνονται για την προστασία του IoT περιβάλλοντος από μια επίθεση DDoS παρουσιάζονται παρακάτω.

Προσέγγιση Machine Learning (ML): *Η* προσέγγιση (ML) μπορεί να χρησιμοποιηθεί για τον εντοπισμό επιθέσεων. Για παράδειγμα, μια προσέγγιση παρακάμπτει τις επιθέσεις μέσω μιας αυτοματοποιημένης λύσης που είναι ενσωματωμένη στη λειτουργία Deep Packet Inspection (DPI) που εντοπίζει ακόμη και άγνωστες επιθέσεις τόσο στην εισερχόμενη όσο και στην εξερχόμενη κυκλοφορία. Αυτή η προσέγγιση δεν απαιτεί δημιουργία υποδομής υψηλού κόστους και είναι γρήγορη.

Ασφάλεια ως υπηρεσία (SaaS): Το SaaS (Security as a Service) είναι ένα είδος υπηρεσίας που παρέχεται από παρόχους cloud. Δίνει τη δυνατότητα στους παρόχους υπηρεσιών και στις επιχειρήσεις να προστατεύουν το δίκτυο από κυβερνοεπιθέσεις.

Encapsulation-aware Traffic Filtering μέθοδος: Αυτή η μέθοδος χρησιμοποιεί DPI (Deep Packet Inspection) και ενσωματώνει τον μηχανισμό φιλτραρίσματος με την αρχιτεκτονική ασφαλείας του 5G.

Automated Signature Extraction (ASE): Το ASE είναι ένα είδος λύσης με την οποία οι οργανισμοί μπορούν να αμυνθούν από επιθέσεις. Το χαρακτηριστικό ASE βοηθά στη μείωση του χρόνου απόκρισης για τον εντοπισμό κακόβουλου λογισμικού εξάγοντας δυναμικά υπογραφές άγνωστων virus και worms που διασχίζουν το δίκτυο χωρίς την ανάγκη ανθρώπινης παρέμβασης.

Κρυπτογραφικοί αλγόριθμοι: Αυτοί οι αλγόριθμοι είναι ικανοί να προστατεύουν δίκτυα IoT και είναι ταχύτεροι από τους αλγόριθμους παλαιού τύπου.

Ασφάλεια δρομολογητή: Οι συσκευές IoT δεν διαθέτουν λογισμικό ασφαλείας που εκτελείται σε αυτές. Ο δρομολογητής που συνδέει συσκευές μπορεί να δημιουργήσει έναν ενισχυμένο μηχανισμό ασφαλείας, καθώς είναι η πύλη που επιτρέπει στις συσκευές να επικοινωνούν μεταξύ τους στο Διαδίκτυο. Οι κατασκευαστές δρομολογητών ανησυχούν πολύ για την παραγωγή δρομολογητών με δυνατότητα ασφάλειας.

Διαχείριση συσκευών και ασφαλής εκκίνηση: Με την επαλήθευση της θέσης των συσκευών και της πλατφόρμας όπου χρησιμοποιούνται, η ασφάλεια του IoT μπορεί να βελτιωθεί.

Εξουσιοδότηση και Έλεγχος Πρόσβασης: Παρέχει έλεγχο πρόσβασης (access control) σε πόρους IoT συσκευών.

Ασφάλεια από άκρο σε άκρο εφαρμογής: Υλοποιείται στο επίπεδο εφαρμογής π.χ. end to end encryption ή 2FA (Two Factor Authentication). [22]

ΚΕΦΑΛΑΙΟ 4ο

4.1 Ταξινόμηση απειλών στο 5G.

Το 5G αποτελεί μεγάλη καινοτομία στα δίκτυα κινητής τηλεφωνίας ενσωματώνοντας πολλαπλούς και διαφορετικούς τύπους τεχνολογιών. Παρά τα σημαντικά οφέλη, οι κίνδυνοι και οι απειλές δεν έχουν ακόμη κατανοηθεί εντελώς. Η πολυπλοκότητα και η επέκταση της επιφάνειας επίθεσης καθιστά τη δραστηριότητα του ακριβούς προσδιορισμού του τοπίου απειλών 5G μια επίπονη εργασία. Οι απειλές στο 5G συνδυάζουν τις παραδοσιακές απειλές που βασίζονται σε IP δίκτυα με το δίκτυο 5G core, 5G access, 5G edge), τις μη ασφαλείς γενιές 2G, 3G, 4G παλαιού τύπου και τις απειλές που εισάγονται από την τεχνολογία virtualisation.

4.1.1 Ταξινομία των απειλών 5G κατά ENISA (ENISA Taxonomy of 5G threats).

Η παρακάτω λίστα παρουσιάζει μια λίστα υψηλού επιπέδου κατηγοριοποίησης απειλών με βάση την ταξινόμηση απειλών (κατά ENISA).

- **Παράνομη δραστηριότητα και κατάχρηση - Nefarious activity, abuse (NAA)**: Αυτή η κατηγορία απειλής ορίζεται ως «παράνομες ενέργειες που στοχεύουν συστήματα, υποδομές και δίκτυα υπολογιστών μέσω κακόβουλων επιθέσεων με σκοπό είτε την κλοπή, την αλλαγή ή την καταστροφή ενός συγκεκριμένου στόχου.
- **Υποκλοπή/Πειρατεία - Eavesdropping/Interception/ Hijacking (EIH)**: Αυτή η κατηγορία απειλής ορίζεται ως «ενέργειες που στοχεύουν στην ακρόαση, διακοπή ή κατάληψη του ελέγχου επικοινωνίας τρίτου μέρους χωρίς συναίνεση».
- **Φυσικές επιθέσεις - Physical attacks (PA)**: Αυτή η κατηγορία απειλής ορίζεται ως «ενέργειες που στοχεύουν να καταστρέψουν, να εκθέσουν, να τροποποιήσουν, να απενεργοποιήσουν, να κλέψουν ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε φυσικά περιουσιακά στοιχεία, όπως υποδομή, υλικό ή διασύνδεση».
- **Καταστροφή - Damage (DAM)**: Αυτή η απειλή ορίζεται ως ενέργειες που είναι σκόπιμες και στοχεύουν στην πρόκληση καταστροφής περιουσίας, βλάβης και καταλήγουν σε αστοχία ή μείωση της χρησιμότητας.

- **Ακούσια ζημιά - Unintentional Damage (UD)**: Αυτή η απειλή ορίζεται ως ενέργειες που είναι όμως ακούσιες και στοχεύουν στην πρόκληση καταστροφής περιουσίας, βλάβης και καταλήγουν σε αστοχία ή μείωση της χρησιμότητας.
- **Βλάβες και δυσλειτουργίες -Failures and malfunctions (FM)**: Αυτή η κατηγορία απειλής ορίζεται ως η ανεπαρκής λειτουργία ενός στοιχείου (υλικό ή λογισμικό).
- **Διακοπές - Outages (OUT)**: Αυτή η απειλή ορίζεται ως απρόσμενες διακοπές της υπηρεσίας ή μείωση της ποιότητας πέρα από ένα απαιτούμενο επίπεδο.
- **Καταστροφή - Disaster (DIS)**: Αυτή η απειλή ορίζεται ως ένα ξαφνικό ατύχημα ή μια φυσική καταστροφή που προκαλεί μεγάλη ζημιά ή καταστροφή υποδομών.
- **Νομικά - Legal (LEG)**: Αυτή η κατηγορία απειλής ορίζεται ως «νομικές ενέργειες τρίτων (συμβαλλόμενων ή μη), με σκοπό την απαγόρευση ενεργειών ή την αποζημίωση για απώλεια βάσει της ισχύουσας νομοθεσίας». [23]

Εικόνα 23: Κατηγορίες απειλών κατά ENISA. [23]

4.1.2 Κατηγορίες ενεργητικού στο 5G (5G Assets).

Στην παρούσα παράγραφο, παρουσιάζουμε τις διάφορες κατηγορίες περιουσιακών στοιχείων που χρησιμοποιούνται για τη δόμηση ενός δικτύου 5G, μαζί με μια χαρτογράφηση που δείχνει τον ρόλο αυτών των περιουσιακών στοιχείων για τη διατήρηση των ιδιοτήτων της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας (Confidentiality, Integrity, Availability).

Το διάγραμμα περιουσιακών στοιχείων είναι δομημένο χρησιμοποιώντας ομάδες στοιχείων σύμφωνα με την έκθεσή τους σε απειλές. Λαμβάνοντας υπόψη τον ρόλο των περιουσιακών στοιχείων στη διατήρηση των ιδιοτήτων εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας (γνωστές ως CIA), έχει αναπτυχθεί μια αρχική εκτίμηση της σημασίας τους. Με τον τρόπο αυτό, δόθηκε έμφαση στα περιουσιακά στοιχεία που είναι υπεύθυνα για τη διατήρηση της συνολικής ασφάλειας και διαθεσιμότητας της υποδομής 5G και που είναι γνωστοί στόχοι κυβερνοεπιθέσεων. [23]

Οι κατηγορίες περιουσιακών στοιχείων φαίνονται στο ακόλουθο σχήμα και το περιεχόμενό τους έχει ως εξής:

Εικόνα 24 : Στοιχεία ενεργητικού στο 5G. [23]

Στον παρακάτω πίνακα, παρουσιάζουμε τη σχέση των ομάδων περιουσιακών στοιχείων σε σχέση με τη CIA.

Πίνακας 4 : Τα περιουσιακά στοιχεία του 5G σε συνάρτηση με τη CIA. [23]

Asset Group	CIA Triad		
	Confidentiality	Integrity	Availability
Policy	🟡	🟡	🔵
Management processes	🟡	🟡	🟡
Business applications	🔴	🔴	🟡
Business services	🟡	🟡	🟡
Protocols	🔵	🔴	🟡
Data network	🔵	🔵	🟡
Slicing	🔵	🔵	🔴
Data	🔴	🔴	🔴
Human assets	🔴	🟡	🟡
Time	🟢	🟡	🔴
Legal	🔴	🔵	🟡
Legacy	🔴	🔴	🟡
Data storage/repository	🔴	🔴	🟡
Physical infrastructure	🟡	🔴	🔵
Management and orchestration (MANO)	🔴	🔴	🔴
Radio access network (RAN)	🟡	🔵	🟡
Network functions virtualisation (NFV)	🔴	🔴	🔴
Software defined networks (SDN)	🔴	🔴	🔴
Lawful Interception (LI)	🔴	🟡	🟢
Transport	🔵	🟡	🔴
Virtualisation	🔴	🔴	🔴
Cloud	🟡	🟡	🔵
Application programing interfaces (APIs)	🟡	🔴	🔴
Security controls	🔴	🔴	🟡

Very high relevance of asset group to maintain the property: 🔴
High relevance of asset group to maintain the property: 🟡
Medium relevance of asset group to maintain the property: 🔵
Low relevance of asset group to maintain the property: 🟢
Very low relevance of asset group to maintain the property: 🟢

4.1.3 Ταξινόμηση με βάση το στόχο εκμετάλλευσης.

Πέρα από την παραπάνω γενική ταξινόμηση, κατηγοριοποιούμε επίσης τις απειλές ανάλογα με το αν ο στόχος εκμετάλλευσης είναι μέρος του core network, της ραδιοπρόσβασης, του network virtualization ή της γενικής υποδομής. Με βάση αυτό το κριτήριο, οι απειλές μπορούν να κατηγοριοποιηθούν περαιτέρω σε:

4.1.3.1 Απειλές βασικού δικτύου (Core network threats).

Αυτές οι απειλές σχετίζονται με στοιχεία του βασικού δικτύου που περιλαμβάνει SDN, NFV, NS και MANO. Η πλειοψηφία τους εμπίπτει στις κατηγορίες Nefarious activity/abuse (NAA) και Eavesdropping/ Interception/ Hijacking (EIH).

Κατάχρηση της απομακρυσμένης πρόσβασης : Αυτή η απειλή αποτελείται από ένα κακόβουλο άτομο που έχει απομακρυσμένη πρόσβαση σε κρίσιμες υποδομές δικτύου και αναλαμβάνει τον έλεγχο μιας virtual machine για να εκτελέσει άλλους τύπους επιθέσεων. Αποκτώντας παράνομη πρόσβαση στη λειτουργία απομακρυσμένης πρόσβασης, ένας κακόβουλος χρήστης μπορεί να συνδεθεί με λειτουργικά συστήματα και applications, σε έναν σημαντικό τομέα του δικτύου. Με απομακρυσμένη πρόσβαση σε ένα δίκτυο, ένας κακόβουλος χρήστης μπορεί να συμμετάσχει σε άλλες δραστηριότητες, όπως η παραβίαση ρυθμίσεων διαμόρφωσης (system configuration) και η διανομή malware.

Αυξήσεις στον έλεγχο ταυτότητας **:** Αυτή η απειλή σχετίζεται με έναν τεράστιο αριθμό αιτημάτων ελέγχου ταυτότητας που αποστέλλονται από έναν κακόβουλο χρήστη σε μικρό χρονικό διάστημα. Ένας κακόβουλος χρήστης εκκινεί πολλά traffic requests ή ακόμα και παρακολουθεί τις αυξήσεις της κυκλοφορίας με συσκευές IoT. Κατά συνέπεια, το δίκτυο θα αντιμετωπίσει περισσότερα αιτήματα σήματος και ελέγχου ταυτότητας που δεν είναι ικανά να χειριστούν. Αυτό το είδος επίθεσης μπορεί να θεωρηθεί ως ειδική περίπτωση άρνησης υπηρεσίας. Επομένως ο έλεγχος ταυτότητας των εξουσιοδοτημένων συσκευών μπορεί να αποτύχει με αποτέλεσμα την διακοπή της συνδεσιμότητας.[23]

Κατάχρηση λειτουργιών δικτύου που φιλοξενούνται από τρίτους : Αυτή η απειλή σχετίζεται με ζητήματα διαθεσιμότητας και αποκάλυψη ευαίσθητων δεδομένων λόγω

βασικών λειτουργιών δικτύου που φιλοξενούνται σε συστήματα τρίτων παρόχων υπηρεσιών cloud. Ένας αναξιόπιστος πάροχος υπηρεσιών cloud θα μπορούσε να έχει πρόσβαση, να διακόπτει και να τροποποιεί την κυκλοφορία του χρήστη που διέρχεται από τις εγκαταστάσεις του για λογαριασμό του Διαχειριστή του Δικτύου Κινητής Τηλεφωνίας.

Κατάχρηση δεδομένων ελέγχου ταυτότητας και εξουσιοδότησης χρήστη: Αυτή η απειλή σχετίζεται με την αποκάλυψη μακροπρόθεσμων κλειδιών για έλεγχο ταυτότητας και ασφάλειας που διεξάγονται από εχθρικό ή αναξιόπιστο προσωπικό που λειτουργεί στο βασικό δίκτυο κορμού.

Εκμετάλλευση διεπαφής προγραμματισμού εφαρμογών (API): Αυτή η απειλή περιλαμβάνει την εκμετάλλευση διεπαφών προγραμματισμού εφαρμογών (API) για την εκτόξευση διαφορετικών τύπων επιθέσεων. Μεγάλο μέρος της δυνατότητας προγραμματισμού που προσφέρει η νέα αρχιτεκτονική δικτύου 5G βασίζεται στην εκτεταμένη χρήση των API (Application Programming Interface). Η εκμετάλλευση μπορεί να στοχεύει διαφορετικούς τύπους API όπως ονοματολογίας, εσωτερικών λειτουργιών δικτύου, διεπαφών περιαγωγής κ.λπ. που εκτίθενται σε διαφορετικά επίπεδα του δικτύου. Ένα κακώς σχεδιασμένο ή διαμορφωμένο API με ανακριβείς κανόνες ελέγχου πρόσβασης μπορεί να εκθέσει και να προσβάλλει βασικές λειτουργίες δικτύου και ευαίσθητες παραμέτρους. Η απειλή ύπαρξης ενός μικρού εκτεθειμένου σε κίνδυνο API στον πυρήνα του 5G μπορεί να θέσει ολόκληρο το δίκτυο σε κίνδυνο.

Εκμετάλλευση κακώς σχεδιασμένης αρχιτεκτονικής σε δίκτυο, υπηρεσίες και ασφάλεια: Αυτή η απειλή σχετίζεται με ζητήματα που προκύπτουν από τις πολλαπλές επιλογές τεχνολογίας και τα χαρακτηριστικά που έχει να προσφέρει η τεχνολογία 5G από την αρχική της μορφή έως την υλοποίηση. Το επίπεδο πολυπλοκότητας και η δυσκολία επίτευξης βέλτιστης αρχιτεκτονικής όπως και επαρκούς ασφάλειας, μπορεί να οδηγήσουν σε κακή σχεδίαση και εφαρμογή. Τα ελαττώματα στον σχεδιασμό είναι ευκαιρίες για εκμετάλλευση σε αδυναμίες. Γνωρίζοντας ότι ένα συγκεκριμένο χαρακτηριστικό που δεν προστατεύεται επαρκώς ή δεν εφαρμόζεται, τότε ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί την αδυναμία και να εισάγει κακόβουλο λογισμικό στο κεντρικό δίκτυο.

Εκμετάλλευση κακώς διαμορφωμένων συστημάτων και δικτύων: Συχνά η εκμετάλλευση συστημάτων με εσφαλμένες ρυθμίσεις παραμέτρων ή κακών διαμορφώσεων χαρακτηρίζεται ως απειλή. Η εκμετάλλευση ενός κενού ασφαλείας συστήματος, δημιουργεί την ευκαιρία σε έναν επιτιθέμενο να φτάσει σε σημαντικά στοιχεία του δικτύου και να πραγματοποιήσει μια επίθεση. Λάθη διαμόρφωσης μπορεί να συμβούν σε διαφορετικά στάδια του κύκλου ζωής της εφαρμογής, όπως η εγκατάσταση και η συντήρηση του προϊόντος. Παραδείγματα περιλαμβάνουν κακώς διαμορφωμένα API, λειτουργίες δικτύου, κανόνες access control, τμήματα δικτύου, δικαιώματα διαχείρισης, εικονικά περιβάλλοντα, απομόνωση κυκλοφορίας, λογισμικό ενορχήστρωσης, firewalls κ.λπ.

Εσφαλμένη διαχείριση του δικτύου, των συστημάτων και των συσκευών: Εδώ τα σφάλματα που προκύπτουν από κακή συντήρηση και διαχείριση του δικτύου ενδέχεται να θέσουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του δικτύου. Ένα παράδειγμα ενεργειών που σχετίζονται με ένα σύστημα με κακή διαχείριση περιλαμβάνει την έλλειψη και παράλειψη λειτουργικών διαδικασιών που θα μπορούσαν να εκθέσουν το δίκτυο σε επιθέσεις. [23]

Σενάρια απάτης που σχετίζονται με διασυνδέσεις περιαγωγής: Σε ένα σενάριο περιαγωγής, το δίκτυο που επισκέπτεται πρέπει να αποκτήσει διανύσματα ελέγχου ταυτότητας από το οικιακό δίκτυο του χρήστη, τα οποία θα μπορούσαν να πιστοποιήσουν καταχρηστικά τον χρήστη, δίνοντάς του έτσι πρόσβαση στην εξυπηρέτηση πόρων χειριστή δικτύου κινητής τηλεφωνίας.

Memory scraping: Αυτός ο τύπος απειλής έχει εντοπιστεί κυρίως για διακομιστές εφαρμογών SDN. Αυτή η απειλή προκύπτει όταν ένας εισβολέας σαρώνει τη φυσική μνήμη RAM ενός μηχανήματος προκειμένου να εξαγάγει ευαίσθητες πληροφορίες που δεν είναι εξουσιοδοτημένος να έχει. Βέβαια το memory scraping μπορεί να επηρεάσει στοιχεία οποιουδήποτε επιπέδου του δικτύου. Στην απειλή memory scraping μπορεί να γίνει απόρριψη ενός SDN controller ως αποτέλεσμα κακόβουλου λογισμικού, για την εκμετάλλευση ιδιωτικών δεδομένων. Επιπλέον, η επαναδιαμόρφωση του SDN μπορεί να απαιτεί επανεκκινήσεις που θα μπορούσε να χρησιμοποιήσει ένας εισβολέας για να επιτεθεί στη διαδικασία του boot. Μόλις εκτελεστεί επιτυχώς, το memory scraping μπορεί να χρησιμοποιηθεί για την εξαγωγή ευαίσθητων δεδομένων SDN (π.χ. κανόνες ροών στο API).

Χειρισμός κυκλοφορίας δικτύου, αναγνώριση δικτύου και συλλογή πληροφοριών: Η απειλή περιλαμβάνει την τροποποίηση ή παραποίηση δεδομένων κατά τη μεταφορά μηνυμάτων, την τοποθέτηση αθέμιτων δεδομένων στο δίκτυο, είτε με την αναπαραγωγή προηγούμενων μηνυμάτων είτε με τη πλαστογραφία νέων μηνυμάτων, τη χρήση αιχμών κυκλοφορίας και αλλαγή δρομολόγησης ή τροποποίηση των προτεραιοτήτων ροής.[23]

Χειρισμός δεδομένων διαμόρφωσης δικτύου: Ανεπαρκείς χειρισμοί στη διαχείριση και προστασία των ρυθμίσεων διαμόρφωσης μπορεί να οδηγήσουν σε απρόβλεπτη συμπεριφορά του συστήματος και μη εξουσιοδοτημένη πρόσβαση στις υπολογιστικές υποδομές, με αντίκτυπο στην εμπιστευτικότητα και την ακεραιότητα του δικτύου. Αυτή η απειλή συνεπάγεται την παραβίαση ενός βασικού στοιχείου δικτύου (π.χ. ελεγκτής SDN, λειτουργία δικτύου, λειτουργία διαχείρισης και ενορχήστρωσης) με τη δημιουργία προϋποθέσεων για την εκτόξευση άλλων επιθέσεων (π.χ. DoS). Αυτή η απειλή αναφέρεται συγκεκριμένα σε δεδομένα διαμόρφωσης επιπέδου ελέγχου (control level). Συνήθη παραδείγματα χειρισμού δεδομένων διαμόρφωσης παρατίθενται παρακάτω.

- *Χειρισμός πινάκων δρομολόγησης (routing tables manipulation)*

- *Παραποίηση δεδομένων διαμόρφωσης (falsification of configuration data)*

- *Χειρισμός DNS (DNS manipulation)*

Κακόβουλη πλημμύρα (flooding) βασικών στοιχείων δικτύου: Αυτή η απειλή περιλαμβάνει την πλημμύρα ενός υπολογιστικού συστήματος δικτύου με πολλά αιτήματα ή μεγάλη επισκεψιμότητα, που θέτει σε κίνδυνο τη διαθεσιμότητά του. Μπορεί να προκύψει πλημμύρα κατά τη μετάδοση δεδομένων, εξαντλώντας τους πόρους των εξαρτημάτων και οδηγώντας σε μείωση ή πλήρη τερματισμό της υπηρεσίας που παρέχεται από το εξάρτημα.

Οι επιθέσεις κορεσμού πόρων και πλημμύρας λαμβάνουν χώρα σε συγκεκριμένα στοιχεία SDN όπου μια μικρή ροή requests από έναν πλαστό αποστολέα προκαλεί μια τεράστια πλημμύρα από reply. Ενώ η προστασία από τέτοιες επιθέσεις έχει μελετηθεί για πολλά γνωστά πρωτόκολλα δικτύου, η έκθεση των λειτουργιών δικτύου NFV (Network Function Virtualization) από ελεγκτές SDN παρουσιάζει ένα νέο τοπίο απειλών.[23]

Οι επιθέσεις πλημμύρας (flooding attacks) μπορεί να έχουν τη γεύση των κατανεμημένων επιθέσεων DoS, όπου ένας τεράστιος αριθμός πηγών μπορεί να ενορχηστρωθεί για να δημιουργήσει πλημμύρες μηνυμάτων. Αυτές οι πηγές θα μπορούσαν, για παράδειγμα, να είναι τα μέλη ενός botnet, π.χ. μια συλλογή συσκευών που έχουν μολυνθεί με κακόβουλο λογισμικό σε σημείο που μπορούν όλες να ελεγχθούν από έναν εισβολέα για την εκτέλεση της επίθεσης. Οι επιθέσεις πλημμύρας μπορεί να επηρεάσουν όλα τα είδη διεπαφών που παρέχει ένα δίκτυο 5G, όπως της διεπαφής ραδιοπρόσβασης, το διαδίκτυο ή και άλλα δίκτυα κινητής τηλεφωνίας.

Κακόβουλη εκτροπή της ροής κυκλοφορίας: Η απειλή αυτή έχει να κάνει με την παραβίαση του δικτύου για την εκτροπή της ροής κυκλοφορίας και για να επιτραπεί σε έναν κακόβουλο χρήστη να παρακολουθεί την κυκλοφορία του δικτύου. Σχετίζεται με στοιχεία δικτύου του επιπέδου δεδομένων. Ένα συγκεκριμένο είδος εκτροπής κυκλοφορίας που συνηθίζεται σε εικονικά δίκτυα είναι η παραβίαση τμημάτων δικτύου. Αυτή η απειλή μπορεί να προκύψει όταν η υποχρεωτική απομόνωση μεταξύ κομματιών γίνεται σε οποιονδήποτε ενεργό κόμβο ή όταν η πρόσβαση σε ένα τμήμα του υπολογιστικού εξοπλισμού είτε παρακαμφθεί είτε διαμορφωθεί εσφαλμένα.

Εκμετάλλευση του ενορχηστρωτή πόρων δικτύου: Η απειλή εξετάζει τον χειρισμό της διαμόρφωσης ενορχηστρωτή πόρων δικτύου για την εκτέλεση μιας επίθεσης. Περιλαμβάνει την αλλαγή μιας συμπεριφοράς λειτουργίας δικτύου τροποποιώντας τις ρυθμίσεις στον ενορχηστρωτή και κατά συνέπεια θέτοντας σε κίνδυνο τον διαχωρισμό μεταξύ των λειτουργιών του δικτύου.

Ευκαιριακές και παράνομες χρήσεις κοινόχρηστων πόρων: Η απειλή αυτή σχετίζεται με μη εξουσιοδοτημένη πρόσβαση και τροποποίηση σημαντικών δεδομένων των συσκευών 5G. Τα κλειδιά κρυπτογράφησης ενδέχεται να κλαπούν από άκρο σε άκρο ή να διαρρεύσουν από τους κεντρικούς διακομιστές κλειδιών. Επομένως, η ασφαλής επικοινωνία από άκρο σε άκρο είναι ευάλωτη σε διαφορετικές επιθέσεις και οι αντίπαλοι αποκτούν πρόσβαση στα τελικά κρίσιμα σημεία. Βασική αιτία είναι η διαρροή των στοιχείων ελέγχου ταυτότητας, εξουσιοδότησης και λογιστικής (authentication, authorization, accounting- AAA) από τους εργαζομένους της εταιρίας παρόχου κινητής τηλεφωνίας.

Side-channel attacks: Οι Side-channel attacks είναι μια απειλή που σχετίζεται με στοιχεία δικτύου του επιπέδου δεδομένων. Η απειλή αυτή περιλαμβάνει την εξαγωγή πληροφοριών σχετικά με υπάρχοντες κανόνες ροής στο SDN που χρησιμοποιούνται από μέρη του δικτύου. Η απειλή μπορεί να πραγματοποιηθεί με την εκμετάλλευση εξ ορισμού προτύπων λειτουργιών δικτύου (π.χ. εκμετάλλευση της χρονικής διάρκειας που απαιτείται για τη δημιουργία μιας σύνδεσης στο δίκτυο).

Καταχώρηση κακόβουλων λειτουργιών δικτύου: Η απειλή αυτή ταξινομείται ως κακόβουλες δραστηριότητες ή κατάχρηση περιουσιακών στοιχείων. Μια μη εξουσιοδοτημένη ρύθμιση στο δίκτυο που ενσωματώνει έναν Trojan ιό, - που εισάγεται από έναν εσωτερικό χρήστη ή έναν πάροχο υπηρεσιών - θα μπορούσε να εγκατασταθεί κρυφά στην αρχιτεκτονική βάσης υπηρεσιών και να καταχωρηθεί στον πυρήνα δικτύου μέσω NRF (Network repository function), προκειμένου να εκτεθούν άλλα κακόβουλα API. Με την εγκατάσταση ή την ενεργοποίηση μιας μη εξουσιοδοτημένης λειτουργίας δικτύου, ένας κακόβουλος χρήστης μπορεί να έχει πρόσβαση σε ευαίσθητα στοιχεία του δικτύου για να εκτελέσει άλλου τύπου επιθέσεις όπως DoS, διανομή κακόβουλου λογισμικού, κλοπή ευαίσθητων πληροφοριών κ.λπ.

Traffic sniffing: Το sniffing ή αλλιώς παρακολούθηση- υποκλοπή, είναι μια δημοφιλής μέθοδος που χρησιμοποιείται από κακόβουλους παράγοντες για τη λήψη και ανάλυση πληροφοριών επικοινωνίας δικτύου. Με το sniffing, ένας κακόβουλος χρήστης μπορεί επίσης να κρυφακούει δεδομένα από το δικτύου και να κλέβει πολύτιμες πληροφορίες. Το sniffing μπορεί να συμβεί οπουδήποτε υπάρχει συνεχής κίνηση ροών δικτύου. Στο SDN, για παράδειγμα, ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί τις μη κρυπτογραφημένες επικοινωνίες για να υποκλέψει κίνηση από και προς έναν κεντρικό controller. Τα δεδομένα που συλλέγονται θα μπορούσαν να περιλαμβάνουν σημαντικές πληροφορίες για τις ροές ή την κίνηση που επιτρέπεται στο δίκτυο. [23]

4.1.3.2 Απειλές πρόσβασης δικτύου (Access network threats).

Κατάχρηση πόρων φάσματος (Abuse of spectrum resources): Η παράνομη χρήση αυτών των πόρων, λόγω της δυναμικής κατανομής/ανακατανομής αυτών, μπορεί να επιτρέψει την κατάληψη συγκεκριμένης ζώνης αδρανούς φάσματος μιμούμενος τα χαρακτηριστικά μιας μονάδας με νόμιμη άδεια χρήσης και

προκαλώντας παρεμβολές στις ραδιοσυχνότητες. Η παράνομη κατάληψη του φάσματος συχνοτήτων μπορεί επίσης να προκαλέσει σε έναν κόμβο δικτύου την απόρριψη πόρων φάσματος που ζητούνται από μονάδες χωρίς εξουσιοδότηση - λόγω της προφανούς έλλειψης πόρων σε διαθεσιμότητα - αποκλείοντας έτσι κάποιον έξω από το δίκτυο.

Ψεύτικη πρόσβασης σε κόμβο δικτύου (Fake access network node): Αυτή η απειλή θεωρεί την αποδοχή ενός μεταμφιεσμένου σταθμού βάσης ως νόμιμο, διευκολύνοντας διαφορετικούς τύπους επιθέσεων όπως MITM ή η χειραγώγηση της κυκλοφορίας του δικτύου. Η απειλή εξετάζει την παραβίαση της επικοινωνίας μεταξύ του εξοπλισμού κινητού χρήστη και του δικτύου για την έναρξη άλλων κακόβουλων ενεργειών.

Επίθεση πλημμύρας (Flooding attack): Η απειλή αυτή περιλαμβάνει πλημμύρες ραδιο-επαφών με πολλαπλά αιτήματα. Η πλημμύρα συμβαίνει μέσω της μετάδοσης δεδομένων που μπορεί να εξαντλήσουν τους πόρους των εξαρτημάτων και να οδηγήσουν σε μείωση ή πλήρη διακοπή της ραδιοσυχνότητας που παρέχεται από το εξάρτημα.

Address Resolution Protocol (ARP) poisoning: Αυτό το είδος επίθεσης ονομάζεται αλλιώς και ARP cache spoofing και είναι μια τεχνική με την οποία ένας εισβολέας στέλνει πλαστά μηνύματα ARP στο δίκτυο. Ο στόχος είναι να συσχετιστεί η διεύθυνση MAC του εισβολέα με τη διεύθυνση IP ενός άλλου υπολογιστή, όπως η προεπιλεγμένη πύλη (default gateway), προκαλώντας την αποστολή οποιασδήποτε κίνησης που προορίζεται για αυτήν τη διεύθυνση IP, στον εισβολέα.

Επιθέσεις σύλληψης IMSI (IMSI catching attacks): Αυτή η απειλή σχετίζεται με πρωτόκολλα σελιδοποίησης κινητής τηλεφωνίας που μπορεί να εκμεταλλευτεί ένας κακόβουλος χρήστης στην περιοχή του θύματος για να συσχετίσει την ταυτότητα του θύματος (π.χ. αριθμό τηλεφώνου) με την περίσταση σελιδοποίησης του. Μέσω μιας επίθεσης που ονομάζεται «$mathsf{ToRPEDO}$», ένας κακόβουλος χρήστης μπορεί να επαληθεύσει τις πληροφορίες τοποθεσίας ενός θύματος, να εισάγει κατασκευασμένα μηνύματα σελιδοποίησης και να πραγματοποιήσει επιθέσεις άρνησης υπηρεσίας (DoS).

MAC Spoofing: Η πλαστογράφηση MAC είναι μια τεχνική παραπλάνησης για την αλλαγή της εργοστασιακά εκχωρημένης διεύθυνσης Media Access Control (MAC) μιας διεπαφής δικτύου σε μια συσκευή δικτύου. Η διεύθυνση MAC που είναι κωδικοποιημένη σε μια κάρτα διασύνδεσης δικτύου (NIC) δεν μπορεί να αλλάξει. Ωστόσο, υπάρχουν εργαλεία που μπορούν να κάνουν ένα λειτουργικό σύστημα να πιστέψει ότι το NIC έχει τη διεύθυνση MAC της επιλογής ενός χρήστη. Επιπλέον, πολλά προγράμματα επιτρέπουν την αλλαγή της διεύθυνσης MAC. Η διαδικασία πλαστογράφησης μιας διεύθυνσης MAC είναι γνωστή ως MAC Spoofing. Ουσιαστικά, η πλαστογράφηση MAC συνεπάγεται την αλλαγή της ταυτότητας ενός υπολογιστή για τη διεξαγωγή μιας επίθεσης. [23]

Εκμετάλλευση δεδομένων διαμόρφωσης δικτύου πρόσβασης: Η απειλή αυτή συνεπάγεται την παραβίαση ενός στοιχείου δικτύου πρόσβασης όπως σταθμοί βάσης, για τη δημιουργία δεδομένων διαμόρφωσης και την εκτόξευση άλλων επιθέσεων (π.χ. DoS).

Μπλοκάρισμα της ραδιοσυχνότητας (Jamming RF): Αυτή η απειλή αναφέρεται σε σκόπιμη διακοπή της ραδιοσυχνότητας δικτύου που προκαλεί το κεντρικό δίκτυο ώστε να μην είναι προσβάσιμες για τους επηρεαζόμενους χρήστες. Η απειλή αναφέρεται επίσης στη μη διαθεσιμότητα του επιπέδου μεταφοράς κατά τη χρήση δικτύων που βασίζονται σε ραδιοφωνικές συχνότητες και στην παρεμβολή στα συστήματα γεωγραφικής τοποθέτησης GPS.

Παρεμβολή ραδιοκυμάτων: Κατά την απειλή αυτή ο δράστης επιδιώκει να καταστήσει τους πόρους δικτύου μη διαθέσιμους στους χρήστες για τους οποίους προορίζεται, παρεμβαίνοντας προσωρινά ή διακόπτοντας την υπηρεσία του Δικτύου Πρόσβασης Ραδιοκυμάτων. Η εισαγωγή παραβιασμένων 5G συσκευών σε ένα δίκτυο ραδιοπρόσβασης θα παρουσιάσει μια πιο επικίνδυνη απειλή DoS.

Παραβίαση συνεδρίας (Session hijacking): Αυτή η απειλή θεωρείται ως κακόβουλη δραστηριότητα ή κατάχρηση περιουσιακών στοιχείων και σχετίζεται με επιθέσεις σε υπαίθριες υποδομές. Η απειλή θεωρεί την κλοπή του νόμιμου πιστοποιημένου αναγνωριστικού συνεδρίας συνομιλίας από έναν κακόβουλο παράγοντα, για τον έλεγχο ολόκληρης της περιόδου σύνδεσης συγκεκριμένης κυκλοφορίας για τη διεξαγωγή άλλων τύπων επιθέσεων.

Εκμετάλλευση ραδιοεπικοινωνίας (Radio traffic manipulation): Η απειλή αυτή λαμβάνει υπόψη την παρακολούθηση της κυκλοφορίας του δικτύου σε επίπεδο σταθμού βάσης. Μια επίθεση MITM μπορεί να ξεκινήσει με βάση έναν ψεύτικο σταθμό βάσης όταν ένας κακόβουλος χρήστης μεταμφιέζει τον σταθμό βάσης πομπού του (BTS) ως BTS ενός πραγματικού δικτύου. Αυτή η απειλή εξακολουθεί να θεωρείται επίκαιρη λόγω της συμβατότητας με προηγούμενες γενιές κινητής τεχνολογίας.

Καταιγίδες σηματοδότησης (Signalling storms): Τα δίκτυα κινητής τηλεφωνίας υπόκεινται σε αδιάλειπτη εκπομπή σηματοδότησης που εκτοξεύεται από κακόβουλο λογισμικό ή εφαρμογές, οι οποίες υπερφορτώνουν το εύρος ζώνης στην εκάστοτε κυψέλη, στους διακομιστές σηματοδότησης κορμού και στους διακομιστές Cloud. Επίσης μπορούν να εξαντλήσουν την ισχύ της μπαταρίας των κινητών συσκευών. Οι καταιγίδες σηματοδότησης γίνονται πιο απαιτητικές λόγω της υπερβολικής συνδεσιμότητας των συσκευών χρηστών, των μικρών σταθμών βάσης και της υψηλής κινητικότητας των συνδρομητών.

Απάτη στη σηματοδότηση (Signalling fraud): Η διεθνής διασύνδεση σηματοδοσίας μεταξύ των δικτύων μπορεί να χρησιμοποιηθεί για απάτη ,όπως ψευδής χρέωση και αυτό είναι πολύ ανησυχητικό. Άλλο ένα παράδειγμα είναι η απειλή εν ενεργεία κινητών κόμβων που μεταδίδουν πλαστά σήματα και αναγκάζουν όλους τους άλλους χρήστες να εκκενώσουν μια συγκεκριμένη ζώνη για να αποκτήσουν την αποκλειστική χρήση της. [23]

4.1.3.3 Απειλές πολλαπλών υπολογιστικών άκρων (Multi edge computing threats)

Υπερφόρτωση κόμβου άκρης (Edge node overload): Η απειλή αυτή σχετίζεται με επιθέσεις εναντίον δικτύων που διακόπτουν την περιοχή των ευάλωτων δικτύων, σε τοπικό επίπεδο ή σε επίπεδο υπηρεσίας. Η υπερφόρτωση μπορεί να λάβει χώρα πλημμυρίζοντας τον κόμβο άκρης με αίτημα ή κίνηση που κατευθύνεται σε αυτό το στοιχείο, που ξεκινά από μια συγκεκριμένη εφαρμογή για κινητά ή συσκευή IoT.

Rogue multi-access edge computing gateway: Η ανοιχτή φύση των συσκευών υπολογιστικού άκρου, όπου ακόμη και συσκευές που ανήκουν στον χρήστη μπορούν να γίνουν πλήρως διαμοιραζόμενες, δημιουργεί ένα σενάριο όπου οι κακόβουλοι

χρήστες μπορούν να αναπτύξουν τη δική τους πύλη gateway συσκευής. Αυτή η συγκεκριμένη απειλή παράγει το ίδιο αποτέλεσμα με την επίθεση MITM.

Κατάχρηση διεπαφών προγραμματισμού ανοιχτών εφαρμογών (APIs): Η κατάχρηση ανοιχτών API σε κόμβους Υπολογιστών Multi Edge γίνεται μέσω της εκμετάλλευσης τρωτών σημείων σε εφαρμογές τύπου MEC (Multi-access edge computing). Η ανάγκη για ανοιχτά API είναι κυρίως η παροχή υποστήριξης για τηλεπικοινωνιακές υπηρεσίες και αλληλεπιδράσεις με διαφορετικούς παρόχους και δημιουργούς περιεχομένου. Αυτή η απειλή μπορεί να συσχετιστεί με προβλήματα DoS, MITM, κακόβουλης λειτουργίας, διαρροές απορρήτου και χειραγώγηση εικονικών μηχανών VM. [23]

4.1.3.4 Απειλές εικονικοποίησης (Virtualization Threats)

Κατάχρηση υπολογιστικών πόρων cloud: Η κατάχρηση μιας cloud υποδομής υπολογιστών, συμπεριλαμβανομένων του λογισμικού και του υλικού, θα μπορούσε εύκολα να γίνει χρησιμοποιώντας μια συνήθη διαδικασία εγγραφής σε έναν πάροχο υπηρεσιών υπολογιστικού νέφους. Εκμεταλλευόμενοι την μεγάλη υπολογιστική ισχύ των δικτύων cloud, οι χάκερ μπορούν να εξαπολύσουν επιθέσεις σε πολύ σύντομο χρονικό διάστημα. Για παράδειγμα, οι επιθέσεις DoS μπορούν να ξεκινήσουν με κατάχρηση της ισχύος μιας υποδομής υπολογιστικού νέφους.

Κατάχρηση του πρωτοκόλλου διασύνδεσης κέντρων δεδομένων (DCI-Data Centers Interconnect): Τα εικονικά συστήματα αναπτύσσονται εντός κέντρων δεδομένων, επομένως, θα πρέπει να λαμβάνονται υπόψη οι απειλές για την ασφάλεια των Κέντρων Δεδομένων. Η απειλή αυτή σχετίζεται με την εκμετάλλευση συγκεκριμένων ευπαθών σημείων των πρωτοκόλλων Data Centers Interconnect όπως έλλειψη ελέγχου ταυτότητας και κρυπτογράφησης. Ένας εισβολέας θα μπορούσε να δημιουργήσει πλαστογραφημένη κίνηση με τέτοιο τρόπο ώστε να δημιουργήσει μια επίθεση DoS σε συνδέσεις των πρωτοκόλλων DCI.

Κατάχρηση εικονικού κεντρικού υπολογιστή (Virtualised host abuse): Η απειλή αυτή σχετίζεται με εφαρμογές που εκτελούνται σε κεντρικούς υπολογιστές με virtualization και που κάνουν κατάχρηση των κοινόχρηστων πόρων από ένα περιβάλλον virtualized. Σε εικονικά περιβάλλοντα, όπου υπάρχει διαμοιρασμός

φυσικών πόρων μεταξύ των ενοικιαστών, μπορεί να υπάρχει ένα σύνολο συμπεριφορών που έχουν ως αποτέλεσμα την αποκάλυψη ευαίσθητων πληροφοριών. Μάλιστα η έκθεση σε εικονικά περιβάλλοντα είναι ακόμη πιο σοβαρή από ό,τι σε φυσικά συστήματα. Ενώ η υποκλοπή είναι μια κοινή απειλή σε φυσικά συστήματα, η επίδρασή της επιδεινώνεται περαιτέρω σε εικονικά περιβάλλοντα.

Παράκαμψη εικονικοποίησης του δικτύου (Network virtualisation bypassing): Η κακή εφαρμογή τεμαχισμού δικτύου (network slicing) ή μια ακατάλληλη απομόνωση μπορεί να προκαλέσουν απώλεια του απόρρητου δεδομένων. Ένα δίκτυο που χρησιμοποιείται από διαφορετικούς ενοικιαστές – πελάτες, θα πρέπει να διασφαλίζει ότι μόνο η νόμιμη κίνηση εισέρχεται ή εξέρχεται από ένα κομμάτι δικτύου, αλλά και ότι οποιοδήποτε στοιχείο διαχείρισης ελέγχει και επιβάλλει την απομόνωση κυκλοφορίας εγκαθιστώντας νόμιμους κανόνες ροής που αποτρέπουν την παραβίαση του τμήματος. Σε επίπεδο δικτύου πυρήνα, ο εχθρικός παράγοντας θα εκμεταλλευόταν τα τρωτά σημεία του hypervisor και τη διαμόρφωση κανόνων ροής για να παραβιάσει την απομόνωση τμημάτων και να αποκαλύψει δεδομένα που ανήκουν σε άλλους ενοικιαστές. [23]

4.1.3.5 Απειλές φυσικών υποδομών (Physical infrastructure threats)

Φυσική δολιοφθορά της υποδομής δικτύου: Η απειλή αυτή είναι η εσκεμμένη φυσική επίθεση που σχετίζεται με ενέργειες που πραγματοποιούνται από άτομα που στοχεύουν στην καταστροφή, την απενεργοποίηση ή την κλοπή φυσικών περιουσιακών στοιχείων που υποστηρίζει το δίκτυο 5G. Μια δολιοφθορά σε σημαντικές 5G υποδομές μπορεί να διαταράξει, να παρεμποδίσει και τελικά να προκαλέσει μη διαθεσιμότητα της υπηρεσίας δικτύου. Παρά την ύπαρξη μηχανισμών φυσικής προστασίας (π.χ. παρακολούθησης με φύλακες, κάμερες παρακολούθησης CCTV και κλειδαριές ασφαλείας με βιομετρικές μεθόδους), ενδέχεται να εξακολουθήσουν να συμβαίνουν φυσικές παραβιάσεις και επιθέσεις από εσωτερικές απειλές.

Χειρισμός εξοπλισμού υλικού: Αυτή η απειλή λαμβάνει υπόψη τη συμπερίληψη κρυφού υλικού ή λογισμικού στο προϊόν από έναν πωλητή ή προμηθευτή. Μπορεί να

προκύψει σε ένα αρχικό στάδιο της υλοποίησης εγκατάστασης του προϊόντος ή κατά τη συντήρηση με την εφαρμογή ενημερώσεων μη εγκεκριμένων και νέων λειτουργιών.

Φυσικές καταστροφές που επηρεάζουν την υποδομή του δικτύου: Είναι η φυσική ή περιβαλλοντική καταστροφή. Η απειλή αυτή αναφέρεται σε φυσικά γεγονότα όπως πυρκαγιές, πλημμύρες και σεισμοί που μπορούν να επηρεάσουν τον εξοπλισμό του δικτύου 5G και συνεπώς τη διαθεσιμότητα της υπηρεσίας σε τοπικό και περιφερειακό επίπεδο. Συνήθως οι εγκαταστάσεις σε εξωτερικό περιβάλλον είναι περισσότερο εκτεθειμένες σε φυσικές καταστροφές, όπως ο εξοπλισμός ραδιοπρόσβασης, οι σταθμοί βάσης και οι υποδομές μεταφοράς δικτύου.

Κίνδυνος στον εξοπλισμού του χρήστη : Νέος εξοπλισμός χρήστη, όπως οι χαμηλού κόστους ανασφαλείς συσκευές IoT, θα μπορούσαν να εισαγάγουν νέους τύπους ευάλωτων σημείων, τα οποία μπορεί να αξιοποιηθούν για τη στόχευση του απορρήτου και της ακεραιότητας των δεδομένων χρήστη. Οι καταχρήσεις στην υλοποίηση υλικού και λογισμικού από την πλευρά της ΕΕ για την εγκατάσταση κακόβουλων στοιχείων ενδέχεται να θέσουν σε κίνδυνο την εμπιστευτικότητα και την ακεραιότητα των δεδομένων προφίλ συνδρομητή.

Εκμετάλλευση UICC (Universal Integrated Circuit Card) – SIM card: Οι νέες τεχνολογίες καρτών κινητής τηλεφωνίας θα μπορούσαν να οδηγήσουν σε νέους τύπους ευπαθειών που μπορεί να αξιοποιηθούν για σκοπούς κλοπής δεδομένων, απάτης ή επίθεσης DoS. Διαφορετικοί τύποι νέων τεχνολογιών UICC – SIM cards προϋποθέτουν νέα πρωτόκολλα διαχείρισης για την εξυπηρέτηση των χρηστών τους. Αυτά τα πρωτόκολλα μπορούν να αξιοποιηθούν για τη δημιουργία DoS επιθέσεων προς τον χρήστη, όπως και για σενάρια απάτης, συμπεριλαμβανομένης της πλαστοπροσωπίας του χρήστη. [23]

4.1.3.6 Γενικές απειλές (General threats)

Υποκλοπή - Παρακολούθηση (Eavesdropping): Η υποκλοπή είναι μια απειλή κατά την οποία ο δράστης επιδιώκει να παραβιάσει τα επίπεδα εφαρμογής και επικοινωνίας των διάφορων στοιχείων του δικτύου 5G (π.χ SDN controller, λειτουργία δικτύου, κόμβος άκρων, ενορχηστρωτής εικονικοποίησης). Περιλαμβάνει την υποκλοπή δεδομένων συνδρομητή, εμπιστευτικές πληροφορίες, ώρα συστήματος, τοποθεσία

συνδρομητή, ηλεκτρονικά μηνύματα, σήμα δεδομένων που αναμεταδίδονται μέσω του δικτύου. Ο παράγοντας της απειλής παρακολουθεί, κατασκοπεύει ή και κρυφακούει πολίτες και οργανισμούς εθνικού κράτους για να παρακολουθεί την τοποθεσία ή να έχει πρόσβαση σε ευαίσθητες πληροφορίες.

Άρνηση υπηρεσίας (DoS): Σε μια DoS απειλή ο δράστης επιδιώκει να καταστήσει έναν πόρο δικτύου μη διαθέσιμο στους προβλεπόμενους χρήστες του παρεμβαίνοντας προσωρινά ή διακόπτοντας επ' αόριστον την υπηρεσία του δικτύου. Η επίθεση περιλαμβάνει τη δημιουργία ενός μεγάλου αριθμού αιτημάτων, με τρόπο που το δίκτυο καθίσταται εν μέρει ή εντελώς μη διαθέσιμο για τους τακτικούς χρήστες. Πολλαπλοί τύποι απειλών μπορεί να οδηγήσουν σε άρνηση παροχής υπηρεσιών, όπως πλημμύρες, σηματοδότηση καταιγίδας και επιθέσεις κορεσμού. Μια επίθεση που συνδυάζει πολλαπλούς επιτιθέμενους μπορεί να οδηγήσει σε επίθεση κατανεμημένου DoS (DDoS).

Παραβίαση δεδομένων, διαρροή, κλοπή, καταστροφή και χειραγώγηση πληροφοριών: Περιλαμβάνει, την κλοπή προσωπικών πληροφοριών μέσω της μη εξουσιοδοτημένης πρόσβασης στα συστήματα και το δίκτυο. Έτσι είναι πιθανή η δημοσίευση προσωπικών στοιχείων ταυτοποίησης είτε βιομετρικών είτε ιατρικών απορρήτων ,η αποκάλυψη εταιρικών εμπιστευτικών πληροφοριών και η διαρροή κρατικών διαβαθμισμένων πληροφοριών. Η κλοπή, η παραβίαση ή η διαρροή άλλων τύπων δεδομένων, όπως διαπιστευτήρια χρήστη, κλειδιά κρυπτογράφησης, αρχεία καταγραφής ασφάλειας δικτύου, διαμόρφωση λογισμικού κ.λπ. μπορεί επίσης να βοηθήσει τους κακόβουλους χρήστες να διεξάγουν συγκεκριμένους και στοχευμένους τύπους επιθέσεων.[23]

Κακόβουλος κώδικας ή λογισμικό: Η απειλή περιλαμβάνει την εγκατάσταση και διανομή κακόβουλου λογισμικού ή την εμφύτευση συγκεκριμένου κώδικα ή λογισμικού μέσα σε ένα προϊόν ή με τη μορφή ενημερώσεων. Παραδείγματα κακόβουλου λογισμικού περιλαμβάνουν ransomware, virus, worms, trojans, malware, SQL injections, adaware και λογισμικό συντήρησης. Ένα παράδειγμα κακόβουλου λογισμικού στο πλαίσιο του 5G εξετάζει τη χρήση ενός μη εξουσιοδοτημένου VNF που θα μπορούσε να εγκατασταθεί και να εγγραφεί καταχρηστικά στο κεντρικό δίκτυο προκειμένου να αποκαλύψει κακόβουλα API.

Παραβιασμένη εφοδιαστική αλυσίδα προμηθευτών και παρόχων υπηρεσιών: Η απειλή αυτή λαμβάνει υπόψη την σκόπιμη εισαγωγή στο προϊόν κρυφών ελαττωμάτων υλικού και κακόβουλου λογισμικού. Εξετάζει επίσης την εφαρμογή ενημερώσεων λογισμικού χωρίς την συγκατάθεση του χρήστη και τη χειραγώγηση λειτουργιών για παράκαμψη των μηχανισμών ελέγχου. Ενδέχεται να εγκατασταθούν backdoors και μη αποδεκτές ρυθμίσεις που έχουν απομείνει στην έκδοση παραγωγής. Η απειλή αυτή επίσης σχετίζεται με δραστηριότητες που εκτελούνται από αναξιόπιστο προσωπικό τρίτων κατά τον κύκλο ζωής προϊόντος (διάρκεια δοκιμών, συντήρησης, διαμόρφωσης και λειτουργίας του). Το αναξιόπιστο προσωπικό έχει πρόσβαση στις εγκαταστάσεις διαχείρισης δικτύου (τόσο τοπικά όσο και μέσω απομακρυσμένης διαχείρισης) προκειμένου να παρέχει τεχνική υποστήριξη και να εκτελεί δραστηριότητες συντήρησης.

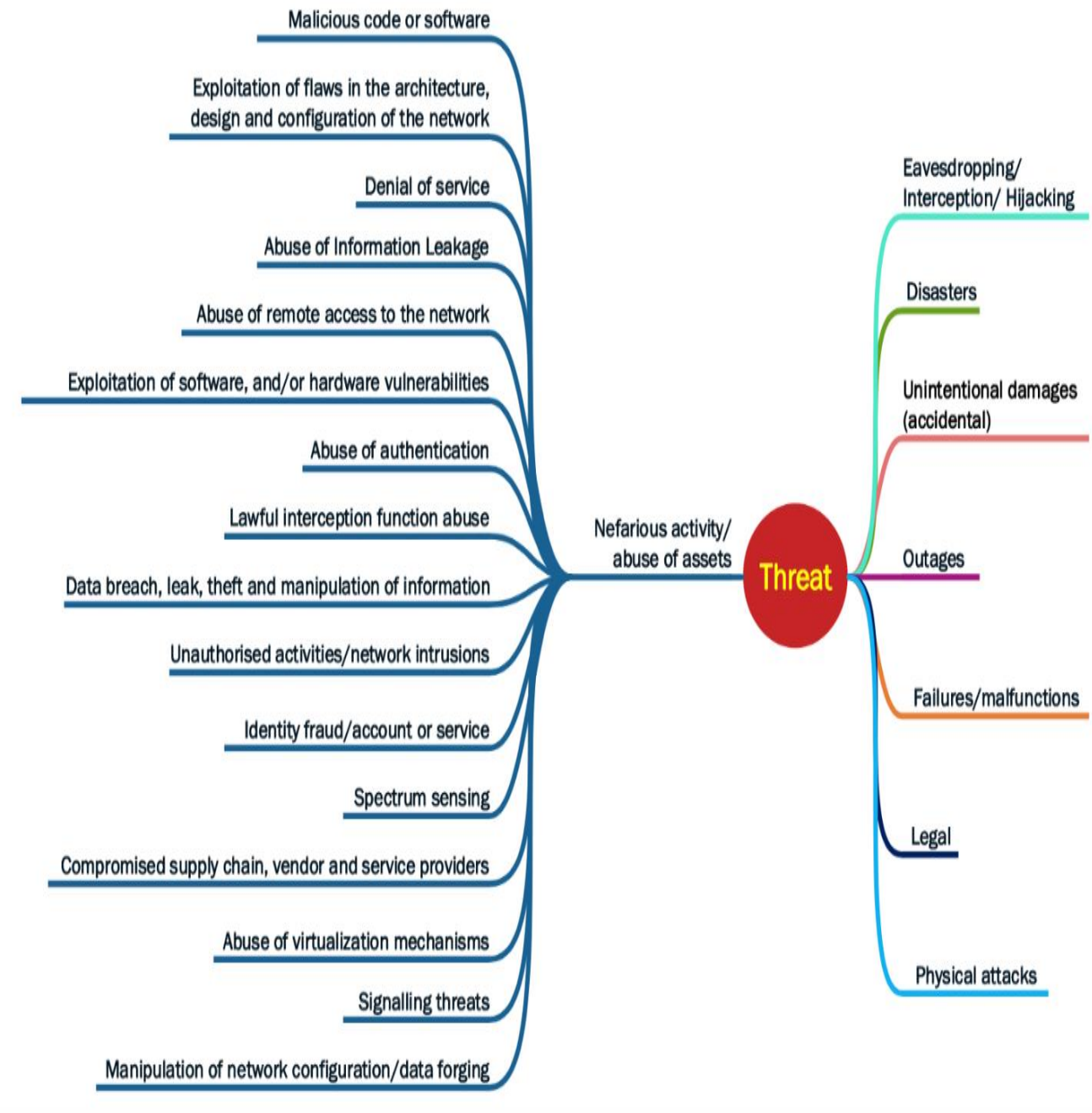
Εκμετάλλευση τρωτών σημείων λογισμικού και υλικού: Αυτός ο τύπος απειλής επιτρέπει σε έναν κακόβουλο χρήστη να εκμεταλλευτεί άγνωστα (για τον προμηθευτή και τον χρήστη) ή μη επιδιορθωμένα σφάλματα λογισμικού ή υλικού για να εκτελέσει μια επίθεση. Το παράδειγμα περιλαμβάνει την εκμετάλλευση γνωστών ελαττωμάτων υλικού και λογισμικού, όπως η κατάρρευση στο φάσμα και η υπερχείλιση του buffer. Περιλαμβάνει επίσης την εκμετάλλευση άλλων γνωστών τρωτών σημείων που σχετίζονται με προηγούμενες γενιές κινητών τηλεπικοινωνιών και παλαιότερα πρωτόκολλα σηματοδότησης όπως το SS7 (Signalling System 7) και το Diameter.

Στοχευμένες απειλές: Οι σύγχρονες επιθέσεις ή οι προηγμένες απειλές ενδέχεται να στοχεύουν σε ευαίσθητες πληροφορίες, όπως κρατικά μυστικά, βιομηχανικά μυστικά ή κλοπή πνευματικής ιδιοκτησίας ή διαθεσιμότητα ευαίσθητων και κρίσιμων υπηρεσιών.

Κατάχρηση ελέγχου ταυτότητας: Αυτή η απειλή περιλαμβάνει κλοπή διαπιστευτηρίων χρηστών, παραβίαση των λογαριασμών χρηστών και των κωδικών πρόσβασης, απόκρυψη της ταυτότητας χρήστη και παραβίαση ελέγχου ταυτότητας. Πρόκειται για τεχνικές που χρησιμοποιούνται από επιτιθέμενους για την κατάχρηση των συστημάτων ελέγχου ταυτότητας στο 5G. Μπορεί να επηρεάσει πολλαπλά σημεία εισόδου δικτύου, όπως εξοπλισμό χρήστη (κινητές συσκευές και IoT), διεπαφές λειτουργίας και διαχείρισης, περιαγωγή και υπηρεσίες. [23]

Κλοπή ταυτότητας ή πλαστογράφηση: Αυτή η απειλή μπορεί να πραγματοποιηθεί όταν ένας κακόβουλος χρήστης καταφέρει να προσδιορίσει με επιτυχία την ταυτότητα μιας νόμιμης οντότητας και στη συνέχεια μεταμφιέζεται για να εξαπολύσει περαιτέρω επιθέσεις. Σε αυτήν την επίθεση, ο εισβολέας πλαστογραφεί την ταυτότητα ενός νόμιμου χρήστη και αλληλοεπιδρά με τις λειτουργίες δικτύου που ελέγχονται από τον νόμιμο χρήστη για να πυροδοτήσει άλλους τύπους επιθέσεων. Η χρήση της κοινωνικής μηχανικής (social engineering), μια brute force attack για το σπάσιμο του κωδικού πρόσβασης λογαριασμού χρήστη μπορεί επίσης να χρησιμοποιηθεί ως τεχνική για πλαστογράφηση ή κλοπή διαπιστευτηρίων χρήστη. Η πλαστογράφηση ταυτότητας είναι μια απειλή που μπορεί να επηρεάσει οποιοδήποτε στοιχείο λογισμικού ή ανθρώπινο παράγοντα.

Εκμετάλλευση ευπαθειών στις διαδικασίες ασφάλειας, διαχείρισης και λειτουργίας: Η απειλή αυτή θα γίνει σχετική όταν αντιμετωπίζουμε την πολυπλοκότητα της τεχνολογίας και την ανάγκη εισαγωγής διαδικασιών στη διαχείριση του δικτύου. Αυτή η απειλή περιλαμβάνει, την εκμετάλλευση ελαττωμάτων στη λειτουργική διαχείριση και τη διαχείριση ασφάλειας του δικτύου. ρύθμιση παραμέτρων, ενημέρωση και διαχείριση ενημερώσεων του κώδικα του λογισμικού. Τα λάθη από την έλλειψη ή την κακή σχεδίαση λειτουργικών διαδικασιών και διαδικασιών ασφαλείας μπορεί να έχουν συνέπειες στην ακεραιότητα και τη διαθεσιμότητα του δικτύου. [23]



Εικόνα 25: ENISA threats landscape on 5G networks. [23]

4.2 Κατάλογος 5G και γενικών απειλών

Παράνομη δραστηριότητα και κατάχρηση - Nefarious activity, abuse (NAA)

Στον ακόλουθο πίνακα παρουσιάζονται οι απειλές που στοχεύουν συστήματα, υποδομές και δίκτυα υπολογιστών μέσω κακόβουλων επιθέσεων με σκοπό είτε την κλοπή, την αλλαγή ή την καταστροφή ενός συγκεκριμένου στόχου. Επίσης αναφέρονται οι επιπτώσεις στις πληροφορίες και υπηρεσίες καθώς και τι ζημιές γίνονται στις υποδομές.

Πίνακας 5: Παράνομη δραστηριότητα και κατάχρηση - Nefarious activity, abuse (NAA)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Επίθεση διαμόρφωσης δικτύου και πλαστογράφηση δεδομένων - Αλλαγή πινάκων δρομολόγησης - Παραποίηση δεδομένων διαμόρφωσης - Επίθεση στο DNS - Εκμετάλλευση δικτύου πρόσβασης και ράδιο συχνότητας - Εκμετάλλευση λάθους ή κακής διαμόρφωσης στα συστήματα δικτύου - Καταχώρηση κακόβουλων λειτουργιών στο δίκτυο	- Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών - Μη διαθεσιμότητα υπηρεσίας - SDN, NFV, MANO, RAN, RAT	- Δεδομένα διαμόρφωσης συστήματος (system configuration) - Δεδομένα διαμόρφωσης δικτύου (network configuration) - Δεδομένα διαμόρφωσης ασφαλείας (security configuration) - Επιχειρηματικές υπηρεσίες
Software Exploitation, Hardware Vulnerabilities - Zero-day exploits - Κατάχρηση και εκμετάλλευση στα API.	- Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών - Μη διαθεσιμότητα υπηρεσίας - SDN, NFV, MANO, RAN, RAT - Cloud, Virtualization	- Subscribers' data - Application data - Security data - Network data - Επιχειρηματικές υπηρεσίες
Άρνηση υπηρεσίας (DoS) - Πλημμύρα network core - Πλημμύρες base stations - Επιθέσεις ενίσχυσης - Επιθέσεις επιπέδου MAC - Εμπλοκή ράδιο δικτύου - Υπερφόρτωση κόμβου άκρης και DDoS - Απότομες αυξήσεις επισκεψιμότητας	- Μη διαθεσιμότητα υπηρεσίας - Διακοπή λειτουργίας	-Network services -Business services - SDN, NFV, RAN, RAT - Cloud

Malicious code / software - Injection attacks(SQL, XSS) - Virus - Malware - Rootkits - Worms / trojan - Botnet - Ransomware	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών - Καταστροφή περιουσιακών στοιχείων λογισμικού	- Δεδομένα συνδρομητή - Application data - Security data - Network data - Business services - Network services - Cloud, Virtualization
Κατάχρηση διαρροής πληροφοριών - Κλοπή και διαρροή από το ttaffic του δικτύου - Κλοπή και διαρροή δεδομένων από το cloud - Κατάχρηση δεδομένων ασφαλείας από εργαλεία ελέγχου - Κλοπή και παραβίαση στα κλειδιά ασφαλείας	- Ακεραιότητα και εμπιστευτικότητα πληροφοριών - Καταστροφή πληροφοριών	- Αποθήκευση δεδομένων και στοιχεία συνδρομητών - Κρυπτογραφικά κλειδιά - Δεδομένα παρακολούθησης - Δεδομένα προφίλ συνδρομής χρήστη
Εκμετάλλευση υλικού και λογισμικού - Εκμετάλλευση εξοπλισμού υλικού και των πόρων του δικτύου ενορχηστρωτής - MAC Spoofing - Επιθέσεις πλευρικών καναλιών - Ψεύτικος κόμβος δικτύου πρόσβασης - Εκμετάλλευση μορφής UICC - Κίνδυνος εξοπλισμού χρήστη	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών	- Δεδομένα συνδρομητή - Υπηρεσίες δικτύου - Cloud data center equipment - User equipment - SDN, MANO - RAN, RAT - Virtualization
Παραβίαση δεδομένων, διαρροή, κλοπή και χειραγώγηση πληροφοριών	- Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών - Εμπιστευτικότητα πληροφοριών	- Στοιχεία και γεωγραφικές τοποθεσίες συνδρομητών - Εμπορικά και οικονομικά δεδομένα - Δεδομένα διαμόρφωσης δικτύου
Μη εξουσιοδοτημένες εισβολές στο δίκτυο - Επιθέσεις σύλληψης IMSI - Πλευρική κίνηση	- Ακεραιότητα πληροφοριών - Ακεραιότητα συστήματος	- Εξοπλισμός χρήστη - Υπηρεσίες δικτύου - Επιχειρηματικές υπηρεσίες
Παραβιασμένη αλυσίδα εφοδιασμού, ύποπτοι	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Επιχειρηματικές υπηρεσίες

προμηθευτές και πάροχοι υπηρεσιών - Απειλή από το προσωπικό τρίτων για πρόσβαση στις εγκαταστάσεις της αλυσίδας εφοδιασμού	- Καταστροφή πληροφοριών	- SDN, NFV, MANO - RAN, RAT, API - Φυσικές υποδομές - Έλεγχοι ασφαλείας - Cloud, virtualisation
Κατάχρηση μηχανισμών εικονικοποίησης - Παράκαμψη εικονικοποίησης δικτύου - Εκμετάλλευση εικονικής μηχανής - Απειλές για τα data center - Κατάχρηση πόρων cloud	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών	- Υπηρεσίες δικτύου - Επιχειρηματικές υπηρεσίες - Virtualisation - SDN, NFV, MANO - Cloud
Απειλές σηματοδότησης - Σηματοδότηση καταιγίδας - Απάτη σηματοδότησης	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών - Καταστροφή πληροφοριών	- Υπηρεσίες δικτύου - RAT , Protocols - Υποδομές ράδιο πρόσβασης

Υποκλοπή/Πειρατεία - Eavesdropping/Interception/ Hijacking (EIH)

Στον επόμενο πίνακα παρουσιάζονται οι απειλές που στοχεύουν στην ακρόαση, διακοπή ή κατάληψη του ελέγχου επικοινωνίας τρίτου μέρους χωρίς τη συναίνεσή του. Επίσης αναφέρονται οι επιπτώσεις στην ακεραιότητα και εμπιστευτικότητα των πληροφοριών καθώς και τι ζημιές γίνονται στις υποδομές όπως σε στοιχεία και γεωγραφικές τοποθεσίες συνδρομητών ή οικονομικά στοιχεία.

Πίνακας 6: Υποκλοπή/Πειρατεία - Eavesdropping/Interception/ Hijacking (EIH)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Κατασκοπεία σε κράτη και επιχειρήσεις	- Ακεραιότητα και εμπιστευτικότητα πληροφοριών	- Στοιχεία και γεωγραφικές τοποθεσίες συνδρομητών - Οικονομικά στοιχεία
Παρακολούθηση του traffic δικτύου και συλλογή πληροφοριών - Εκμετάλλευση κυκλοφορίας ράδιο δικτύου - Κακόβουλη εκτροπή και ανακατεύθυνση της κυκλοφορίας - Κατάχρηση των διασυνδέσεων περιαγωγής	- Ακεραιότητα και εμπιστευτικότητα πληροφοριών	- Διακίνηση δεδομένων - Στοιχεία και γεωγραφικές τοποθεσίες συνδρομητών
MITM και Session hijacking Υποκλοπή πληροφοριών	- Ακεραιότητα και εμπιστευτικότητα πληροφοριών	- Διακίνηση δεδομένων - Στοιχεία και γεωγραφικές τοποθεσίες συνδρομητών

Φυσικές επιθέσεις - Physical attacks (PA)

Στον επόμενο πίνακα παρουσιάζονται οι απειλές που στοχεύουν να καταστρέψουν, να εκθέσουν, να τροποποιήσουν, να απενεργοποιήσουν, να κλέψουν ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε φυσικά περιουσιακά στοιχεία, όπως υποδομή, υλικό ή διασύνδεση. Επίσης αναφέρονται οι επιπτώσεις στην μη διαθεσιμότητα υπηρεσίας και στην καταστροφή και ακεραιότητα πληροφοριών. Αποτέλεσμα είναι να υπάρχουν ζημιές στις υποδομές εξοπλισμού, στις μονάδες ράδιο πρόσβασης και στις υπηρεσίες δικτύου και data center.

Πίνακας 7: Φυσικές επιθέσεις - Physical attacks (PA)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Σαμποτάζ και βανδαλισμός υποδομής δικτύου	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Μονάδες ράδιο πρόσβασης - Υπολογιστικός εξοπλισμός - Cloud data center - Υπηρεσίες δικτύου
Μη εξουσιοδοτημένη φυσική πρόσβαση σε σταθμούς που βρίσκονται σε κοινόχρηστες τοποθεσίες	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Μονάδες ράδιο πρόσβασης - Υπολογιστικός εξοπλισμός - Cloud data center - Υπηρεσίες δικτύου
Κλοπή περιουσιακών στοιχείων και τρομοκρατική επίθεση στις υποδομές του δικτύου	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Μονάδες ράδιο πρόσβασης - Υπολογιστικός εξοπλισμός - Υπηρεσίες δικτύου

Καταστροφή περιουσίας - Damage (DAM)

Στον επόμενο πίνακα παρουσιάζονται οι απειλές που περιλαμβάνουν ενέργειες που είναι σκόπιμες και στοχεύουν στην πρόκληση καταστροφής περιουσίας, βλάβης και καταλήγουν σε αστοχία ή μείωση της χρησιμότητας. Επίσης αναφέρονται οι επιπτώσεις στην μη διαθεσιμότητα υπηρεσίας και στην ακεραιότητα των πληροφοριών. Αποτέλεσμα είναι να υπάρχουν ζημιές στις υποδομές εξοπλισμού, στις φυσικές υποδομές και στα δεδομένα δικτύου και ασφαλείας.

Πίνακας 8: Καταστροφή - Damage (DAM)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ ΣΕ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Ανεπαρκείς σχεδιασμοί και έλλειψη σωστών προσαρμογών - Ξεπερασμένο σύστημα από την έλλειψη updates ή patches - Σφάλματα από την έλλειψη κεντρικής διαχείρισης διαμόρφωσης - Κακή σχεδίαση δικτύου και αρχιτεκτονικής συστήματος	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών	- Στις πολιτικές διαχείρισης - SDN, NFV, MANO - RAN, API - Φυσικές υποδομές - Business applications - Έλεγχοι ασφαλείας - Cloud, virtualisation
Απώλεια δεδομένων από ακούσια διαγραφή ή διαρροή πληροφοριών λόγω ανθρώπινου λάθους	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών	- Στοιχεία συνδρομητών - Δεδομένα εφαρμογής - Δεδομένα ασφαλείας - Δεδομένα δικτύου
Κακώς διαμορφωμένα συστήματα και δίκτυα	- Μη διαθεσιμότητα υπηρεσίας - Ακεραιότητα πληροφοριών	- Στις πολιτικές διαχείρισης - SDN, NFV, MANO - RAN, API - Φυσικές υποδομές - Business applications - Έλεγχοι ασφαλείας - Cloud, virtualisation

Βλάβες και δυσλειτουργίες - Failures and malfunctions (FM)

Στον ακόλουθο πίνακα παρουσιάζονται οι απειλές που περιλαμβάνουν διακοπή της σύνδεσης επικοινωνίας , δυσλειτουργία εξοπλισμού ή βλάβη δικτύου και συσκευών. Επίσης αναφέρονται οι επιπτώσεις σε μη διαθεσιμότητα υπηρεσίας καταστροφή και ακεραιότητα πληροφοριών. Αποτέλεσμα είναι να υπάρχουν ζημιές στις υπηρεσίες δικτύου, στις υποδομές εξοπλισμού, στο data center και στις μονάδες ράδιο πρόσβασης.

Πίνακας 9: Βλάβες και δυσλειτουργίες - Failures and malfunctions (FM)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Διακοπή της σύνδεσης επικοινωνίας ή της κύριας παροχής ρεύματος	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services - Cloud data center
Δυσλειτουργία εξοπλισμού (συσκευών ή συστημάτων)	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Radio access units - ICT εξοπλισμός - Cloud data center

Βλάβη δικτύου, συσκευών ή συστημάτων	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Cloud data center - Εξοπλισμός χρήστη - RAT, Radio unit

Διακοπές - Outages (OUT)

Στον ακόλουθο πίνακα παρουσιάζονται οι απειλές που ορίζονται ως απρόσμενες διακοπές της υπηρεσίας ή μείωση της ποιότητας πέρα από ένα απαιτούμενο επίπεδο. Επίσης αναφέρονται οι επιπτώσεις σε μη διαθεσιμότητα υπηρεσίας καταστροφή και ακεραιότητα πληροφοριών. Αποτέλεσμα είναι να υπάρχουν ζημιές στις υπηρεσίες δικτύου, στις υποδομές εξοπλισμού, στο data center αλλά και ύπαρξη αντίκτυπου στο ανθρώπινο δυναμικό.

Πίνακας 10: Διακοπές - Outages (OUT)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Δίκτυο δεδομένων Πρόσβασης και παροχή ηλεκτρικού ρεύματος	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services - Cloud data center
Απώλεια πόρων - Ανθρώπινο δυναμικό - Φυσικοί πόροι	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services - Human assets
Υπηρεσίες υποστήριξης	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services - Human asstes - Διαδικασίες διαχείρισης - Πολιτικές - Νομικά θέματα

Καταστροφή - Disaster (DIS)

Στον ακόλουθο πίνακα παρουσιάζονται οι απειλές που ορίζονται ως ένα ξαφνικό ατύχημα ή μια φυσική καταστροφή που προκαλεί μεγάλη ζημιά ή καταστροφή υποδομών. Επίσης αναφέρονται οι επιπτώσεις σε μη διαθεσιμότητα υπηρεσίας καταστροφή και ακεραιότητα πληροφοριών. Αποτέλεσμα είναι να υπάρχουν ζημιές στις υπηρεσίες δικτύου, σε μονάδες ράδιο πρόσβασης και στις υποδομές εξοπλισμού και στο data center.

Πίνακας 11: Καταστροφή - Disaster (DIS)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Φυσικές καταστροφές - Σεισμοί - Κατολισθήσεις	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services - Μονάδες ράδιο πρόσβασης - ICT equipment - Cloud data center
Περιβαλλοντική καταστροφή - Πλημμύρες, καταιγίδες - Φωτιές, δυνατοί άνεμοι - Δυσμενείς κλιματολογικές συνθήκες	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services - Μονάδες ράδιο πρόσβασης - ICT equipment - Cloud data center

Νομικά - Legal (LEG)

Στον ακόλουθο πίνακα παρουσιάζονται οι απειλές που σχετίζονται με νομικές ενέργειες τρίτων, με σκοπό την απαγόρευση ενεργειών ή την αποζημίωση για απώλεια βάσει της ισχύουσας νομοθεσίας. Επίσης αναφέρονται οι επιπτώσεις σε μη διαθεσιμότητα υπηρεσίας καταστροφή και ακεραιότητα πληροφοριών.

Πίνακας 12: Νομικά - Legal (LEG)

ΑΠΕΙΛΕΣ	ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ	ΖΗΜΙΕΣ ΣΤΙΣ ΥΠΟΔΟΜΕΣ
Μη τήρηση συμβατικών απαιτήσεων και νομοθεσίας	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services
Παραβίαση συμφωνίας επιπέδου υπηρεσίας (SLA) και της νομοθεσίας	- Μη διαθεσιμότητα υπηρεσίας - Καταστροφή πληροφοριών - Ακεραιότητα πληροφοριών	- Υπηρεσίες δικτύου - Business services

ΚΕΦΑΛΑΙΟ 5ο

5.1 Πιθανοί φορείς απειλής στις υποδομές 5G-Σενάρια περιπτώσεων χρήσης

5.1.1 Πολιτική και Πρότυπα (Policy and Standards).

Η ανάπτυξη πολιτικών και προτύπων στα δίκτυα 5ης γενιάς θεωρείται ως το θεμέλιο για τη διασφάλιση της απρόσκοπτης λειτουργίας των επικοινωνιών στο 5G. Μέσω παγκόσμιων φορέων καθορισμού προτύπων, όπως το 3rd Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF) και η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), οργανισμοί ανάπτυξης τηλεπικοινωνιακών προτύπων αναπτύσσουν τεχνικά πρότυπα και ελέγχους ασφαλείας που θα επηρεάσουν το σχεδιασμό και την αρχιτεκτονική νέων τεχνολογιών, όπως αυτόνομα οχήματα, υπολογιστές αιχμής και τηλεϊατρική. Είναι σημαντικό τα διεθνή πρότυπα και οι πολιτικές υλοποίησης να είναι ανοιχτά, διαφανή και με συναίνεση στην υιοθέτηση της 5G τεχνολογίας.

Όσο κυκλοφορούν νέες πολιτικές και πρότυπα στο 5G, εξακολουθεί να υπάρχει η πιθανότητα για απειλές που επηρεάζουν τον τελικό χρήστη. Υπάρχει περίπτωση κάποια κράτη να επιχειρήσουν να ασκήσουν πίεση εφαρμογής στα πρότυπα που ωφελούν τις αποκλειστικές τεχνολογίες τους. Έτσι περιορίζουν τις επιλογές των πελατών να χρησιμοποιούν συγκεκριμένο υλικό ή λογισμικό. Υπάρχουν επίσης κίνδυνοι, όπου οι φορείς τυποποίησης ενδέχεται να αναπτύξουν προαιρετικούς ελέγχους, για την παρακολούθηση των πελατών τους. Με την μη εφαρμογή αυτών των πρακτικών, οι φορείς εκμετάλλευσης θα μπορούσαν να εισάγουν κενά ασφαλείας στο δίκτυο και να ανοίξουν την πόρτα για κακόβουλες απειλές. [24]

5.1.2 Εφοδιαστική αλυσίδα (Supply Chain).

Ο κίνδυνος αλλοίωσης της εφοδιαστικής αλυσίδας αναφέρεται στις προσπάθειες των κακόβουλων παραγόντων να εκμεταλλευτούν τις τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) και τις σχετικές αλυσίδες εφοδιασμού, για σκοπούς κατασκοπείας, δολιοφθοράς, ξένης παρέμβασης και παράνομης δραστηριότητας. Η αλυσίδα εφοδιασμού στο 5G είναι κι αυτή επιρρεπής στην εισαγωγή κινδύνων όπως κακόβουλο λογισμικό και υλικό, κακή σχεδίαση, πλαστά και ελλαττωματικά

εξαρτήματα και τέλος διαβλητές διαδικασίες κατασκευής και συντήρησης. Η έκθεση τους στους κινδύνους αυτούς ενισχύεται από την ευρεία απήχηση των τεχνολογιών 5G και τη βιασύνη για ανάπτυξη. Αυτό μπορεί να έχει αρνητικές συνέπειες, όπως κλοπή δεδομένων και πνευματικής ιδιοκτησίας, απώλεια εμπιστοσύνης στην ακεραιότητα του δικτύου 5G ή εκμετάλλευση για την πρόκληση αστοχίας συστήματος και δικτύου.

Με τη δυνατότητα σύνδεσης δισεκατομμυρίων συσκευών 5G, υπάρχει αυξημένος κίνδυνος εισαγωγής μη αξιόπιστων ή πλαστών εξαρτημάτων στην αλυσίδα εφοδιασμού 5G. Αυτό θα μπορούσε να περιλαμβάνει παραβιασμένες rooted συσκευές ή υποδομές διαχείρισης που τελικά επηρεάζουν συσκευές τελικού χρήστη, όπως υπολογιστές, τηλέφωνα, και άλλες συσκευές όπως server παρόχων. Οι μη αξιόπιστες εταιρείες ή οι προμηθευτές που υποστηρίζονται από την κυβέρνηση συμβάλλουν επίσης στον κίνδυνο της εφοδιαστικής αλυσίδας, ειδικά εκείνες που έχουν σημαντικό διεθνές μερίδιο αγοράς στα τηλεπικοινωνιακά δίκτυα. Για παράδειγμα, οι χώρες που προμηθεύονται εξοπλισμό 5G από εταιρείες με ύποπτες αλυσίδες εφοδιασμού θα μπορούσαν να είναι ευάλωτες στην υποκλοπή, χειραγώγηση, διακοπή ή καταστροφή δεδομένων. Έτσι το ασφαλές δίκτυο μιας χώρας θα μπορούσε να είναι ευάλωτο σε απειλές λόγω ενός μη αξιόπιστου δικτύου τηλεπικοινωνιών κατά την αποστολή δεδομένων σε μια άλλη χώρα. [24]

5.1.3 Αρχιτεκτονική Συστημάτων 5G (5G Systems Architecture).

Καθώς αναπτύσσονται νέα στοιχεία και τεχνολογίες 5G, θα ανακαλυφθούν και νέες αδυναμίες. Η μελλοντική αρχιτεκτονική συστημάτων στο 5G (Software Defined Networking, cloud native infrastructure, network slicing, edge computing) μπορεί να δημιουργήσει μια αυξημένη πιθανότητα επίθεσης για εκμετάλλευση κακόβουλων παραγόντων. Για παράδειγμα, η επικάλυψη αρχιτεκτονικών παλαιού τύπου 4G και 5G θα μπορούσε να δώσει την ευκαιρία σε έναν κακόβουλο χρήστη να πραγματοποιήσει μια επίθεση υποβάθμισης δηλαδή ένας χρήστης με 5G θα μπορούσε να αναγκαστεί να χρησιμοποιήσει δίκτυο 4G, επιτρέποντας έτσι στον κακόβουλο παράγοντα να εκμεταλλευτεί γνωστά και ευπαθή σημεία που υπάρχουν στο 4G. Αυτές οι απειλές και τα τρωτά σημεία θα μπορούσαν να χρησιμοποιηθούν από κακόβουλες οντότητες απειλών για να επηρεάσουν αρνητικά τους οργανισμούς και τους χρήστες. Χωρίς

συνεχή εστίαση σε φορείς απειλών 5G και έγκαιρο εντοπισμό αδυναμιών στην αρχιτεκτονική του συστήματος, τα νέα τρωτά σημεία θα αυξήσουν τον αντίκτυπο των περιστατικών στον κυβερνοχώρο.

Οι αρχιτεκτονικές συστημάτων 5G σχεδιάζονται και αναπτύσσονται για να ανταποκρίνονται στις αυξανόμενες απαιτήσεις δεδομένων, χωρητικότητας και επικοινωνιών. Παρόλο που οι κατασκευαστές εξαρτημάτων 5G και οι πάροχοι υπηρεσιών ενισχύουν την ασφάλεια μέσω τεχνολογικών βελτιώσεων, τόσο τα παλαιού τύπου όσο και οι νέες τρύπες ασφαλείας ενδέχεται να γίνουν αντικείμενο εκμετάλλευσης από κακόβουλους χρήστες. Επιπλέον, τα δίκτυα 5G θα χρησιμοποιούν περισσότερα στοιχεία τεχνολογίας υπολογιστών και επικοινωνιών από ό,τι οι προηγούμενες γενιές ασύρματων δικτύων. Έτσι θα μπορούσαν να παρέχουν σε κακόβουλους φορείς τη δυνατότητα να υποκλέψουν, να χειραγωγήσουν, να διαταράξουν και να καταστρέψουν σημαντικά δεδομένα. Η αυξημένη χωρητικότητα του 5G διευκολύνει τη διάδοση του Διαδικτύου των Πραγμάτων IoT, το οποίο προσθέτει πολλές και λιγότερο ασφαλείς συσκευές στο δίκτυο 5G.

Αυτή η αυξημένη ποικιλία στοιχείων μπορεί να οδηγήσει σε πολυπλοκότητα στην αρχιτεκτονική 5G και μπορεί να δημιουργήσει απρόβλεπτες, συνολικές αδυναμίες ή ευπάθειες του συστήματος. [24]

5.2 5G Φορείς απειλής.

Στη συνέχεια περιγράφονται λεπτομερώς οι επιμέρους απειλές κάθε κύριου φορέα απειλής. Αυτό με βάση τα τρία σενάρια απειλών που προαναφέραμε. Δηλαδή της Πολιτικής και των Προτύπων, της Εφοδιαστικής Αλυσίδας και της Αρχιτεκτονικής Συστημάτων 5G,

5.2.1 Υπό-απειλές πολιτικής και προτύπων (Policy and Standards Sub-Threat Vectors)

Προαιρετικοί έλεγχοι (Optional Controls): Οι παγκόσμιοι φορείς τυποποίησης προτύπων αναπτύσσουν πρωτόκολλα για κινητές τηλεπικοινωνίες, ορισμένα από τα οποία περιέχουν ελέγχους ασφαλείας που είναι είτε υποχρεωτικοί είτε προαιρετικοί.

Όσοι φορείς εκμετάλλευσης δικτύων δεν εφαρμόζουν προαιρετικούς ελέγχους ασφαλείας ενδέχεται να έχουν πιο ευάλωτα δίκτυα και να διατρέχουν μεγαλύτερο κίνδυνο για επιθέσεις στο διαδίκτυο.

Ανοιχτά Πρότυπα (Open Standards): Καθώς τα αντίπαλα κράτη συμβάλλουν στην ανάπτυξη τεχνικών προτύπων, υπάρχει η δυνατότητα τα πρότυπα να περιλαμβάνουν μη αξιόπιστες τεχνολογίες και εξοπλισμό που είναι μοναδικά για τα συστήματά τους. Οι προσαρμοσμένες τεχνολογίες 5G που δεν πληρούν τα πρότυπα διαλειτουργικότητας μπορεί να είναι δύσκολο να ενημερωθούν, να επισκευαστούν και να αντικατασταθούν ή θα μπορούσαν να είναι εντελώς αόρατες στον πελάτη. Αυτό δυνητικά αυξάνει το κόστος κύκλου ζωής του προϊόντος και καθυστερεί την ανάπτυξη 5G εάν ο εξοπλισμός απαιτεί αντικατάσταση. [25]

5.2.2 Υπό-απειλές εφοδιαστικής αλυσίδας (Supply Chain Sub-Threat Vectors).

Κληρονομικά εξαρτήματα (Inherited Components):*Τα* εξαρτήματα αυτά μπορεί να προέρχονται από αλυσίδες εφοδιασμού που αποτελούνται από τρίτους προμηθευτές, πωλητές και παρόχους υπηρεσιών. Οι αλυσίδες εφοδιασμού ενδέχεται να τεθούν σε κίνδυνο μέσω επιθέσεων σε προμηθευτές, συμπεριλαμβανομένων των προμηθευτών ,οι οποίοι ενδέχεται να έχουν ασθενέστερους ελέγχους ασφαλείας στα κανάλια μεταφοράς, παραγωγής ή παράδοσης. Το κακόβουλο ή ελλαττωματικό λογισμικό που έχει εισαχθεί νωρίς στις φάσεις ανάπτυξης είναι πιο δύσκολο να εντοπιστεί και θα μπορούσε να οδηγήσει στην παραπλάνηση του προγραμματιστή και του τελικού χρήστη ως νόμιμο μέσω ψηφιακών υπογραφών ή άλλων εγκρίσεων.

Πλαστά εξαρτήματα (Counterfeit Components):Τα πλαστά εξαρτήματα είναι πιο επιρρεπή σε επιθέσεις και είναι πιο πιθανό να αλλοιωθούν λόγω της κακής ποιότητάς τους. Παραβιασμένα πλαστά στοιχεία θα μπορούσαν να επιτρέψουν σε έναν κακόβουλο χρήστη να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων των συσκευών και να εισέλθει σε άλλα πιο ευαίσθητα μέρη του δικτύου. [25]

5.2.3 Υπό-απειλές αρχιτεκτονικής συστημάτων 5G.

Ασφάλεια δικτύου (Network Security): Οι τεχνολογίες 5G δίνουν τη δυνατότητα για δισεκατομμύρια συνδεδεμένες συσκευές δικτύου. Αυτές οι συσκευές και οι εγκαταστάσεις υποδομής, όπως οι κυψελοειδείς πύργοι, ο σχηματισμός δέσμης προς μετάδοση, οι μικρές κυψέλες και οι κινητές συσκευές, δίνουν την ευκαιρία στους κακόβουλους παράγοντες να εκμεταλλευτούν τα ευπαθή σημεία σε καταστάσεις απειλής. Εάν οι συσκευές δικτύου παραβιάζονταν, τότε κακόβουλοι χρήστες θα μπορούσαν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο δίκτυο 5G με αποτέλεσμα την διαταραχή των λειτουργιών και να επιτρέψουν την υποκλοπή, την εκμετάλευση και την καταστροφή σημαντικών δεδομένων.

Διαμόρφωση στο Λογισμικού (Software Configuration): Η πρόσβαση χωρίς εξουσιοδότηση σε λογισμικό ή υπηρεσίες δικτύου παρέχει σε έναν κακόβουλο χρήστη την ευκαιρία να τροποποιήσει τις ρυθμίσεις για να μειώσει τους ελέγχους ασφαλείας, να εγκαταστήσει ένα malware στο σύστημα ή να εντοπίσει τις αδυναμίες του προϊόντος. Αυτά τα ευπαθή σημεία θα μπορούσαν να χρησιμοποιηθούν για πρόσβαση σε ένα σύστημα ή σε ένα δίκτυο.

Τεμαχισμός δικτύου (Network Slicing): Ο τεμαχισμός δικτύου επιτρέπει στους χρήστες τον έλεγχο λειτουργίας για μόνο μία απομονωμένη περιοχή του δικτύου, επιτρέποντας την πρόσβαση σε συγκεκριμένα δεδομένα και έτσι μεγαλύτερη ασφαλείας. Ωστόσο, η διαχείριση σε ένα τεμαχισμένο δικτύου μπορεί να είναι δύσκολη και να αυξάνεται η πολυπλοκότητα στο κομμάτι του δικτύου. Δυστυχώς δεν υπάρχουν σαφείς προδιαγραφές για τον τρόπο με τον οποίο οι διαχειριστές των δικτύων θα πρέπει να αναπτύσσουν και να εφαρμόζουν πολιτικές ασφάλειας για τον τεμαχισμό δικτύου. Η εσφαλμένη διαχείριση τμημάτων δικτύου μπορεί να επιτρέψει σε κακόβουλους χρήστες να έχουν πρόσβαση σε δεδομένα από διαφορετικά τμήματα ή να αρνηθούν την πρόσβαση σε χρήστες με δικαιώματα σύνδεσης.

Δικτύωση που καθορίζεται από λογισμικό (Software Defined Networking): Το SDN είναι μια αρχιτεκτονική για την αυτόματη διαμόρφωση διαδρομών και ροών σε ένα δίκτυο, κυρίως χρησιμοποιώντας έναν ελεγκτή SDN. Ενώ το SDN βελτιώνει την ευελιξία του δικτύου και διευκολύνει τη διαχείρισή του, οι κακόβουλοι χρήστες μπορούν

να ενσωματώσουν κώδικα σε εφαρμογές ελεγκτών SDN για να περιορίσουν το εύρος ζώνης και να επηρεάσουν αρνητικά τις λειτουργίες του.

Υπολογισμός άκρων πολλαπλής πρόσβασης : Το Multi-Access Edge Computing μεταμορφώνει τον τρόπο επεξεργασίας και αποθήκευσης των δεδομένων μετακινώντας ορισμένες βασικές λειτουργίες δικτύου πιο κοντά στον τελικό χρήστη και μάλιστα στην άκρη του δικτύου. Αντί να βασίζεται σε μια κεντρική τοποθεσία που μπορεί να απέχει εκατοντάδες χιλιόμετρα, ο χρήστης έχει πιο άμεση πρόσβαση στη διαχείριση. Στην περίπτωση αυτή η εισαγωγή μη αξιόπιστων εξαρτημάτων 5G θα μπορούσε να εκθέσει τα βασικά στοιχεία του δικτύου σε κινδύνους που δημιουργούνται από ευπάθειες λογισμικού και υλικού, πλαστά εξαρτήματα και ελαττωματικά εξαρτήματα που προκαλούνται από κακές διαδικασίες κατασκευής ή συντήρησης.

Κοινή χρήση φάσματος (Spectrum Sharing): Τα συστήματα 5G για να αξιοποιήσουν τις δυνατότητές τους, απαιτούν ένα σύνολο συχνοτήτων φάσματος (χαμηλή, μεσαία και υψηλή συχνότητα). Αυτό γιατί κάθε τύπος συχνότητας προσφέρει μοναδικά οφέλη και προκλήσεις. Με έναν συνεχώς αυξανόμενο αριθμό συσκευών που προσπαθούν να έχουν πρόσβαση στο ίδιο φάσμα, η κοινή χρήση φάσματος μπορεί να παρέχει ευκαιρίες σε κακόβουλους χρήστες να μπλοκάρουν ή να παρέμβουν σε σημαντικές διαδρομές επικοινωνίας.

Υποδομές παλαιού τύπου επικοινωνιών: Ενώ η υποδομή του δικτύου 5G έχει σχεδιαστεί για να είναι πιο ασφαλής, δυστυχώς πολλές από τις προδιαγραφές ασφαλείας και τα πρωτόκολλα από την υποδομή επικοινωνιών του 4G υποστηρίζονται και σε δίκτυα 5G. Αυτή η παλαιού τύπου υποδομή επικοινωνιών περιέχει εξ αρχής ευπάθειες που, εάν δεν αντιμετωπιστούν, μπορούν να κληρονομηθούν στα δίκτυα 5G. [25]

5.3 Σενάρια απειλών πολιτικής και προτύπων.

5.3.1 Επιρροή Κρατών στα πρότυπα 5G.

Γενική εικόνα: Η επιρροή από τα κράτη σε συγκεκριμένους κλάδους της πληροφορικής ή αναδυόμενα τεχνολογικά πρότυπα, (π.χ. αυτόνομα οχήματα,

υπολογιστές αιχμής, τηλεϊατρική) μπορεί να επηρεάσει αρνητικά την ισορροπία στην αγορά του 5G, περιορίζοντας τη διαθεσιμότητα αξιόπιστων προμηθευτών και οδηγώντας σε μια κατάσταση αβεβαιότητας. Τα κράτη ενδέχεται να επιδιώξουν την έγκαιρη υιοθέτηση αναδυόμενων τεχνολογιών για να αυξήσουν την παγκόσμια επιρροή τους στις τεχνολογίες του 5G. Στόχος είναι να περάσουν σε ένα περιβάλλον στο οποίο οι εταιρείες τους αναγκάζονται να χρησιμοποιούν μη αξιόπιστα στοιχεία στα δίκτυά τους λόγω πρόχειρου σχεδιασμού.

Σενάριο: Ο τομέας της υγειονομικής περίθαλψης αναγκάζεται να υιοθετήσει πρότυπα που αναπτύχθηκαν από ένα κράτος που ωφελούν στην διαδικασία παραγωγής και στο διαδίκτυο. Τα νοσοκομεία αρχίζουν να υιοθετούν την τήλε χειρουργική για να παρέχουν καλύτερη υποστήριξη σε απομακρυσμένες και μειονεκτούσες κοινότητες, καθώς και για να ανταποκριθούν στην αυξανόμενη ζήτηση για την αναδυόμενη ιατρική υπηρεσία. Το ίδιο κράτος ξεκίνησε την ανάπτυξη υλικού και λογισμικού τήλε χειρουργικής πριν από αρκετά χρόνια και είναι πλέον πρωτοπόρος ηγέτης στον τομέα. Τα νοσοκομεία αναγκάζονται είτε να χρησιμοποιούν τις μη αξιόπιστες τεχνολογίες τους είτε να χρησιμοποιούν τεχνολογίες από αξιόπιστους παρόχους που είναι κατασκευασμένες σύμφωνα με τα ισχύοντα πρότυπα του εθνικού κράτους. [25]

5.3.2 Πανεπιστημιακή εφαρμογή προαιρετικού ελέγχου ασφαλείας 5G.

Γενική εικόνα: Οι πάροχοι επικοινωνιών που επιλέγουν να μην εφαρμόσουν προαιρετικούς ελέγχους ασφαλείας θα έχουν πιθανώς περισσότερες ευπάθειες και θα διατρέχουν μεγαλύτερο κίνδυνο για επιθέσεις στο διαδίκτυο. Σε αυτές τις περιπτώσεις, οι φορείς των κρατών, οι οποίοι έχουν συμβάλει στην ανάπτυξη ελέγχων ασφάλειας ή έχουν επίγνωση των τρωτών σημείων σε συστήματα στα οποία δεν έχουν εφαρμοστεί οι έλεγχοι, ενδέχεται να στοχεύουν αυτές τις οντότητες. Ως αποτέλεσμα, οι κακόβουλοι χρήστες θα μπορούσαν να εντοπίσουν και να χρησιμοποιήσουν μεθόδους για να επωφεληθούν από τρύπες ασφαλείας σε ιδιωτικά δίκτυα που δεν θέτουν σε εφαρμογή αυτούς τους ελέγχους.

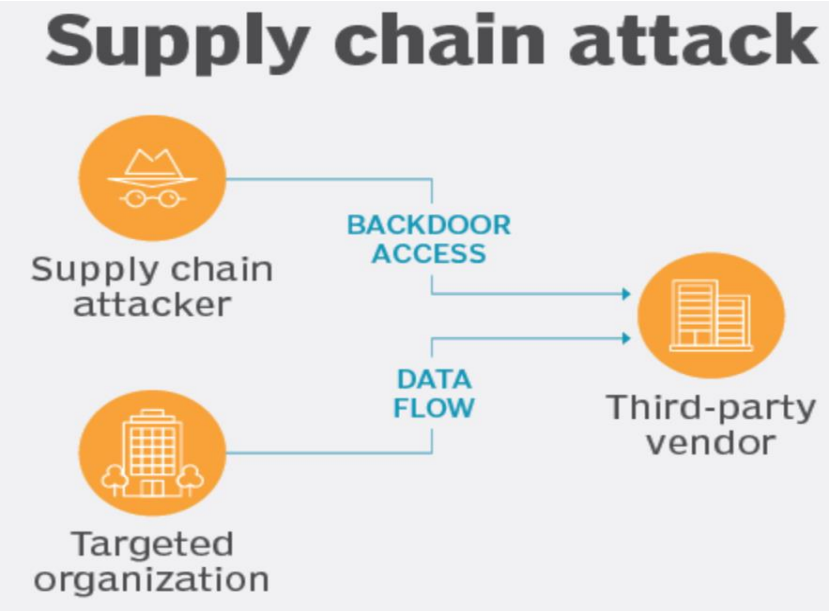
***Σενάριο*:** Ένα πανεπιστήμιο αρχίζει να αντικαθιστά τις Wi-Fi υποδομές του και εφαρμόζει ένα δίκτυο 5G σε όλη τη πανεπιστημιούπολή του, αλλά δεν διαμορφώνει ή διατηρεί επαρκώς όλους τους προτεινόμενους ελέγχους ασφαλείας. Πολλοί από τους προαιρετικούς ελέγχους ασφαλείας ακολουθούνται και υποστηρίζονται από εταιρείες

τηλεπικοινωνιών και από άλλες επιχειρήσεις που τους υιοθετούν. Η απόφαση του πανεπιστημίου να μην εφαρμόσει όλους τους ελέγχους ασφαλείας οδηγεί σε σημαντικά κενά στο εσωτερικό δίκτυό του (intranet). Ένας κακόβουλος χρήστης στοχεύει και δοκιμάζει την έλλειψη αυτών των ελέγχων και τους εκμεταλλεύεται εντός του δικτύου 5G του πανεπιστημίου με δυσάρεστες συνέπειες. [25]

5.4 Σενάρια απειλών στην εφοδιαστική αλυσίδα.

5.4.1 Εφαρμογή πλαστών εξαρτημάτων.

Γενική εικόνα: Τα πλαστά και ελλαττωματικά εξαρτήματα εισάγονται στο στάδιο κατασκευής ή διανομής εξαρτημάτων στην αλυσίδα εφοδιασμού προκειμένου να επηρεαστεί αρνητικά και σκόπιμα ένα σύνολο πελατών. Τα πλαστά ανταλλακτικά μοιάζουν με κανονικά ανταλλακτικά και αποτελούν μια μορφή απάτης. Στόχος είναι να βρεθούν πελάτες που αναζητούν ανταλλακτικά υψηλής ποιότητας από αξιόπιστους κατασκευαστές και αντί αυτού τους πωλούνται εν αγνοία τους κατώτερα ή ελαττωματικά ανταλλακτικά. Η εξαπάτηση ενός απατεώνα είναι η διανομή ενός πλαστού και ελλαττωματικού εξαρτήματος, το οποίο έχει προβλήματα ή κακόβουλες λειτουργίες που είναι άγνωστες στον κατασκευαστή ή τον διανομέα ή τον τελικό πελάτη. [24]



Εικόνα 26: Απειλή στην εφοδιαστική αλυσίδα. [25]

***Σενάριο*:** Ένας κακόβουλος χρήστης εντοπίζει έναν κρατικό εργολάβο που παρέχει υλικά πληροφορικής και τηλεπικοινωνιών και προσπαθεί να του πουλήσει ελλαττωματικά ή πλαστά προϊόντα σε μειωμένες τιμές. Ενώ ο ανάδοχος είναι νόμιμος και έχει να χάσει τα περισσότερα από τα παραποιημένα προϊόντα, δεν γνωρίζει ότι υπάρχει πιθανό πρόβλημα και δεν διενεργεί αρχική ανάλυση των πιθανών κινδύνων παραποίησης που υπάρχουν στον κλάδο του. Για να εξοικονομήσει χρήματα, ο ανάδοχος αγοράζει τα πλαστά και ελλαττωματικά εξαρτήματα από τον κακόβουλο προμηθευτή και τα εισάγει στο προϊόν του. Δυστυχώς το πλαστό ανταλλακτικό έχει περάσει απαρατήρητο στο στάδιο των λειτουργικών δοκιμών και τίθεται στην γραμμή παραγωγής. Η τελική επίδραση στο παραγόμενο σύστημα και στον τελικό πελάτη μπορεί να επηρεάσει την απόδοση του συστήματος, τη μη διαθεσιμότητα σημαντικών υπηρεσιών ή και να οδηγήσει σε απώλεια δεδομένων. [24]

5.4.2 Ακούσια υιοθέτηση μη εμπιστευτικών στοιχείων.

Γενική εικόνα: Μια επίθεση στην αλυσίδα εφοδιασμού λογισμικού συμβαίνει όταν προστίθεται σκόπιμα κακόβουλος κώδικας σε ένα στοιχείο που αποστέλλεται στους χρήστες-στόχους. Ο κακόβουλος κώδικας μπορεί να εισαχθεί στο σύστημα με πολλούς διαφορετικούς τρόπους, όπως μέσω παραβίασης του αποθετηρίου πηγαίου κώδικα, την κλοπή κλειδιών υπογραφής, την διείσδυση σε τοποθεσίες διανομής ή με τρόπους κοινωνικής μηχανικής. Ως μέρος ενός εξουσιοδοτημένου και κανονικού καναλιού διανομής, οι πελάτες εν αγνοία τους αποκτούν και αναπτύσσουν αυτά τα παραβιασμένα στοιχεία στα συστήματα και τα δίκτυά τους. Αυτός ο κακόβουλος κώδικας συνήθως δεν διακόπτει τις κανονικές λειτουργίες και ενδέχεται να μην ενεργοποιηθεί μέχρι να γίνει η ενεργοποίηση, με αποτέλεσμα να παραμένει κρυφός από τις τυπικές δοκιμές στο στάδιο ελέγχου εφαρμογών και λογισμικού.

***Σενάριο*:** Μια εταιρεία τηλεπικοινωνιών και δικτύων αγοράζει λογισμικό διαχείρισης βασικών συστημάτων δικτύου από έναν αξιόπιστο προμηθευτή. Ωστόσο, ένα από τα στοιχεία που χρησιμοποιείται στο προϊόν έχει παραβιαστεί και περιέχει κακόβουλο κώδικα. Αυτό γίνεται χωρίς να το γνωρίζει ο αξιόπιστος πάροχος. Αυτή η απειλή που προκύπτει από παραβίαση εντός της αλυσίδας εφοδιασμού επηρεάζει τον τελικό χρήστη και φυσικά το τελικό προϊόντος ή την παρεχόμενη υπηρεσία. Όσο πιο βαθιά

εμφανίζεται στην αλυσίδα εφοδιασμού η παραβίαση, τόσο πιο δύσκολο είναι να εντοπιστεί εκ των προτέρων. Αυτή η ευπάθεια μπορεί να χρησιμοποιηθεί από τον κακόβουλο χρήστη ως μέρος μιας μεγαλύτερης αλυσίδας επίθεσης που χρησιμοποιεί τον κακόβουλο κώδικα για να αποκτήσει πρόσβαση στο κεντρικό δίκτυο της υποδομής δικτύου και τηλεπικοινωνιών. [25]

5.5 Σενάρια απειλών αρχιτεκτονικής συστημάτων 5G.

5.5.1 Ευπάθεια firmware στο multi-access edge.

Γενική εικόνα Σε αντίθεση με τις συνήθεις αρχιτεκτονικές δικτύου, το Multi-Access Edge Compute (MEC) παρέχει βασικές λειτουργίες κυκλοφορίας όπως η επεξεργασία και αποθήκευση δεδομένων στο τελευταίο μίλι των τηλεπικοινωνιακών δικτύων. Η παρουσία στοιχείων του συστήματος, όπως hypervisors, λειτουργικά συστήματα και εφαρμογές, μπορεί να παρέχει σε κακόβουλους χρήστες πρόσθετες μορφές επιθέσεων για την εκμετάλλευση και την καταστροφή σημαντικών δεδομένων. Μη αξιόπιστα στοιχεία ή malware που έχει εισαχθεί στο MEC ενδέχεται να επηρεάσει το απόρρητο των χρηστών παρέχοντας στους κακόβουλους χρήστες τη δυνατότητα να κλωνοποιούν συσκευές κινητής τηλεφωνίας και να κάνουν πλαστοπροσωπία των τελικών χρηστών. Οι κακόβουλοι χρήστες στη συνέχεια μπορούν να χρησιμοποιήσουν μη αξιόπιστα στοιχεία ή κακόβουλο λογισμικό για να αποκτήσουν πρόσβαση στο MEC και στα στοιχεία τελικού χρήστη, αξιοποιώντας τα για να αποκτήσουν πρόσβαση στο ευρύτερο δίκτυο ράδιο πρόσβασης.

Σενάριο**:** Μια ευπάθεια firmware επιτρέπει σε έναν επιτιθέμενο να αποκτήσει σταθερή βάση στο σύστημα υπολογιστικού άκρου, κάτι που το κάνει να αρνηθεί την πρόσβαση στα δεδομένα και να επηρεάσει την εξαιρετικά χαμηλή απόκριση που απαιτείται από την τεχνολογία του 5G. Ο κακόβουλος χρήστης μπορεί να χρησιμοποιήσει αυτήν την πρόσβαση για να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του δικτύου κλέβοντας ευαίσθητα δεδομένα αισθητήρων και εξοπλισμού χρήστη. Επιπλέον ροές δεδομένων τροποποιούνται και υπάρχει άρνηση στην πρόσβαση σε ορισμένα δεδομένα ή ροές αισθητήρων. Ο κακόβουλος χρήστης έχει τώρα το εύρος ζώνης για να αποκτήσει πλήρη πρόσβαση στο ράδιο δίκτυο και

είναι σε θέση να κλωνοποιήσει τις συσκευές των τελικών χρηστών προς όφελός του. [24]

5.5.2 Κληρονομούμενες ευπάθειες από τα δίκτυα 4G.

Γενική εικόνα: Το 5G βασίζεται σε προηγούμενες γενιές ασύρματων δικτύων και αρχικά ενσωματώνεται με τα δίκτυα 4G που περιέχουν ευπάθειες παλαιού τύπου. Ενώ οι τεχνολογίες 5ης γενιάς σχεδιάζονται για να είναι πιο ασφαλείς από τις προηγούμενες γενιές δικτύων κινητής, ενδέχεται να είναι ευάλωτες σε ορισμένες παλαιού τύπου αδυναμίες. Τέτοιες αδυναμίες είναι οι επιθέσεις στο Signaling System 7 (SS7) και οι ευπάθειες πρωτοκόλλου διαμέτρου.

***Σενάριο*:** Ένας επιτιθέμενος αποκτά πρόσβαση σε μια κυψέλη 5G κοντά σε γραφείο της κυβέρνησης και διαμορφώνει την κυψέλη ώστε να επιτρέπει την πλαστογράφηση 4G δικτύου. Στη συνέχεια, ο επιτιθέμενος προκαλεί μια υποβάθμιση του δικτύου 5G σε μια ευάλωτη διαμόρφωση 4G. Με τον τρόπο αυτό τους επιτρέπει να χρησιμοποιούν τρωτά σημεία στο SS7 για να αποκτήσουν πρόσβαση σε στοιχεία υποδομών πληροφορικής και τηλεπικοινωνιών που χρησιμοποιούν οι υπάλληλοι στο κοντινό κυβερνητικό γραφείο. Ο επιτιθέμενος έτσι μπορεί στη συνέχεια να χρησιμοποιήσει αυτές τις πληροφορίες για να αποκτήσει περαιτέρω πρόσβαση σε πιο διαβαθμισμένα δίκτυα, έχοντας τη δυνατότητα να αποκτήσει πρόσβαση σε πιο ευαίσθητα δεδομένα. [25]

ΚΕΦΑΛΑΙΟ 6ο

6.1 Νέες ευπάθειες στα δίκτυα 5G.

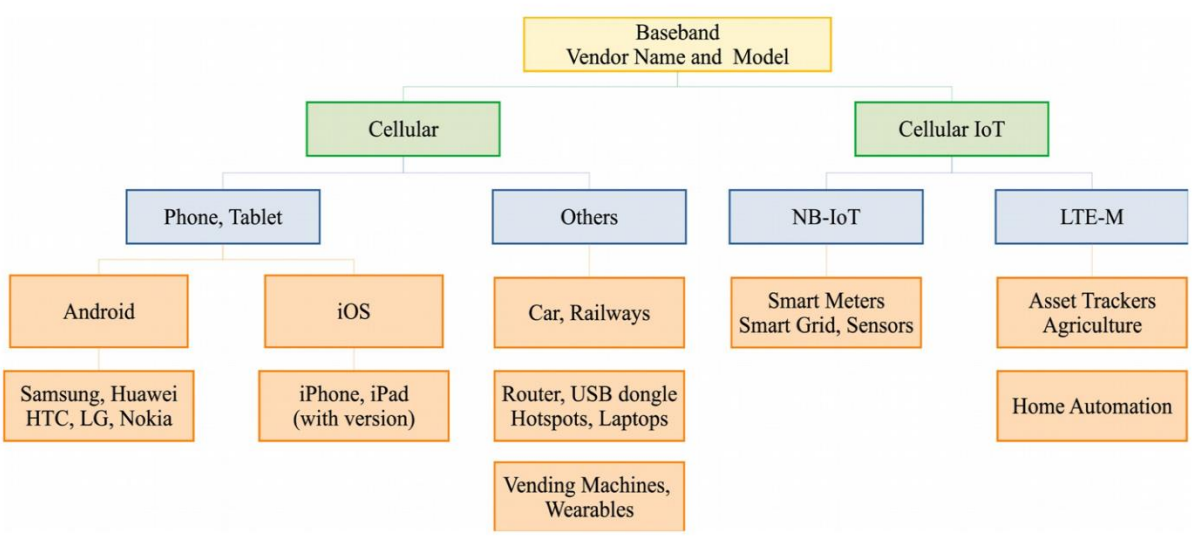
Η ασφάλεια στα δίκτυα 5G έχει εξελιχθεί και είναι πιο αποτελεσματική από τις προηγούμενες γενιές. Σε αυτήν την ενότητα, μελετάμε τα χαρακτηριστικά ασφαλείας των ραδιοδικτύων 5G και αποκαλύπτουμε νέα τρωτά σημεία που επηρεάζουν τόσο την υποδομή του χρήστη όσο και τις τελικές συσκευές. Δείχνουμε πώς αυτές οι νέες ευπάθειες στα πρότυπα ασφαλείας 5G - 4G μπορούν να γίνουν exploit χρησιμοποιώντας πλατφόρμες υλικού και λογισμικού χαμηλού κόστους. Συγκεκριμένα, αποκαλύπτουμε ζητήματα υλοποίησης σε εκατοντάδες σταθμούς βάσης 4G σε όλο τον κόσμο και σε εμπορικά διαθέσιμα πρωτόκολλα NB-IoT που μπορούν να χρησιμοποιηθούν για την εγκατάσταση επιθέσεων εξάντλησης της μπαταρίας (Battery draining attacks), Identification attacks και μείωσης προσφοράς (Bidding down attacks). Οι επιθέσεις αυτές επηρεάζουν το εύρος από συσκευές LTE υψηλής ταχύτητας gigabit έως συσκευές NB-IoT.

Οι συσκευές κινητής τηλεφωνίας υποστηρίζουν διάφορα τεχνικά χαρακτηριστικά και υπηρεσίες για τα δίκτυα 2G, 3G, 4G και τα σύγχρονα δίκτυα 5G. Για παράδειγμα, αυτά τα τεχνικά χαρακτηριστικά περιέχουν πληροφορίες φυσικού επιπέδου (physical layer), πληροφορίες radio protocol, αλγόριθμο ασφαλείας, carrier aggregation bands και τύπο υπηρεσιών όπως GSM-R, Voice over LTE κ.λπ. Στο πλαίσιο της τυποποίησης κινητής τηλεφωνίας, αυτά τα τεχνικά χαρακτηριστικά και οι υπηρεσίες δικτύου ονομάζονται δυνατότητες συσκευής (device capabilities) και ανταλλάσσονται με το δίκτυο κατά τη φάση εγγραφής και σύνδεσης της συσκευής.

Σε αυτήν την ενότητα, μελετάμε πληροφορίες σχετικά με τις δυνατότητες της συσκευής που καθορίζονται για συσκευές 4G και 5G και τον ρόλο τους στη δημιουργία συσχέτισης ασφαλείας μεταξύ της συσκευής και του δικτύου. Τα συμπεράσματα μας αποκαλύπτουν ότι οι δυνατότητες της συσκευής ανταλλάσσονται με το δίκτυο πριν από το στάδιο ελέγχου ταυτότητας χωρίς καμία προστασία και δεν επαληθεύονται από το δίκτυο. Κατά συνέπεια, οι πληροφορίες ικανότητας της συσκευής μπορούν να χρησιμοποιηθούν καταχρηστικά από έναν αντίπαλο για την εκτέλεση πολλών επιθέσεων κατά του συνδρομητή κινητής τηλεφωνίας. Στη συνέχεια παρουσιάζουμε τρεις κατηγορίες επιθέσεων.

α) Επιθέσεις αναγνώρισης (Identification attacks): Επιτρέπουν σε έναν αντίπαλο να ανακαλύψει συσκευές στο δίκτυο κινητής τηλεφωνίας και να αποκαλύψει τα χαρακτηριστικά υλικού και λογισμικού (όπως μοντέλο, κατασκευαστή, έκδοση, επεξεργαστής, μνήμη) και εφαρμογές που εκτελούνται σε αυτές.

Στις επιθέσεις αναγνώρισης, το Device Fingerprinting ,δηλαδή η ιχνηλάτηση συσκευής, έρχεται για να προσδιορίσει τον τύπο των συσκευών σε ένα δίκτυο κινητής τηλεφωνίας και να εκτιμήσει τις υποκείμενες εφαρμογές. Ξεκινάμε αναλύοντας τις δυνατότητες του εξοπλισμού χρήστη και χτίζουμε ένα μοντέλο αναφοράς χρησιμοποιώντας ένα σύνολο γνωστών συσκευών και τεχνικών για να διακρίνουμε διάφορες συσκευές και εφαρμογές. Στη συνέχεια χρησιμοποιούμε το μοντέλο αναφοράς μας για να εκτελέσουμε επίθεση χαρτογράφησης δικτύου κινητής τηλεφωνίας (Mobile Nmap). Παρουσιάζουμε διάφορα επίπεδα αναγνώρισης στο ακόλουθο σχήμα. Είτε είναι ενεργός είτε είναι παθητικός ο επιτιθέμενος, αποκτούμε βασικές και ραδιοφωνικές δυνατότητες της συσκευής και πραγματοποιούμε την αναγνώριση.

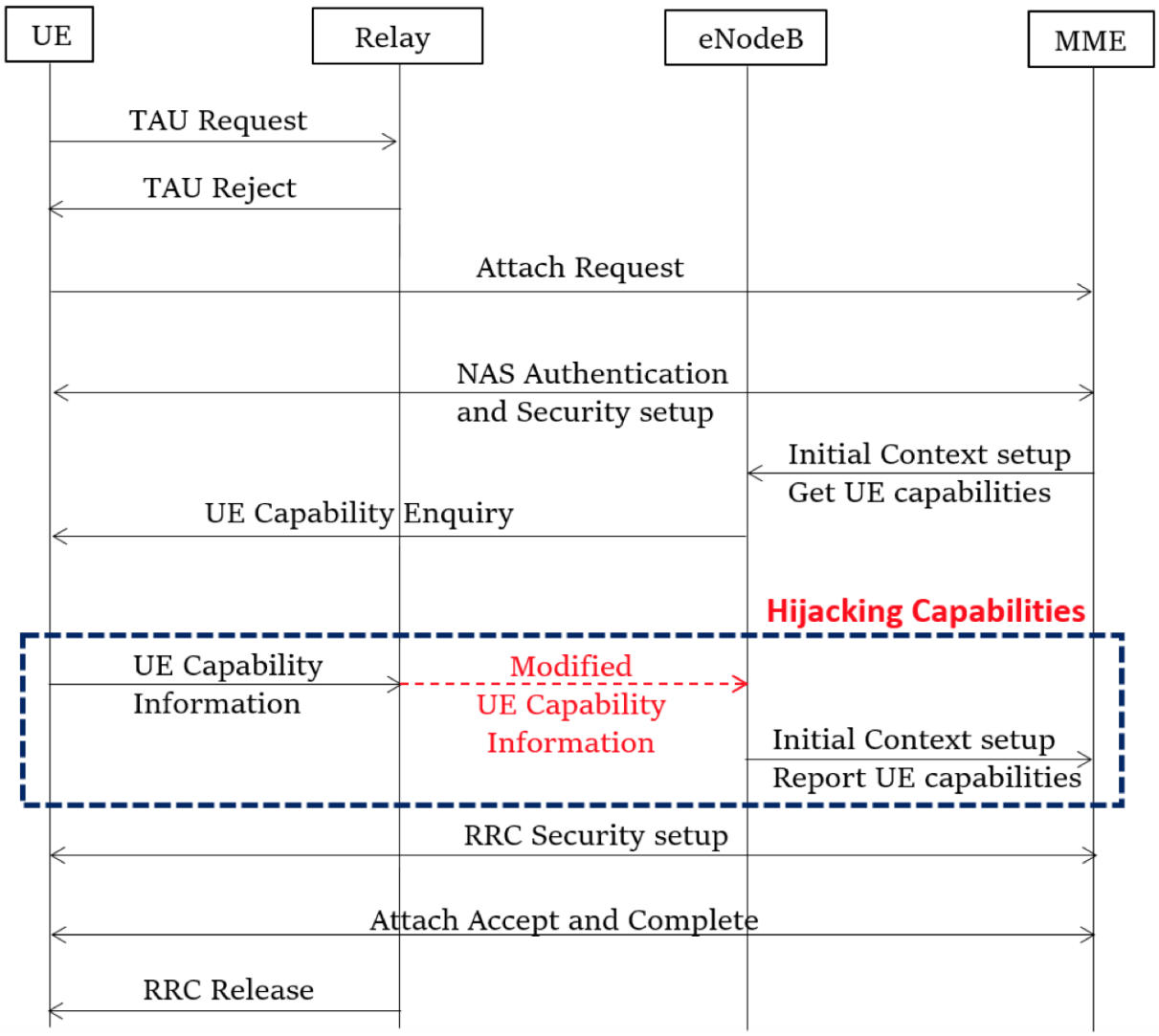


Εικόνα 27: Device Identification Levels. [24]

β) Επιθέσεις υποβάθμισης (Bidding down attacks): Παραβιάζουν τις δυνατότητες της συσκευής που εκτίθενται στη διεπαφή LTE και υποβαθμίζουν την ταχύτητα μιας συσκευής από 27 Mbps σε 3,7 Mbps και περαιτέρω αρνούνται την παροχή τις

υπηρεσίας Voice Over LTE (VoLTE) σε συνδρομητές LTE και τους υποβαθμίζουν σε 3G και 2G δίκτυα.

Στις επιθέσεις υποβάθμισης (bidding down) οι χάκερ μπορούν να χρησιμοποιήσουν συσκευές που πλαστοπροσωπούν το IMSI για να εκτελέσουν επιθέσεις DoS, αλλά αυτό δεν είναι το μόνο που μπορούν να κάνουν αυτές οι συσκευές. Μπορούν επίσης να χρησιμοποιήσουν την κατάστασή τους ως αξιόπιστοι κόμβοι δικτύου για να πραγματοποιήσουν επιθέσεις MITM, όπου στέλνουν κακόβουλες εντολές σε συνδεδεμένες συσκευές. Μια τέτοια επίθεση αναγκάζει τις συσκευές να υποπέσουν σε πρωτόκολλα δικτύου χαμηλότερης ποιότητας, προκαλώντας υποβάθμιση της ποιότητας της υπηρεσίας τους. Αυτή θα μπορούσε να είναι μια εξαιρετικά επιζήμια επίθεση εναντίον εταιρικών δικτύων.

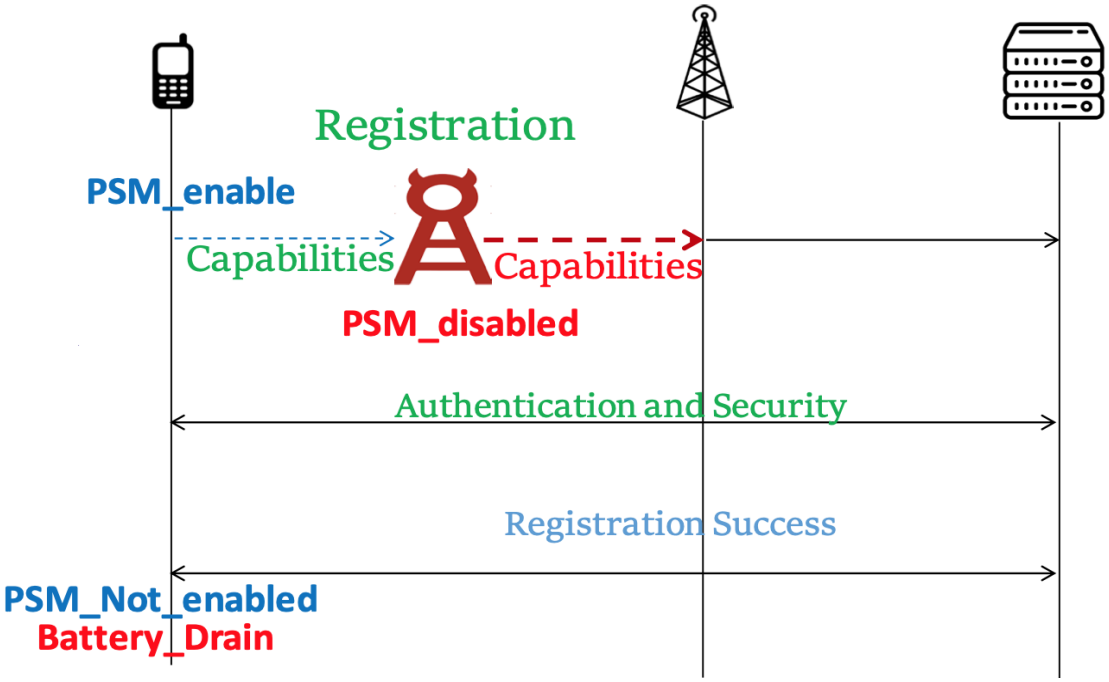


Εικόνα 28: Device Bidding down attack TAU=Tracking Area Updating RRC=Radio Resource Control [24]

Λόγω της διαμόρφωσης των φορέων εκμετάλλευσης δικτύων κινητής τηλεφωνίας ή των υλοποιήσεων προμηθευτή, το eNodeB ζητά τις δυνατότητες ασύρματης πρόσβασης του UE πριν από τη ρύθμιση ασφαλείας RRC. Αυτό επιτρέπει σε ένα MitM (Man-in-the-Middle) να αλλάξει τις πληροφορίες ικανότητας UE που αποστέλλονται από το UE, όπως φαίνεται στο πάνω σχήμα. Η επίθεση είναι επίμονη αφού οι δυνατότητες αποθηκεύονται στο MME (Mobility Management Entity) και επαναχρησιμοποιούνται από το eNodeB για κάθε συναλλαγή του UE.

γ) Επιθέσεις εξάντλησης μπαταρίας (Battery draining attacks): στοχεύουν τις συσκευές NB-IoT και LTE-M για να αναλύσουν τις ικανότητές τους εξοικονόμησης ενέργειας και να εξαντλήσουν τη διάρκεια ζωής της μπαταρίας τους 5 φορές πιο γρήγορα από την αναμενόμενη διάρκεια ζωής. Στις επιθέσεις εξάντλησης μπαταρίας

(Battery draining attacks) εξαντλούμε την μπαταρία των συσκευών NB-IoT χαμηλής κατανάλωσης με το να είμαστε MITM κόμβος στη διεπαφή του LTE. Στην επίθεση, το σήμα αναμετάδοσης μας τροποποιεί τα περιεχόμενα του μηνύματος Attach Request όπως φαίνεται στην εικόνα παρακάτω. Ο εισβολέας απενεργοποιεί τη λειτουργία εξοικονόμησης ενέργειας από το αίτημα επισύναψης και επομένως δεν μπορεί να λάβει μήνυμα PSM ON (Power Saving Mode) από το δίκτυο. Ως εκ τούτου, η μπαταρία αδειάζει συνεχώς λόγω της χρήσης της για μετρήσεις σήματος και άλλες εσωτερικές δραστηριότητες από το μόντεμ, καθώς δεν είναι απενεργοποιημένη. Έτσι η διάρκεια ζωής της μπαταρίας μειώνεται κατά 5 φορές. [24]



Εικόνα 29: Battery draining attack [24]

6.2 Μελέτη ευπαθειών

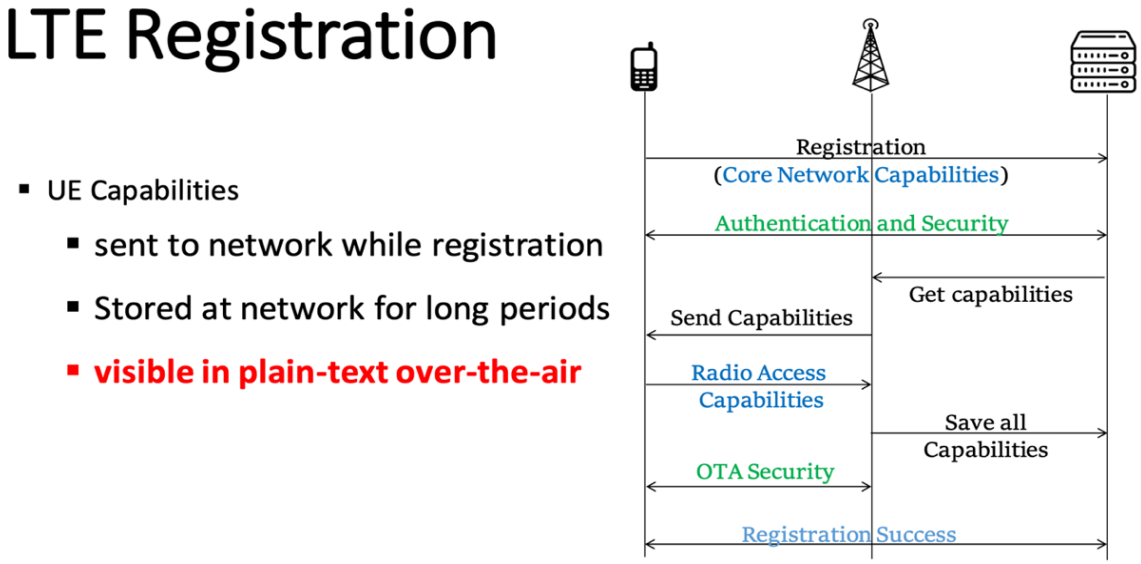
Εντοπίσαμε τρία τρωτά σημεία στη διαδικασία του LTE registration. Ο επιτιθέμενος εκμεταλλεύεται τις δυνατότητες UE capabilities που αποστέλλονται στο δίκτυο κατά τις διαδικασίες εγγραφής και περιγράφονται ως εξής.

• **Πρώτον**, τόσο οι δυνατότητες πρόσβασης στο κεντρικό δίκτυο όσο και οι δυνατότητες πρόσβασης ραδιοσυχνότητας μπορούν να αποκτηθούν από ένα UE χωρίς να καθιερωθεί έλεγχος ταυτότητας. Αυτό επιτρέπει σε έναν ενεργό ή παθητικό

επιτιθέμενο να αποκτήσει όλες τις δυνατότητες μιας συσκευής χρήστη. Έτσι εκμεταλλευόμενος αυτήν την ευπάθεια πραγματοποιεί επιθέσεις αναγνώρισης τύπου συσκευής.

• **Δεύτερον**, το μήνυμα επισύναψης αιτήματος αποστέλλεται πάντα μη κρυπτογραφημένο από τη συσκευή στο δίκτυο, αλλά μπορεί να προστατεύεται η ακεραιότητα σε περίπτωση υπάρχοντος περιβάλλοντος ασφαλείας στη συσκευή. Ωστόσο, η διαδικασία εγγραφής δεν διακόπτεται ακόμη και αν η επαλήθευση ακεραιότητας αποτύχει. Σε μια τέτοια περίπτωση, το περιεχόμενο του μηνύματος Attach Request είναι ευάλωτο σε επιθέσεις injection ή τροποποίησης. Συγκεκριμένα, οι δυνατότητες του βασικού δικτύου μέσα σε αυτό το μήνυμα μπορούν να παραβιαστούν από έναν αντίπαλο. Η τροποποίηση ορισμένων δυνατοτήτων του βασικού δικτύου μπορεί να προκαλέσει επιθέσεις εξάντλησης ενέργειας (power drain attacks) σε συσκευές NB-IoT.

Τρίτον, οι φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας ζητούν τις δυνατότητες ασύρματης πρόσβασης από τη συσκευή πριν από τη ρύθμιση ασφαλείας RRC (Radio Resource Control). Ως αποτέλεσμα, οι δυνατότητες του εξοπλισμού χρήστη μεταφέρονται σε απλό κείμενο και ένας αντίπαλος μπορεί να παραβιάσει αυτές τις δυνατότητες. [24]



Εικόνα 30: Διαδικασία LTE Registration. [24]

Μια επίθεση πλευρικού καναλιού (side channel attack) είναι μια εκμετάλλευση ασφαλείας που στοχεύει στη συλλογή πληροφοριών, ή στο να επηρεάσει την εκτέλεση του προγράμματος ενός συστήματος. Αντί δηλαδή να στοχεύει απευθείας το πρόγραμμα ή τον κώδικά του, εκμεταλλεύεται έμμεσα επιδράσεις του συστήματος ή του υλικού του. Συνηθέστερα, αυτές οι επιθέσεις στοχεύουν στη διείσδυση ευαίσθητων πληροφοριών, συμπεριλαμβανομένων των κρυπτογραφικών κλειδιών, μετρώντας τις συμπωματικές εκπομπές υλικού. Μια επίθεση πλευρικού καναλιού μπορεί επίσης να αναφέρεται ως επίθεση πλευρικής γραμμής ή επίθεση υλοποίησης.

Η υιοθέτηση της Τέταρτης Γενιάς Long Term Evolution (4G LTE)—το de facto πρότυπο για τις κυψελοειδείς τηλεπικοινωνίες—έχει σημειώσει σταθερή ανάπτυξη τα τελευταία χρόνια, αντικαθιστώντας τις προηγούμενες γενιές λόγω της υπόσχεσής της για βελτιωμένες διασφαλίσεις (π.χ. υψηλότερο εύρος ζώνης, αξιόπιστη συνδεσιμότητα, βελτιωμένη ασφάλεια). Επιπλέον, η επικείμενη ανάπτυξη του κυψελοειδούς δικτύου πέμπτης γενιάς (5G) έχει δημιουργήσει μεγάλο ενθουσιασμό τόσο στη βιομηχανία όσο και στον ακαδημαϊκό κόσμο, ιδίως λόγω της υπόσχεσής του να ενεργοποιήσει νέες εφαρμογές όπως έξυπνα οχήματα και εξ αποστάσεως ρομποτική χειρουργική. [24]

Η σελιδοποίηση είναι ένα από τα πολλά σημαντικά πρωτόκολλα σε δίκτυα κινητής τηλεφωνίας που επιτρέπει σε μια κινητή συσκευή - που δεν επικοινωνεί ενεργά με έναν σταθμό βάσης - να ανταποκρίνεται σε μια τηλεφωνική κλήση ή ένα SMS ή σε τυχόν εισερχόμενα μηνύματα για τη συσκευή. Το πρωτόκολλο κυψελοειδούς σελιδοποίησης (cellular paging protocol) προσπαθεί να εξισορροπήσει την κατανάλωση ενέργειας μιας κινητής συσκευής και την ποιότητα της υπηρεσίας, επιτρέποντας στη συσκευή να πραγματοποιεί μόνο περιοδικές εκπομπές για εκκρεμείς υπηρεσίες στην κατάσταση αδράνειας και χαμηλής κατανάλωσης. Για μια δεδομένη συσκευή κινητής τηλεφωνίας και δίκτυο εξυπηρέτησης, οι ακριβείς χρονικές περίοδοι κατά τις οποίες η συσκευή πραγματοποιεί εκπομπές για υπηρεσίες (που ονομάζεται περίσταση σελιδοποίησης) καθορίζονται βάσει σχεδίου στο κυψελοειδές πρωτόκολλο 4G/5G.

Μια συσκευή, εξοπλισμένη με κάρτα SIM, έχει μια μοναδική διεθνή ταυτότητα συνδρομητή κινητής τηλεφωνίας (International Mobile Subscriber Identity). Το IMSI

αποθηκεύεται σε μια κάρτα SIM και δεν αλλάζει. Προσδιορίζει τη χώρα, τον πάροχο και τον χρήστη. Με αυτές τις πληροφορίες, το άτομο που παρακολουθεί αυτήν την κίνηση μπορεί να αναγνωρίσει και να εντοπίσει τον χρήστη του τηλεφώνου στο ελάχιστο και ενδεχομένως να υποκλέψει και να πλαστογραφήσει το traffic του χρήστη.

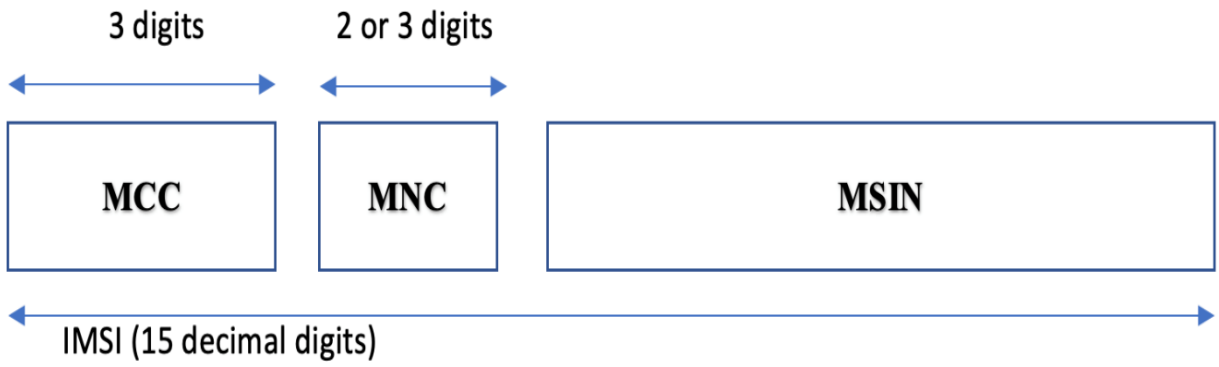
Η μόνιμη ταυτότητα για συγκεκριμένη κάρτα SIM στο 5G ονομάζεται Μόνιμος Αναγνωριστικός Συνδρομητής (Subscriber Permanent Identifier - SUPI). Το SUPI μπορεί να είναι είτε της φόρμας IMSI είτε της φόρμας αναγνωριστικού πρόσβασης δικτύου (Network Access Identifier). Για τη συζήτησή μας, εστιάζουμε στο IMSI το οποίο δεν χρησιμοποιείται μόνο στο 5G αλλά χρησιμοποιείται επίσης και στο 4G για να προσδιορίσει μοναδικά τον συνδρομητή για τον έλεγχο ταυτότητας.

Ο αριθμός IMSI είναι ένας παγκοσμίως μοναδικός αριθμός που προσδιορίζει τον χρήστη. Είναι έως και 15 ψηφία και περιλαμβάνει:

MCC (Mobile Country Code): Κωδικός χώρας κινητής τηλεφωνίας. Έχει 3 δεκαδικά ψηφία και προσδιορίζει τη χώρα του κατόχου της κινητής συσκευής.

MNC (Mobile Network Code): Κωδικός δικτύου κινητής τηλεφωνίας. Έχει 2 δεκαδικά ψηφία και προσδιορίζει το δίκτυο κινητής τηλεφωνίας.

MSIN (Mobile Subscriber Number): Αριθμός συνδρομητή κινητής τηλεφωνίας. Έχει 10 δεκαδικά ψηφία και προσδιορίζει τον συνδρομητή.



Εικόνα 31: Η δομή του αριθμού IMSI. [24]

Μια mobile συσκευή έχει επίσης μια Προσωρινή Ταυτότητα Συνδρομητή κινητής τηλεφωνίας (Temporary Mobile Subscriber Identity-TMSI), η οποία είναι η ταυτότητα που αποστέλλεται πιο συχνά μεταξύ της mobile συσκευής και του δικτύου. Το TMSI

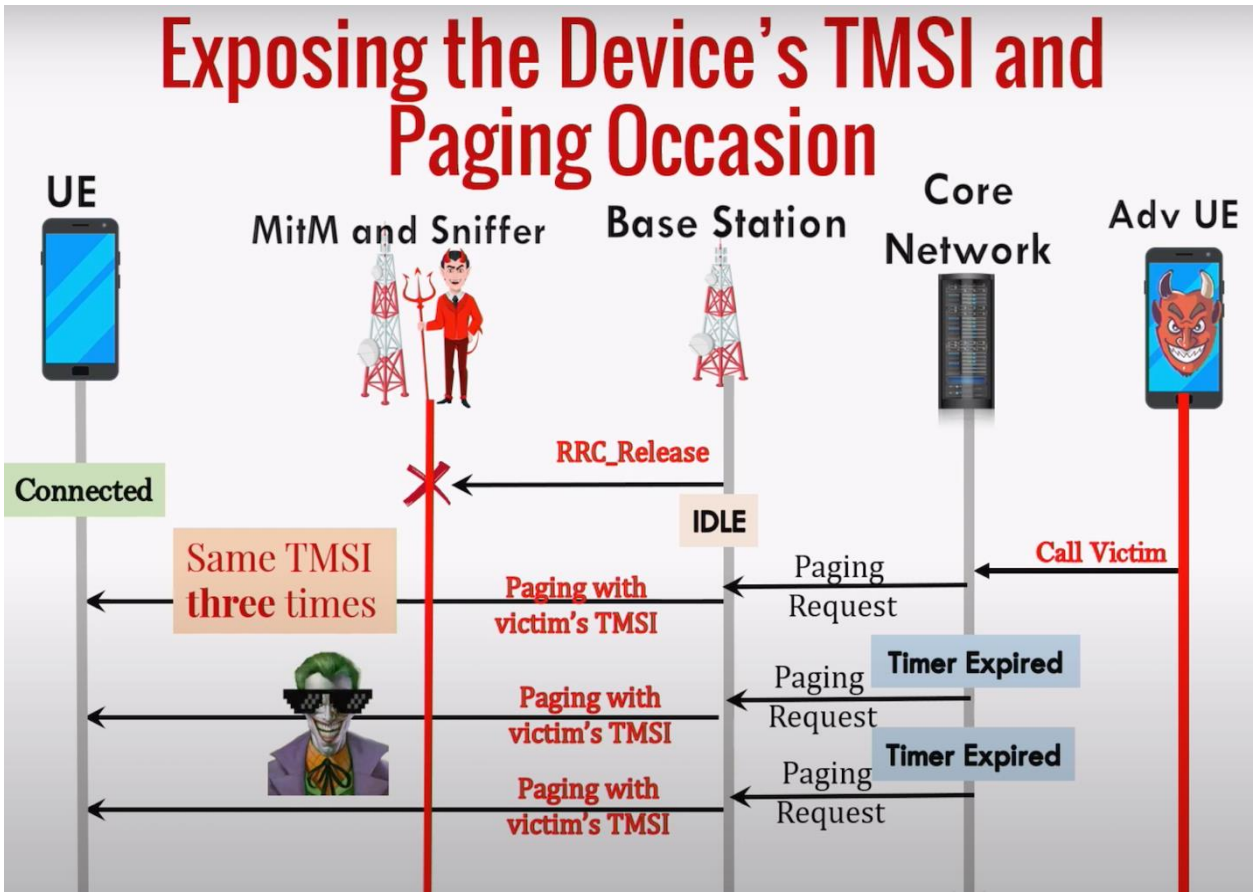
εκχωρείται τυχαία από το MME (Mobility Management Entity) σε ένα UE, όταν το UE συνδέεται για πρώτη φορά σε έναν σταθμό βάσης στην περιοχή παρακολούθησης. Το TMSI είναι τοπικό σε μια περιοχή παρακολούθησης και επομένως πρέπει να ενημερώνεται κάθε φορά που η συσκευή χρήστη μετακινείται σε μια νέα γεωγραφική περιοχή. Το MME μπορεί επίσης να ενημερώσει το TMSI μιας κινητής συσκευής εάν το επιθυμεί. Το TMSI είναι μοναδικό στην περιοχή τοποθεσίας στην οποία βρίσκεται ο συνδρομητής. Αντίστοιχα, κάθε φορά που ο συνδρομητής επισκέπτεται μια νέα περιοχή τοποθεσίας, το κεντρικό δίκτυο πρέπει να ενημερώνει την τιμή TMSI.

Όταν μια κινητή συσκευή δεν επικοινωνεί ενεργά με έναν σταθμό βάσης, εισέρχεται σε κατάσταση αδράνειας, χαμηλής κατανάλωσης ενέργειας για εξοικονόμηση ενέργειας της μπαταρίας. Όταν υπάρχει μια τηλεφωνική κλήση ή ένα μήνυμα SMS για τη συσκευή, πρέπει να ειδοποιηθεί. Αυτό επιτυγχάνεται με το πρωτόκολλο σελιδοποίησης, το οποίο προσπαθεί να επιτύχει τη σωστή ισορροπία μεταξύ της κατανάλωσης ενέργειας της συσκευής και της έγκαιρης παροχής υπηρεσιών όπως οι τηλεφωνικές κλήσεις. Όταν υπάρχει μία ή περισσότερες υπηρεσίες σε εκκρεμότητα για μια συσκευή, η οντότητα διαχείρισης κινητής τηλεφωνίας (MME) του δικτύου ζητά από τους σταθμούς βάσης να μεταδώσουν ένα μήνυμα σελιδοποίησης, το οποίο περιλαμβάνει την Προσωρινή Ταυτότητα Συνδρομητή κινητής τηλεφωνίας (TMSI) της συσκευής. Το TMSI εκχωρείται τυχαία από το MME στη συσκευή και συνιστάται να αλλάζει συχνά. [25]

Η παρουσία ενός χρήστη σε μια γεωγραφική περιοχή μπορεί να αναγνωριστεί από μια επίθεση sniffing που εκμεταλλεύεται το γεγονός ότι στην πράξη το TMSI αλλάζει πολύ σπάνια. Ένας εισβολέας πραγματοποιεί πολλαπλές τηλεφωνικές κλήσεις στη συσκευή θύματος σε σύντομο χρονικό διάστημα και παρακολουθεί τα μηνύματα σελιδοποίησης. Εάν το πιο συχνό TMSI μεταξύ των μηνυμάτων σελιδοποίησης εμφανίζεται αρκετά συχνά, τότε ο εισβολέας συμπεραίνει ότι η συσκευή θύματος είναι παρούσα. Τα μηνύματα σελιδοποίησης μπορούν να ενεργοποιηθούν με SMS καθώς και ειδοποιήσεις από instant messengers.

Αυτές οι επιθέσεις εκμεταλλεύονται την αδυναμία ότι το TMSI αλλάζει σπάνια. Επιπλέον, τέτοιες επιθέσεις μπορούν να γίνουν μυστικές με την έννοια ότι ο εισβολέας μπορεί να πραγματοποιεί τηλεφωνικές κλήσεις και να στέλνει μηνύματα SMS που ενεργοποιούν μηνύματα σελιδοποίησης χωρίς να ειδοποιεί τον χρήστη της συσκευής

του θύματος. Η φυσική άμυνα ενάντια σε αυτές τις επιθέσεις είναι να αλλάζει συχνά το TMSI και να χρησιμοποιεί τυχαίες, απρόβλεπτες τιμές για το νέο TMSI. Αυτό καθιστά αναποτελεσματικές τις υπάρχουσες επιθέσεις.



Εικόνα 32: Exposing the device's TMSI and paging occasion. [25]

Το IMSI χρησιμοποιείται για την αναγνώριση του συνδρομητή για έλεγχο ταυτότητας και παροχή πρόσβασης, ο περιορισμός του βαθμού στον οποίο η χρήση του διακυβεύει το απόρρητο των χρηστών είναι ο κύριος στόχος αυτής της εργασίας. Όταν ένας συνδρομητής βρίσκεται σε περιαγωγή, δηλαδή έχει πρόσβαση σε υπηρεσία από ένα δίκτυο διαφορετικό από το κεντρικό του δίκτυο, το IMSI αποστέλλεται από το UE μέσω του δικτύου επίσκεψης στο οικιακό κεντρικό δίκτυο. Δεδομένου ότι το IMSI είναι μια μόνιμη ταυτότητα χρήστη, τα πρωτόκολλα διεπαφής αέρα έχουν σχεδιαστεί για να ελαχιστοποιούν τον αριθμό των περιστάσεων στις οποίες αποστέλλεται μέσω της διεπαφής αέρα.

Η παροχή απορρήτου χρήστη απαιτεί να μην μπορεί να υποκλαπεί η μόνιμη ταυτότητα χρήστη όταν αποστέλλεται μέσω της ραδιοζεύξης. Ένα επίπεδο εμπιστευτικότητας ταυτότητας παρέχεται με τη χρήση του TMSI αντί του IMSI. Ωστόσο, σε ορισμένες περιπτώσεις ένας UE χρειάζεται να στείλει το IMSI του μέσω της διεπαφής αέρα σε καθαρό κείμενο (plaintext). Μια τέτοια περίπτωση είναι όταν ένας UE είναι ενεργοποιημένος και επιθυμεί να συνδεθεί σε ένα νέο δίκτυο και ως εκ τούτου δεν θα έχει εκχωρημένο TMSI. Μια άλλη περίπτωση είναι όπου το δίκτυο εξυπηρέτησης δεν μπορεί να αναγνωρίσει το IMSI από το TMSI. [25]

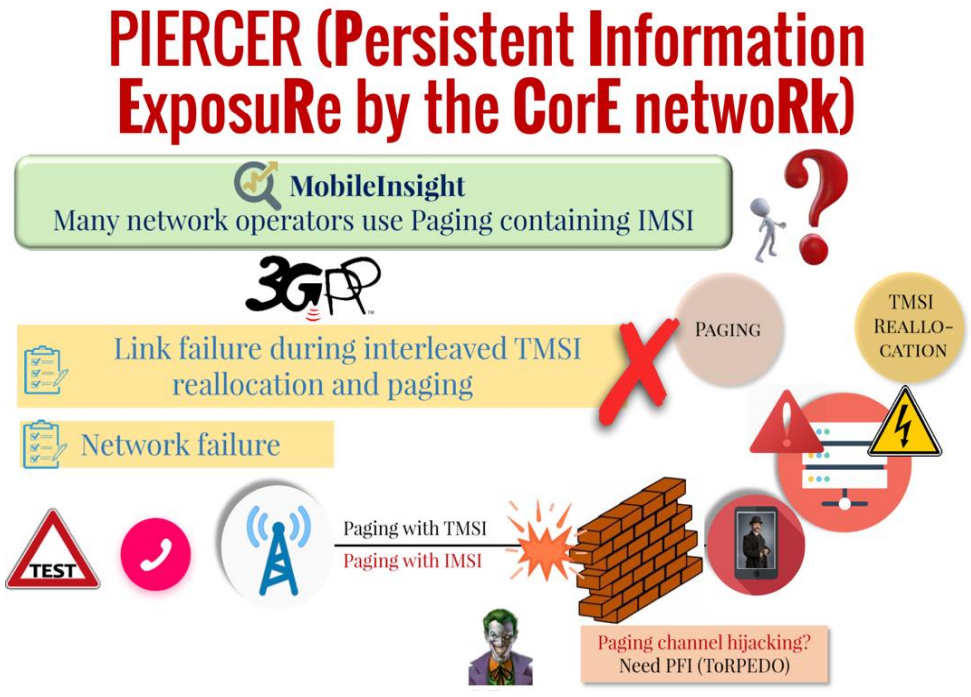
6.2.1 Επίθεση IMSI-Cracking για το 5G.

Αυτή η ενότητα αρχικά παρουσιάζει πώς η σταθερή φύση των περιπτώσεων σελιδοποίησης μπορεί να εκμεταλλευτεί ως πλευρικό κανάλι από έναν αντίπαλο στην περιοχή του θύματος για να συσχετίσει την ταυτότητα του θύματος (π.χ. αριθμός τηλεφώνου) με την περίσταση σελιδοποίησης του, με μόνο ένα μέτριο κόστος, μέσω μιας επίθεσης που ονομάστηκε ToRPEDO (TRacking via Paging mEssage DistributiOn). Κατά συνέπεια, δείχνουμε πώς το ToRPEDO μπορεί να επιτρέψει σε έναν αντίπαλο να επαληθεύσει τις πληροφορίες τοποθεσίας ενός θύματος, να εισάγει κατασκευασμένα μηνύματα σελιδοποίησης και να τοποθετήσει επιθέσεις άρνησης υπηρεσίας (DoS).

Το ToRPEDO δεν ισχύει μόνο για το 4G αλλά και για την τρέχουσα έκδοση του 5G. Μόλις ο εισβολέας γνωρίζει την περίσταση σελιδοποίησης του θύματος από το ToRPEDO, ο εισβολέας μπορεί να παραβιάσει το κανάλι σελιδοποίησης του θύματος. Αυτό θα επέτρεπε κατά συνέπεια στον εισβολέα να πραγματοποιήσει μια επίθεση DoS εισάγοντας κατασκευασμένα, κενά μηνύματα σελιδοποίησης, αποκλείοντας έτσι το θύμα από τη λήψη οποιωνδήποτε εκκρεμών υπηρεσιών (π.χ. SMS). Ο εισβολέας μπορεί επίσης να εισάγει κατασκευασμένα μηνύματα έκτακτης ανάγκης (π.χ. Amber alert) χρησιμοποιώντας πειρατεία καναλιού τηλεειδοποίησης. Με το ToRPEDO, ο εισβολέας μπορεί επίσης να ανιχνεύσει την παρουσία του θύματος σε οποιαδήποτε περιοχή κινητής τηλεφωνίας, υπό την προϋπόθεση ότι ο εισβολέας έχει έναν sniffer σε αυτήν την περιοχή. Επιπλέον, για μια στοχευμένη επίθεση, εάν ο εισβολέας γνωρίζει τις τοποθεσίες που επισκέπτεται συχνά το θύμα, τότε ο εισβολέας μπορεί να εγκαταστήσει sniffers σε αυτές τις τοποθεσίες για να δημιουργήσει το προφίλ

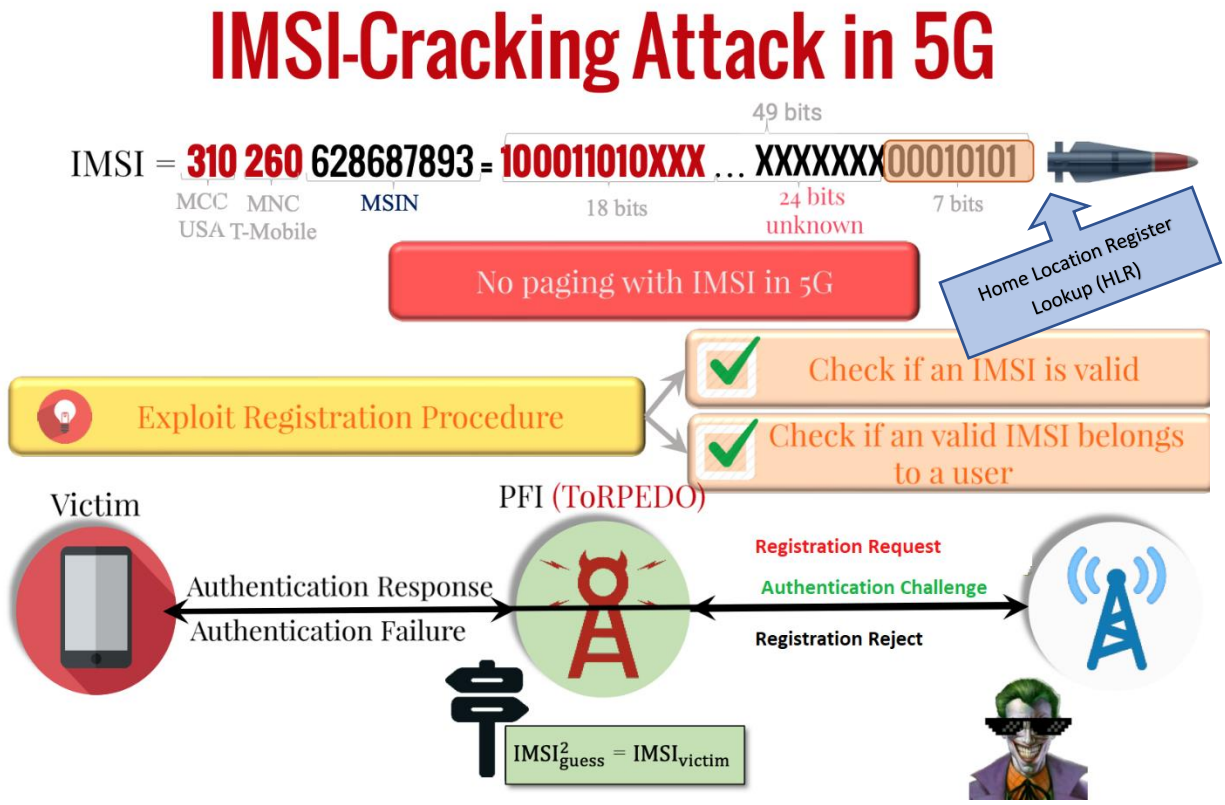
κινητικότητας του θύματος σε επίπεδο κυψέλης. Το ToRPEDO μπορεί επίσης να επιτρέψει στον εισβολέα να ανιχνεύσει την κατάσταση σύνδεσης (δηλαδή, σε αδράνεια/συνδεδεμένη) της συσκευής του θύματος που οδηγεί σε ζητήματα απορρήτου. Τέλος, το ToRPEDO μπορεί επίσης να χρησιμοποιηθεί για την προσάρτηση άλλων επιθέσεων, για παράδειγμα, τις επιθέσεις PIERCER και IMSI-Cracking που συζητούνται παρακάτω. [25]

Επίσης, αποδεικνύουμε ότι, σε 4G και 5G, είναι εύλογο για έναν αντίπαλο να ανακτήσει την επίμονη ταυτότητα μιας συσκευής θύματος (δηλαδή, IMSI) με μια επίθεση ωμής βίας "IMSI−Cracking" ενώ χρησιμοποιεί το ToRPEDO ως δευτερεύον βήμα επίθεσης. Η περαιτέρω έρευνά μας σχετικά με τις αναπτύξεις πρωτοκόλλου σελιδοποίησης 4G εντόπισε επίσης μια επίβλεψη εφαρμογής πολλών παρόχων δικτύου, η οποία επιτρέπει στον αντίπαλο να εξαπολύσει ένα νέο είδος επίθεσης IMSI-Catching, που ονομάζεται PIERCER (Persistent Information ExposuRe by the CorE netwoRk), για τη συσχέτιση του αριθμού τηλεφώνου ενός θύματος με το IMSI του, επιτρέποντας στη συνέχεια στοχευμένη παρακολούθηση της τοποθεσίας χρήστη.



Εικόνα 33: Persistent Information ExposuRe by the CorE network. [25]

Παρατηρούμε ότι το ToRPEDO δίνει τη δυνατότητα σε έναν εισβολέα που γνωρίζει τον αριθμό τηλεφώνου του θύματος να ανακτήσει το IMSI του θύματος εξαπολύοντας μια επίθεση ωμής βίας (brute-force attack). Για τους συνδρομητές των ΗΠΑ, τα IMSI μπορούν να αναπαρασταθούν ως δυαδικοί αριθμοί 49-bit. Τα κύρια 18-bit του IMSI (δηλαδή, ο κωδικός χώρας κινητής τηλεφωνίας και ο κωδικός δικτύου κινητής τηλεφωνίας) μπορούν να ληφθούν από τον αριθμό τηλεφώνου χρησιμοποιώντας υπηρεσίες αναζήτησης καταγραφής τοποθεσίας οικίας επί πληρωμή που βασίζονται στο Διαδίκτυο. Ο εντοπισμός της περίστασης σελιδοποίησης του θύματος με το ToRPEDO διαρρέει επιπλέον τα 7 τελευταία bit IMSI για τους συνδρομητές των ΗΠΑ, αφήνοντας 24 bit για να μαντέψει ο εισβολέας. Χρησιμοποιώντας μια επίθεση ωμής βίας ο εισβολέας μπορεί να μαντέψει το IMSI του θύματος σε λιγότερο από 13 ώρες.



Εικόνα 3164: IMSI-Cracking attack in 5G. [26]

Η επίθεση ToRPEDO, είναι σε θέση να επαληθεύσει εάν μια συσκευή-θύμα υπάρχει σε μια γεωγραφική κυψέλη με λιγότερες από 10 κλήσεις, ακόμη και με την υπόθεση ότι το TMSI αλλάζει μετά από κάθε κλήση. Επιπλέον, στη διαδικασία, ο εισβολέας μαθαίνει ακριβώς πότε μια συσκευή ξυπνά για να ελέγξει για μηνύματα σελιδοποίησης και 7 bit πληροφοριών του IMSI. Αυτή η γνώση επιτρέπει άλλες δύο νέες επιθέσεις που οδηγούν σε πλήρη ανάκτηση του IMSI της συσκευής. Όταν το TMSI αλλάζει κάθε φορά, δεν μπορεί πλέον να συνδέσει μια κλήση που έγινε από τον εισβολέα και το μήνυμα σελιδοποίησης που προκύπτει. Η βασική εικόνα της νέας μας επίθεσης είναι ότι το πρωτόκολλο σελιδοποίησης απαιτεί συγχρονισμό μεταξύ του σταθμού βάσης και της συσκευής.

Ως αντίμετρα -δεδομένου ότι το ToRPEDO είναι ο πρόδρομος των επιθέσεων PIERCER και IMSI- για την άμυνα ενάντια στο ToRPEDO, σχεδιάζουμε και αξιολογούμε ένα αντίμετρο που προσθέτει θόρυβο με τη μορφή πλαστών μηνυμάτων σελιδοποίησης για να διαταραχθεί η υποκείμενη διανομή μηνυμάτων σελιδοποίησης. Η αξιολόγησή μας υποδηλώνει ότι αυτό μπορεί να καταστήσει απαγορευτικά δαπανηρή την τοποθέτηση της επίθεσης ToRPEDO, ενώ συνεπάγεται μόνο μέτρια επιβάρυνση ενέργειας για τις συσκευές. [20]

6.3 Αναγνωριστικά 5G SUPI και SUCI.

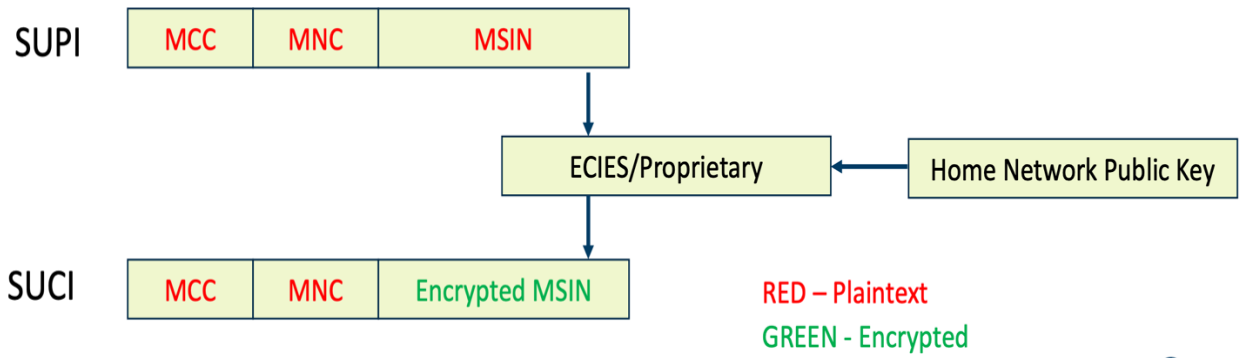
Στα τηλεπικοινωνιακά συστήματα, ο πάροχος δικτύου εκχωρεί σε κάθε κάρτα SIM ένα μοναδικό αναγνωριστικό, γνωστό μέχρι το 4G ως IMSI (International Mobile Subscriber Identity) και για το 5G ως SUPI (Μόνιμο Αναγνωριστικό Συνδρομής). Καθώς ο έλεγχος ταυτότητας μεταξύ ενός χρήστη και του παρόχου δικτύου του βασίζεται σε ένα κοινό συμμετρικό κλειδί, μπορεί να πραγματοποιηθεί μόνο μετά την αναγνώριση του χρήστη. Ωστόσο, εάν οι τιμές IMSI/SUPI αποστέλλονται σε απλό κείμενο μέσω της σύνδεσης ασύρματης πρόσβασης, τότε οι χρήστες μπορούν να εντοπιστούν, να εντοπιστούν και να παρακολουθηθούν χρησιμοποιώντας αυτά τα μόνιμα αναγνωριστικά.

Για να αποφευχθεί αυτή η παραβίαση απορρήτου, στην κάρτα SIM εκχωρούνται προσωρινά αναγνωριστικά (ονομάζεται Προσωρινή Ταυτότητα Συνδρομητή κινητής τηλεφωνίας (TMSI) μέχρι συστήματα 3G και GUTI για συστήματα 4G και 5G) από το

δίκτυο που επισκέπτεται. Αυτά τα προσωρινά αναγνωριστικά που αλλάζουν συχνά χρησιμοποιούνται στη συνέχεια για σκοπούς αναγνώρισης μέσω της σύνδεσης ασύρματης πρόσβασης. Ωστόσο, υπάρχουν ορισμένες περιπτώσεις όπου ο έλεγχος ταυτότητας μέσω της χρήσης προσωρινών αναγνωριστικών δεν είναι δυνατός π.χ. όταν ένας χρήστης εγγράφεται σε ένα δίκτυο για πρώτη φορά και δεν του έχει εκχωρηθεί ακόμη ένα προσωρινό αναγνωριστικό, μια άλλη περίπτωση είναι όταν το δίκτυο που επισκέπτεται δεν μπορεί να επιλύσει το IMSI/SUPI. από το παρουσιαζόμενο TMSI/GUTI.

Ένας ενεργός αντίπαλος άνθρωπος στη μέση μπορεί να προσομοιώσει σκόπιμα αυτό το σενάριο για να αναγκάσει έναν ανυποψίαστο χρήστη να αποκαλύψει τη μακροπρόθεσμη ταυτότητά του. Αυτές οι επιθέσεις είναι γνωστές ως επιθέσεις "IMSI catching" και παραμένουν στα σημερινά δίκτυα κινητής τηλεφωνίας, συμπεριλαμβανομένου του 4G LTE/LTE-Adv.

Οι επιθέσεις IMSI catching attacks έχουν απειλήσει όλες τις γενιές (2G/3G/4G) κινητών τηλεπικοινωνιών εδώ και δεκαετίες. Ως αποτέλεσμα της διευκόλυνσης της συμβατότητας προς τα πίσω για λόγους παλαιού τύπου, αυτό το πρόβλημα απορρήτου φαίνεται να παραμένει. Ωστόσο, το 3GPP αποφάσισε τώρα να αντιμετωπίσει αυτό το ζήτημα, αν και με το κόστος της συμβατότητας προς τα πίσω. Σε περίπτωση αποτυχίας αναγνώρισης μέσω 5G-GUTI, σε αντίθεση με προηγούμενες γενιές, οι προδιαγραφές ασφαλείας 5G δεν επιτρέπουν μεταδόσεις απλού κειμένου του SUPI μέσω της ραδιοδιεπαφής. Αντίθετα, μεταδίδεται ένα Σχέδιο Ολοκληρωμένης Κρυπτογράφησης Ελλειπτικής Καμπύλης (Elliptic Curve Integrated Encryption Scheme -ECIES) που βασίζεται στο απόρρητο και περιέχει το κρυφό SUPI. Αυτό το κρυφό SUPI είναι γνωστό ως SUCI (Subscription Concealed Identifier). [26]



Εικόνα 35: Η δομή SUPI και SUCI [26]

•Το SUPI (Subscription Permanent Identifier) είναι συνήθως μια συμβολοσειρά 15 δεκαδικών ψηφίων. Τα τρία πρώτα ψηφία αντιπροσωπεύουν τον Κωδικό Κινητής Χώρας (MCC) ενώ τα επόμενα δύο ή τρία σχηματίζουν τον Κωδικό δικτύου κινητής τηλεφωνίας (MNC) που προσδιορίζει τον χειριστή του δικτύου. Τα υπόλοιπα (εννέα ή δέκα) ψηφία είναι γνωστά ως αριθμός αναγνώρισης συνδρομητή κινητής τηλεφωνίας (MSIN) και αντιπροσωπεύουν τον μεμονωμένο χρήστη του συγκεκριμένου παρόχου. Το SUPI είναι ισοδύναμο με το IMSI που προσδιορίζει μοναδικά το ΜΕ, είναι επίσης μια συμβολοσειρά 15 ψηφίων.

•Το SUCI (Subscription Concealed Identifer) είναι ένα αναγνωριστικό που διατηρεί το απόρρητο που περιέχει το κρυφό SUPI. Το UE δημιουργεί ένα SUCI χρησιμοποιώντας ένα σύστημα προστασίας που βασίζεται σε ECIES (Elliptic Curve Integrated Encryption Scheme) με το δημόσιο κλειδί του Οικιακού Δικτύου που παρασχέθηκε με ασφάλεια στο USIM (Universal Subscriber Identity Module) κατά την εγγραφή του USIM. Μόνο το τμήμα MSIN του SUPI αποκρύπτεται από το σύστημα προστασίας, ενώ το αναγνωριστικό οικιακού δικτύου, δηλαδή το MCC/MNC μεταδίδεται σε απλό κείμενο. [26]

ΚΕΦΑΛΑΙΟ 7ο

7.1 Συμπεράσματα

Το 5G είναι υπό προϋποθέσεις πιο ασφαλές από οποιοδήποτε προηγούμενο δίκτυο κινητής τηλεφωνίας, δεδομένου ότι αξιοποιεί πολλές παραδοσιακές και δοκιμασμένες τεχνολογίες δικτύου και η αρχιτεκτονική του είναι ικανή να ενσωματώσει έναν αριθμό προηγμένων μηχανισμών ασφαλείας. Ωστόσο ενέχει τεράστιο κίνδυνο ασφάλειας, όπως στο λογισμικό, στον τεμαχισμό του δικτύου, υπάρχει πολύ μεγαλύτερος αριθμός συσκευών και σταθμοί βάσης κινητής τηλεφωνίας αλλά και η εισροή νέων προμηθευτών στην εφοδιαστική αλυσίδα.

Παρά το μεγάλο έργο στην ασφάλεια του 5G σε επίπεδο προτύπων, εξακολουθούν να υπάρχουν σημαντικοί κίνδυνοι. Οι φορείς παροχής του 5G θα πρέπει να μελετούν και να εφαρμόζουν τακτικά τις συστάσεις κατά 3GPP και GSMA για την προστασία των δικτύων τους. Οι αλλαγές στις πολιτικές ασφαλείας πρέπει να αποτελούν μέρος μιας συνολικής διαδικασίας. Η επαλήθευση πρέπει να πραγματοποιείται πριν και μετά την εφαρμογή. Με άλλα λόγια, η ασφάλεια στο 5G δεν είναι μόνο η ύπαρξη της κατάλληλης αρχιτεκτονικής ή εξοπλισμού ασφαλείας. Απαιτεί τη δημιουργία ροών εργασίας, διαδικασιών και συνεργασίας μεταξύ των ομάδων.

Η παραβίαση του 5G θα μπορούσε να γίνει τόσο απλή όσο και το hacking στο Internet. Ο πυρήνας του δικτύου 5G βασίζεται σε δικτύωση που ορίζεται από λογισμικό (SDN) και εικονικοποίηση λειτουργιών δικτύου (NFV). Το SDN και το NFV κάνουν μεγάλη χρήση των πρωτοκόλλων HTTP και REST API. Αυτά τα δύο πρωτόκολλα είναι πολύ γνωστά και χρησιμοποιούνται ευρέως στο Διαδίκτυο. Εργαλεία για την εύρεση και την εκμετάλλευση των ευπαθών σημείων είναι διαθέσιμα σε κάθε κακόβουλο χρήστη με απρόβλεπτες συνέπειες. Καθώς το SDN και το NFV υλοποιούνται για τον τεμαχισμό του δικτύου στο 5G, η διαχείριση θα γίνει ακόμη πιο δύσκολη. Η ευελιξία στα δίκτυα 5G έχει το κόστος της αυξημένης πολυπλοκότητας και αυτό συνεπάγεται μεγαλύτερη πιθανότητα σφαλμάτων στις ρυθμίσεις και κατάρρευσης της ασφάλειας.

Επίσης δισεκατομμύρια συνδεδεμένες συσκευές IoT προσφέρουν μια μεγάλη απειλή για τα botnets. Ο αριθμός των επιθέσεων στο IoT αυξάνεται. Η προστασία της

συσκευής είναι ανεπαρκής και η διανομή κακόβουλου λογισμικού είναι εύκολα επεκτάσιμη.

Κάθε νέα γενιά δικτύων κινητής τηλεφωνίας έχει την τάση να μειώνει τους κινδύνους για την ασφάλεια των πληροφοριών. Ζητήματα ασφάλειας σχετικά με τα πρωτόκολλα SS7 και Diameter (που είχαν προκύψει στα 2G,3G,4G, LTE δίκτυα), έχουν ληφθεί υπόψη κατά την ανάπτυξη της αρχιτεκτονικής του δικτύου 5G. Παρά όλους τους μηχανισμούς ασφαλείας στα δίκτυα 5G, η επίτευξη διαρκούς ασφάλειας θα απαιτήσει τις επιμελείς προσπάθειες των τηλεπικοινωνιακών παρόχων, που είναι υπεύθυνοι για την εφαρμογή των ιδανικών προτύπων, και την συνεργασία των ίδιων των χρηστών.

Η ασφάλεια των δικτύων 5G και οι τρόποι βελτίωσης τους, αποτελούν ένα πολύ μεγάλο κομμάτι ερευνητικής εργασίας. Στα πλαίσια αυτών των ερευνητικών εργασιών έχουν γίνει πολλές και ενδιαφέροντες προτάσεις, που μπορούν να χρησιμοποιηθούν για την επίτευξη ασφαλέστερων 5G δικτύων. Η έρευνα προς αυτή την κατεύθυνση θα πρέπει να είναι συνεχείς καθώς νέες απειλές ασφαλείας εμφανίζονται συνεχώς, λόγω των νέων και συνεχώς εξελισσόμενων τεχνολογιών που χρησιμοποιούν τα δίκτυα 5^{ης} γενιάς.

Παρόλο που τα δίκτυα 5^{ης} γενιάς εξελίσσονται ακόμα και δεν έχουν διερευνηθεί πλήρως, η ασφάλεια των δικτύων 6^{ης} γενιάς έχουν μπει ήδη στη συζήτηση. Η ασφάλεια των δικτύων 5G σίγουρα θα αποτελέσει μια βάση για την ασφάλεια των δικτύων της επόμενης γενιάς πράγμα που όπως είδαμε συμβαίνει σε κάθε μετάβαση από μια γενιά σε μια άλλη. Ωστόσο όπως κάθε νέα γενιά δικτύων, έτσι και η 6^{η} , θα φέρει νέα ζητήματα ασφαλείας, πολλά από τα οποία θα προκύψουν από τις τεχνολογίες ενεργοποίησης της, όπως η τεχνολογία κατανεμημένης λογιστικής (DLT), η κατανεμημένη AI/ML, η επικοινωνία ορατού φωτός (VLC) κ.α. . Όλα αυτά τα ζητήματα θα πρέπει να μελετηθούν λεπτομερώς και να αντιμετωπιστούν για να τα καταστήσουν τα δίκτυα 6^{ης} γενιάς, αξιόπιστα και ασφαλή για χρήση.

8 ΒΙΒΛΙΟΓΡΑΦΙΑ:

[1] Nelson Machado Junior , A Brief Introduction To 5G Technology , 22 Jan 2021,https://medium.com/the-shadow/a-brief-introduction-to-5gtechnology-b50c0f453f4

[2] Edge Cloud **,** https://5g.systemsapproach.org/intro.html

[3] Shanay Behrad, Emmanuel Bertin, Noel Crespi **"Securing Authentication for Mobile Networks, A Survey on 4G issues and 5G answers",** 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), February 2018.

[4] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, **"A , Comprehensive Guide to 5G Security"**, John Wiley & Sons, 2018.

[5] Alcardo Alex Barakabitzea, Arslan Ahmadb , Rashid Mijumbi , Andrew Hines, **"5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges" ,** Published by Elsevier B.V. , December 2019.

[6] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtov , **"5G Security: Analysis of Threats and Solutions" ,** 2017 IEEE Conference on Standards for Communications and Networking , 2017

[7] Harald Remmert, What Is 5G Network Architecture?, 2021, https://www.digi.com/blog/post/5g-network-architecture

[8] 5G Service-Based Architecture (SBA),20 Oct 2018 https://medium.com/5g-nr/5g-service-based-architecture-sba-47900b0ded0a

[9] Software Defined Networking , https://openairinterface.org/use-cases/cloud-ran-c-ran/

[10] Phillip Tracy, What is massive MIMO? .05 Aug 2016 **,** http://enterpriseiotinsights.com/20160805/5g/massive-mimo-5g-tag31-tag99

[11] W. Mattos, P. Gondim , **"M-Health Solutions Using 5G Networks and M2M Communications",** 25 May 2016 https://www.semanticscholar.org/paper/M-Health-Solutions-Using-5G-

Networks-and-M2M-Mattos-Gondim/58c59a699f5d287ab27c6b14a719e228b219e411

[12] Aleksandra Checko, Henrik L. Christiansen, Ying Yan, Lara Scolari, Georgios Kardaras, Michael S. Berger, and Lars Dittmann **"Cloud RAN for Mobile Networks—A Technology Overview"** in IEEE Communications Surveys & Tutorials , 2015

[13] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar , Jude Okwuibe , Andrei Gurtov , Mika Ylianttila, **"Security for 5G and Beyond"** in IEEE Communications Surveys & Tutorials , May 2019.

[14] 5G Architecture , https://www.viavisolutions.com/en-us/5g-architecture

[15] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, Andrei Gurtov , SDN reference architecture with network constituents ,Jan 2015 https://www.researchgate.net/figure/SDN-reference-architecture-with-network-constituents_fig2_281578191

[16] Wanqing Guan , Xiangming Wen , Luhan Wang , Zhaoming Lu , Yidi Shen ,**"A Service-Oriented Deployment Policy of End-to-End Network Slicing Based on Complex Network Theory"**, in IEEE Access , April 2018.

[17] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, Andrei Gurtov, **"Security in Software Defined Networks: A Survey" ,** in IEEE Communications Surveys & Tutorials · January 2015.

[18] Thomas O. Olwal , Karim Djouani, , Anish M. Kurien **, "A Survey of Resource Management Toward 5G Radio Access Networks" ,** in IEEE Communications Surveys & Tutorials · April 2016.

[19] Ijaz Ahmad , Madhusanka Liyanage , Shahriar Shahabuddin , Mika Ylianttila , Andrei Gurtov , **"Design Principles for 5G Security"** , Jan 2018 ,https://www.researchgate.net/figure/Secure-network-slices-for-different-services_fig4_322466911

[20] Hamidreza Ghorbani, Marzieh Izadyar, Hossein Amini Deilami, M. Hossein Ahmadzadegan **"Massive DDoS Occurrence Investigation in Future IoT devices".**

[21] **"DDoS Attacks on the IoT network with the Emergence of 5G "**

[22] Deivanai Gurusamy , Deva Priya M, Barmura Yibgeta, Assabu Bekalu**, "DDoS Risk in 5G Enabled IoT and Solutions " .**

[23] **"Enisa Threat Landscape for 5G Networks" ,** December 2020

[24] Altaf Shaik, Ravishankar Borgaonkar , **"New Vulnerabilities in 5G Networks" ,** Black Hat USA 201, Mandalay Bay/Las Vegas August 3-8-2019.

[25] Side Channel Attacks in 4G and 5G Cellular Networks (Black Hat Europe 2019, Excel London/UK December 2-5- 2019.

[26] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li and Elisa Bertino**, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information",** The University of Iowa.

9 ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ:

Συντομογραφία	Ανάλυση Συντομογραφίας
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accounting
AAM	Attack Alarm Module
ACK	Acknowledgement
AF	Application Function
AKA	Authentication Key Agreement
AMF	Access and Mobility Function
API	Application Interface
AR	Augmented Reality
ARP	Address Resolution Protocol
ASE	Automated Signature Extraction
AUSF	Authentication Server Function
BBU	Baseband Unit
BTS	Base Transceiver Station
C&C	Command & Control
CAPEX	Capital Expenditures
CCPS	Cloud Cyber Physical System
CCTV	Closed Circuit television
CSI	Channel State Information
CSP	Communication Service Providers
D2D	Device-to-Device
DAM	Damage
DCI	Data Centers Interconnect
DIS	Disaster
DN	Data Network
DNS	Domain Name System
DoS	Denial-of-Service

DPI	Deep Packet Inspection
DTLS	Datagram Transport
E2E	Exchange to exchange
EIH	Eavesdropping/Interception/ Hijacking
ECIES	Elliptic Curve Integrated Encryption Scheme
Embb	Enhanced mobile broadband
Enb	Evolved Node B
ENDER	pre-dEcisioN advaNce Decision, lEaRning
EPC	Evolved Packet Core
EPS	Evolved Packet System
Euicc	Embedded Universal Integrated Circuit Card
E-UTRAN	Evolved- Universal Terrestrial Radio Access Network
EVDO	Evolution-Data Optimized
FC	Fog Computing
FM	Failures or malfunctions
GSM	Global System for Mobile
GUTI	Globally Unique Temporary ID
HIDS	Host Intrusion Detection System
HSPA	High Speed Packet Access
HTTP	HyperText Tranfer Protocol
IaaS	Infrastracture as a Service
ICMP	Internet Control Message Protocol
ICT	Information and communication technologies
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force

IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IRTF	Internet Research Task Force
LBS	Location Based Services
LEG	Legal
LTE	Long Term Evolution
LTE-A	Long Term Evolution Advanced
M2M	Machine-to-Machine
MAC	Media Access Control
MANO	Management & Orchestration
MCC	Mobile Country Code
MEC	Mobile Edge Computing
MIMO	Multiple Input Multiple Output
MITM	Man In The Middle
ML	Machine Learning
MME	Mobility Management Entity
mMTC	Massive Machine Type Communication
MNC	Mobile Network Code
MSIN	Mobile Subscriber Number
MTC	Machine Type Communication
MVNO	Mobile Virtual Network Operators
NAA	Nefarious activity/abuse
NAI	Network Access Identifier
NAS	Non Access Stratum
NB-IoT	NarrowBand-IoT
NEF	Network Exposure Function
NF	Network Functions
NFV	Network Function Virtualization

NGMN	Next Generation Mobile Networks
NIC	Network Interface Controller
NIDS	Network Intrusion Detection System
NRF	Network Repository Function
NRF	Network Repository Function
NSSF	Network Slice Selection Function
ONF	Open Network Foundation
OPEX	Operating expenses
OUT	Outages
PA	Physical attacks
PaaS	Platform as a Service
PCF	Policy Control Function
PIERCER	Persistent Information ExposuRe by the CorE network
PSM	Power Saving Mode
QoS	Quality of Service
RAD	Reconstruct και Drop
RAN	Radio Access Network
RANaaS	RAN-as-a-Service
RAT	Radio Access Technology
RRC	Radio Resource Control
RRH	Remote Radio Head
SaaS	Software as a Service
SBI	Southbound interface
SDN	Software Defined Network
SDSF	Structured Data Storage network function
SIM	Subscriber Identity Module
SIPDAS	Slowly-increasing Polymorphic DDoS Attack Strategy

SMF	Session Management Function
SMS	Short Message Service
SN	Service Network
SOA	Service Oriented Architecture
SS7	Signalling System No 7
SSH	Secure Shell
SUCI	Subscription Concealed Identifier
SUPI	Subscriber Permanent Identifier
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
ToRPEDO	TRacking via Paging mEssage DistributiOn
TVDc	The Trusted Virtual Data Center
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage network function
UD	Unintentional Damage
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
URLLC	Ultra-reliable and low latency communications
VNF	Virtualized Network Functions
VoLTE	Voice Over LTE
VR	Virtual Reality
WAP	Wireless Application Protocol

WiMAX	Worldwide Interoperability for Microwave Access
XaaS	Anything as a service
XML	Extensible Markup Language