ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ασύρματα δίκτυα πέμπτης γενιάς (5G): Νέες προκλήσεις στην κυβερνοασφάλεια, νέες δυνατότητες στους επίδοξους χάκερς

ΡΙΣΜΑΟΥΙ ΓΕΩΡΓΙΟΣ

8^{Ο} ΕΞΑΜΗΝΟ ΑΜ 1743 EMAIL THL16117@UOI.GR

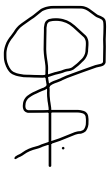
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΤΖΟΡΜΠΑΤΖΟΓΛΟΥ ΑΝΤΡΕΑΣ

FIFTH GENERATION (5G) WIRELLES NETWORKS: NEW CHALLENGES IN CYBERSECURITY, NEW OPPORTUNITIES FOR PROSPECTIVE HACKERS

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα πτυχιακή εργασία είναι εξ ολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

ΡΙΣΜΑΟΥΙ ΓΕΩΡΓΙΟΣ



Ευχαριστίες

Η συγκεκριμένη πτυχιακή εργασία με θέμα «**Ασύρματα δίκτυα πέμπτης γενιάς (5G): Νέες προκλήσεις στην κυβερνοασφάλεια, νέες δυνατότητες στους επίδοξους χάκερς»** πραγματοποιήθηκε εντός του υποχρεωτικού πλαισίου του υπάρχοντος κανονισμού του ιδρύματος Πληροφορικής και Τηλεπικοινωνιών για το έτος 2022.

Θα ήθελα να ευχαριστήσω όλα τα άτομα τα οποία με υποστήριξαν εμπράκτως κατα τη διάρκεια των σπουδών μου στο τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών.

Επίσης, θα ήθελα να ευχαριστήσω την οικογένεια μου η οποία στάθηκε ο κύριος αρωγός και συμπαραστάτης σε αυτή τη προσπάθεια. Επιπρόσθετα, θα ήθελα να ευχαριστήσω τους φίλους μου και συμφοιτητές μου για την βοήθεια και την συνεργασία που είχα μαζί τους.

Τέλος, θα ήθελα να ευχαριστήσω τον εισηγητή και καθηγητή της πτυχιακής μου εργασίας ο οποίος με καθοδήγησε με συμβούλεψε και μου έδωσε όλα τα

εφόδια και τις χρήσιμες οδηγείες του με κύριο στόχο την επίτευξη ενός άρτιου αποτελέσματος.

“Technology is a useful servant, but a dangerous master”

Περίληψη

Σε πολλούς τομείς της καθημερινής ζωής, οι ασύρματες τεχνολογίες έχουν γνωρίσει πρόσφατα ανάπτυξη. Όσον αφορά τις ασύρματες τεχνολογίες, το Διαδίκτυο των πραγμάτων (IoT), η τεχνολογία ασύρματων δικτύων 5G και τα μεγάλα δεδομένα που παράγει αποτελούν πρόκληση και ένα ενδιαφέρον πεδίο για περαιτέρω μελέτη. Τα μεγάλα δεδομένα που παράγονται ως αποτέλεσμα πρέπει να υποβάλλονται σε επεξεργασία, να μεταδίδονται γρήγορα μέσω δικτύων στο Cloud και ίσως να μεταδίδονται προς τα πίσω. Επιπλέον, τα δίκτυα πρέπει να εξοικονομούν πόρους και εύρος ζώνης. Το Διαδίκτυο των πραγμάτων απαιτεί ακόμη πιο άμεσα αποτελέσματα καθώς και μείωση της ηλεκτρικής ενέργειας. Τόσο οι αλγόριθμοι δρομολόγησης που δημιουργήθηκαν για τη μετάδοση δεδομένων στο Cloud όσο και οι τεχνολογίες χιλιοστομετρικών κυμάτων (mmWave) που αναπτύχθηκαν για τα ασύρματα δίκτυα 5ης γενιάς συμβάλλουν σημαντικά στον τομέα της γρήγορης μετάδοσης.

Ορισμένες από τις τρέχουσες τεχνολογίες αιχμής θα ενσωματωθούν με νέες τεχνολογίες και προσεγγίσεις στις επικοινωνίες πέμπτης γενιάς (5G). Τα μελλοντικά κινητά δίκτυα πέμπτης γενιάς θα αντιμετωπίσουν σημαντικά προβλήματα ασφάλειας ως αποτέλεσμα αυτής της ενσωμάτωσης. Το θέμα αυτής της διατριβής προσπαθεί να επιστήσει την προσοχή στα εναπομείναντα ζητήματα με την ασφάλεια των δικτύων 5G. Πριν από τη χαρτογράφηση των υφιστάμενων συστημάτων ασφαλείας που παρέχουν κάποιο είδος άμυνας, προστασίας ή ανίχνευσης σε αυτά, εντοπίζονται και ορίζονται πρώτα οι απειλές και οι μέθοδοι επίθεσης. Θα επικεντρωθούμε και θα εξετάσουμε τους πυλώνες, την αρχιτεκτονική, την ασφάλεια, τα οφέλη και τους κινδύνους της τεχνολογίας 5G.

Λέξεις-Κλειδιά: 5G Δίκτυα Ασφάλεια

Abstract

In many spheres of daily life, wireless technologies have recently experienced a growth. In terms of wireless technologies, the Internet of Things (IoT), 5G wireless network technology, and the Big Data it produces present a challenge and an intriguing area for further study. Big data generated as a result needs to be processed, quickly transmitted through networks in the Cloud, and maybe transmitted backward. Additionally, networks need to save on resources and bandwidth. The Internet of Things demands even more immediate outcomes as well as electricity reductions. Both the routing algorithms created for data transmission in the Cloud and the millimeter wave (mmWave) technologies developed for 5th Generation wireless networks make major contributions to the field of fast transmission.

A number of current state-of-the-art technologies will be integrated with new technologies and approaches in fifth generation (5G) communications. Future fifth generation mobile networks will face significant security concerns as a result of this integration. This thesis' theme tries to draw attention to the remaining issues with 5G network security. Prior to mapping current security systems that provide some sort of defense, protection, or detection to them, threats and attack methods are first identified and defined. We will examine the foundations, architecture, and security of 5G technology as well as its benefits and drawbacks.

Keywards: 5G Security Networks.

Πίνακας Περιεχομένων

Εισαγωγή

Σχεδόν όλες οι πτυχές της κοινωνικής, προσωπικής και επαγγελματικής ζωής έχουν επηρεαστεί από την τεχνολογία δικτύων και πληροφοριών, ιδίως από το διαδίκτυο. Συχνά έχουν μια πραγματική εξάρτηση από αυτές και μια αντικειμενική αδυναμία να λειτουργήσουν χωρίς αυτές, λόγω του πόσο καταλυτική είναι η επίδρασή τους. Ειδικότερα όσον αφορά το διαδίκτυο, η ταχεία ανάπτυξή του και η ποικιλία των εφαρμογών και των χαρακτηριστικών του το έχουν μετατρέψει σε βασικό εργαλείο για ποικίλες εργασίες που αφορούν την οικονομία, τις επιχειρήσεις και τους δημόσιους και ιδιωτικούς οργανισμούς (Ιγγλεζάκης, 2021: 75-79).

Σε καθημερινή βάση, ωστόσο, πολλοί άνθρωποι χρησιμοποιούν το διαδίκτυο για ποικίλους στόχους, όπως η ψυχαγωγία, η ενημέρωση και η εκπαίδευση, οι τραπεζικές συναλλαγές και, τέλος, η εμπλοκή και η επικοινωνία με άλλους χρήστες. Ωστόσο, η αλήθεια είναι ότι όσο αυξάνονται οι υπηρεσίες του διαδικτύου, τόσο αυξάνονται και οι κίνδυνοι που σχετίζονται με την ασφαλή χρήση του. Ορισμένοι από τους κινδύνους που υπάρχουν στο Διαδίκτυο περιλαμβάνουν κακόβουλο λογισμικό, ηλεκτρονική απάτη, διανομή παιδικής πορνογραφίας, εγκλήματα στον κυβερνοχώρο και κλοπή προσωπικών πληροφοριών από ανθρώπους και οργανισμούς. Είναι υποχρέωση των παρόχων υπηρεσιών δικτύου και πληροφοριών να προστατεύουν τους καταναλωτές από αυτούς τους κινδύνους και, κατ' επέκταση, τον ίδιο τον κυβερνοχώρο. Υποχρεούνται να θέσουν σε λειτουργία συστήματα κυβερνοασφάλειας και να τηρούν τις κατευθυντήριες γραμμές ασφαλείας που έχουν θεσπιστεί από τους τελευταίους.

Επί του παρόντος, οι αρμόδιες εθνικές και ευρωπαϊκές αρχές δίνουν μεγάλη σημασία στην ασφάλεια στον κυβερνοχώρο. Η Εθνική Αρχή Κυβερνοασφάλειας στην Ελλάδα και ο ENISA στην Ευρωπαϊκή Ένωση, έργο του οποίου είναι η ανάπτυξη και υλοποίηση των αντίστοιχων στρατηγικών κυβερνοασφάλειας, αποτελούν παραδείγματα αυτού (Ιγγλεζάκης, 2021: 75-79).

Η εξέλιξη της τεχνολογίας συνδέεται με τη μελέτη της ανθρώπινης ιστορίας. Η τεχνολογία έχει αλλάξει σημαντικά την ανθρώπινη σκέψη και συμπεριφορά, καθώς και τις πολιτικές και οικονομικές δομές και τον τρόπο με τον οποίο οι άνθρωποι βλέπουν τη γνώση. Η ίδρυση των Ηνωμένων Εθνών θεωρείται ως η έναρξη της σύγχρονης εποχής, η οποία έχει χαρακτηριστεί "μεταμοντέρνα". Πρακτικά, πρόκειται για την πρώτη προσπάθεια παγκοσμιοποίησης. Πιο συγκεκριμένα, η ανάπτυξη του τρανζίστορ το 1947 έπαιξε ρόλο στην έναρξη της εποχής της πληροφορίας. Οι ηλεκτρονικοί υπολογιστές και το διαδίκτυο λειτούργησαν στη συνέχεια ως σημείο εισόδου στην ψηφιακή εποχή. Η ψηφιακή εποχή γέννησε έναν ολοκαίνουργιο, άυλο κόσμο που υπάρχει παράλληλα με τον φυσικό. Ένα σύμπαν χωρίς προκαθορισμένα θέματα, το οποίο ωστόσο υπόκειται στην κοινωνικοποίηση, την εκπαίδευση, την παρουσία ή την έλλειψη προτύπων και τις ποινές για την παραβίασή τους.

Λόγω της απουσίας βασικών θεσμών όπως η οικογένεια και το σχολείο που διευκολύνουν την εύκολη ομαδική ένταξη, η γρήγορη εξέλιξη αυτού του ψηφιακού κόσμου χωρίς καμία διαδικασία προετοιμασίας και προσαρμογής έχει καταστήσει την "ψηφιακή κοινωνικοποίηση" πρόκληση. Ως αποτέλεσμα, το άτομο ενεργεί ανεξάρτητα, χωρίς περιορισμούς και, συγκαλύπτοντας την ανωνυμία που του παρέχεται, συμπεριφέρεται με μια απεριόριστη αίσθηση ελευθερίας που αγγίζει τα όρια της αναρχίας. Ως αποτέλεσμα αυτής της περίστασης δημιουργούνται απειλές για την εσωτερική και εθνική ασφάλεια ενός κράτους (Ιγγλεζάκης, 2021: 75-79).

1. Εννοιολογικοί Προσδιορισμοί

1.1 Κυβερνοασφάλεια

Η σημασία των συστημάτων δικτύων και πληροφοριών για την κοινωνία δεν μπορεί να υπερτιμηθεί. Η διεκπεραίωση εμπορικών και κοινωνικών συναλλαγών εξαρτάται από την ασφάλεια και την αξιοπιστία αυτών των συστημάτων. Ωστόσο, οι σκόπιμες εχθρικές ενέργειες που αποσκοπούν στη βλάβη ή την παρέμβαση στη λειτουργία αυτών των συστημάτων αποτελούν σοβαρό κίνδυνο, υπονομεύοντας σοβαρά την οικονομική δραστηριότητα και δημιουργώντας αβεβαιότητα στους χρήστες. Για πολλά έθνη που έχουν αναγνωρίσει τη σημασία και τον στόχο της, η ασφάλεια στον κυβερνοχώρο -η προστασία των συστημάτων και των δεδομένων δικτύων και υπολογιστών από περιστατικά κυβερνοεπιθέσεων- αποτελεί μείζον

ζήτημα. Οι στρατηγικές κυβερνοασφάλειας έχουν αναπτυχθεί και βελτιωθεί προκειμένου να διασφαλιστούν από τις απειλές ασφαλείας και να εξασφαλιστεί η κοινωνική και οικονομική επιτυχία. Οι τακτικές αυτές επιδιώκουν να προωθήσουν και να εμβαθύνουν τη διεθνή συνεργασία καθώς και την κυβερνητική συνεργασία και τον επιμερισμό των ευθυνών στον αγώνα κατά του εγκλήματος στον κυβερνοχώρο. Επιδιώκουν επίσης να προωθήσουν τη συνεργασία μεταξύ του δημόσιου και του εμπορικού τομέα, ιδίως των παρόχων υπηρεσιών διαδικτύου. Όσον αφορά τη φράση "κυβερνοασφάλεια", αυτή αναφέρεται συγκεκριμένα σε κάθε προφύλαξη και διαδικασία που εφαρμόζεται για την ασφάλεια των πληροφοριακών συστημάτων και των χρηστών τους από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και ζημιές, προκειμένου να διατηρηθεί η "εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα" των δεδομένων (Provos et al., 2009: 42-47).

Η κυβερνοασφάλεια εργάζεται για να σταματήσει και να εντοπίσει περιστατικά που σχετίζονται με την ασφάλεια και προσφέρει απαντήσεις σε αυτά, καθώς και έναν τρόπο για να τα ξεπεράσει κανείς. Η ακούσια διανομή πληροφοριών, οι επιθέσεις σε σημαντικούς θεσμούς και επιχειρήσεις, η κλοπή ιδιωτικών πληροφοριών, ακόμη και η ανάμειξη στις δημοκρατικές διαδικασίες είναι μερικά μόνο παραδείγματα αυτών των περιστατικών, τα οποία μπορεί να είναι σκόπιμα ή τυχαία. Τα περιστατικά αυτά μπορούν να έχουν αρνητικές επιπτώσεις στους ανθρώπους, τους οργανισμούς και τις κοινότητες με πολλούς διαφορετικούς τρόπους. Ο όρος "κυβερνοασφάλεια" χρησιμοποιείται στο πολιτικό πλαίσιο της Ευρωπαϊκής Ένωσης για να αναφέρεται σε κάθε εγκληματική δραστηριότητα που πραγματοποιείται με τη χρήση ψηφιακής τεχνολογίας στο διαδικτυακό περιβάλλον, καθώς και στην ασφάλεια των δικτύων και των πληροφοριακών συστημάτων. Ως εκ τούτου, η κυβερνοασφάλεια μπορεί επίσης να αναφέρεται σε εγκλήματα στον κυβερνοχώρο, όπως οι μολύνσεις από ιούς υπολογιστών ή η απάτη με μεθόδους πληρωμής, εκτός από τις οικονομικές πληρωμές. Μπορεί επίσης να στοχεύει όχι μόνο σε συστήματα αλλά και σε περιεχόμενο, όπως η διαδικτυακή διανομή σεξουαλικού υλικού για ανηλίκους. Επιπλέον, μπορεί να αποτελέσει στόχο δόλιων δραστηριοτήτων για τον επηρεασμό του διαδικτυακού λόγου και εικασιών για ανάμιξη σε εκλογικές διαδικασίες (Provos et al., 2009: 42-47).

Οι ηλεκτρονικές συσκευές είναι πλέον πιο διαδεδομένες από τους ανθρώπους. Ως αποτέλεσμα, οι απατεώνες αναπτύσσουν πιο δημιουργικές μεθόδους. Οι ψηφιακοί κίνδυνοι, ή οι κυβερνοαπειλές, όπως είναι συχνά γνωστές, βρίσκονται σε άνοδο και

περιλαμβάνουν πράγματα όπως ιούς υπολογιστών, ransomware, κακόβουλο λογισμικό, παραβιάσεις συστημάτων υπολογιστών που προκαλούνται από εχθρικούς χρήστες (χάκερ), ηλεκτρονική κλοπή ταυτότητας κ.λπ. Οι απειλές στον κυβερνοχώρο είναι δραστηριότητες που γίνονται από εξωτερικά μέρη για να αποκτήσουν πρόσβαση σε πόρους στους οποίους δεν έχουν την εξουσία πρόσβασης, να καταστρέψουν εμπιστευτικές πληροφορίες, να εκβιάσουν χρήματα από τους χρήστες ή να παρέμβουν στις λειτουργίες μιας επιχείρησης (Provos et al., 2009: 42-47).

Πολλά έθνη που αναγνωρίζουν τη σημασία της ασφάλειας στον κυβερνοχώρο την έχουν αναγάγει σε ύψιστη προτεραιότητα. Υπονοεί τη διαδικασία που διασφαλίζει ότι οι πληροφορίες είναι ακριβείς, ιδιωτικές και προσβάσιμες. Η κυβερνοασφάλεια είναι η προστασία των δικτύων, των συσκευών, των προγραμμάτων και των δεδομένων από επιθέσεις ή μη εξουσιοδοτημένη πρόσβαση. Αποτελείται από ένα διαρκώς αναπτυσσόμενο μείγμα εργαλείων, στρατηγικών διαχείρισης κινδύνων, τεχνολογιών, εκπαίδευσης και βέλτιστων πρακτικών. Οι χρήστες (άτομα), οι οργανωτικές ή ατομικές διαδικασίες και ο απαραίτητος εξοπλισμός και το λογισμικό για την προστασία από επιθέσεις στον κυβερνοχώρο είναι οι τρεις κύριες και πιο κρίσιμες πτυχές της κυβερνοασφάλειας. Ως αποτέλεσμα έχουν δημιουργηθεί τακτικές κυβερνοασφάλειας. Υπάρχουν για να προστατεύουν από τους κινδύνους για την ασφάλεια και να προάγουν την οικονομική και κοινωνική ευημερία. Επιδιώκουν την αύξηση της διεθνούς συνεργασίας, την αποσαφήνιση των καθηκόντων και των αρμοδιοτήτων για την κυβερνητική συνεργασία και τη δίωξη του εγκλήματος στον κυβερνοχώρο (Provos et al., 2009: 42-47).

1.2 Κυβερνοχώρος

Αρχικά, η φράση "κυβερνοχώρος" αναφέρεται στον φανταστικό χώρο που καθίσταται δυνατός χάρη στο διαδίκτυο και τους υπολογιστές.

Ο William Gibson, συγγραφέας επιστημονικής φαντασίας, πιστώνεται με την επινόηση της φράσης, η οποία εμφανίστηκε αρχικά στο μυθιστόρημά του Neuromancer το 1984: "Μια παγκόσμια ψευδαίσθηση που μοιράζονται δισεκατομμύρια χρήστες που συναινούν κάθε μέρα σε κάθε έθνος καθώς αποκτούν μαθηματικές έννοιες... δεδομένα που διαχωρίζονται από κάθε υπολογιστή στο ανθρώπινο σύστημα, αναπαριστώνται γραφικά. εξαιρετική πολυπλοκότητα Συστάδες

και αστερισμοί πληροφοριών, γραμμές φωτός που εξαπλώνονται στο μη-διάστημα της νοημοσύνης. Σαν τα φώτα της πόλης που σβήνουν..." (Gordon & Ford, 2006: 13-20).

Στην πραγματικότητα, ανεξάρτητα από τον φυσικό τόπο, ο κυβερνοχώρος μπορεί να κατανοηθεί ως η διασύνδεση των ατόμων μέσω των υπολογιστών και των τηλεπικοινωνιών. Αναπτύχθηκε σταδιακά ως αποτέλεσμα της προόδου της επιστήμης και της τεχνολογίας. Δεδομένου ότι οι ανθρώπινες δραστηριότητες διεξάγονται πλέον όλο και περισσότερο σε αυτόν, αποτελείται από έναν ιστό διασυνδεδεμένων δικτύων όπου φυλάσσονται κάθε είδους πληροφορίες και όπου συνδέονται επίσης οι υποδομές των χωρών. Ο κυβερνοχώρος αναπτύσσεται γρήγορα και δεν υπάρχει κανένα ρυθμιστικό όργανο που να εμποδίζει άτομα, πολιτικά κόμματα ή συνασπισμούς κυβερνήσεων να επιδίδονται σε εγκληματικές δραστηριότητες. Ουσιαστικά, το Διαδίκτυο και ο επακόλουθος κυβερνοχώρος είναι περίπλοκα περιβάλλοντα των οποίων η απεραντοσύνη είναι πρακτικά ατελείωτη και καθιστά την πλήρη προσβασιμότητα ανέφικτη. Κατά συνέπεια, η διατήρηση του ελέγχου του και η προστασία του από παράνομες και εγκληματικές δραστηριότητες είναι αρκετά δύσκολη (Gordon & Ford, 2006: 13-20).

1.3 Κυβερνοτρομοκρατία

Η κυβερνοτρομοκρατία και οι κυβερνοεπιθέσεις θεωρούνται εγκλήματα. Η λέξη "κυβερνοτρομοκρατία", η οποία περιγράφει τη συγχώνευση της τρομοκρατίας με τον κυβερνοχώρο, δημιουργήθηκε από τον Barry Collin, ανώτερο υπάλληλο του Ινστιτούτου Πληροφοριών των Ηνωμένων Πολιτειών. Όσον αφορά τους κινδύνους της επικείμενης ψηφιακής εποχής, ξεκίνησε στα μέσα της δεκαετίας του 1990. Ο φόβος ενός απροσδόκητου αλλά τρομερού τρομοκρατικού χτυπήματος και ο φόβος της απρόβλεπτης και περίπλοκης ηλεκτρονικής τεχνολογίας είναι δύο από τις πιο διαδεδομένες ανησυχίες των ημερών μας που συνδυάζονται σε αυτό.

Η κυβερνοτρομοκρατία ως έννοια δεν καλύπτεται ούτε από το διεθνές ούτε από το εθνικό δίκαιο. Το 2000, η Dorothy Denning, ερευνήτρια και καθηγήτρια της επιστήμης της πληροφορικής, προσέθεσε στον όρο συνδέοντάς τον με παράνομες επιθέσεις εναντίον υπολογιστών, δικτύων ή δικτυακών πληροφοριών με σκοπό τον εκφοβισμό ή τον εξαναγκασμό μιας κυβέρνησης για την επίτευξη πολιτικών ή κοινωνικών στόχων. Ωστόσο, μια ανάγκη είναι ότι η επίθεση πρέπει να καταλήγει σε

βία κατά των ατόμων που αποτελούν στόχο ή τουλάχιστον να ενσταλάζει βαθύ αίσθημα φόβου ή να προκαλεί θάνατο, σωματική βλάβη ή υλική απώλεια. Ένας άλλος ορισμός της τρομοκρατίας στον κυβερνοχώρο είναι η εκτέλεση μιας αιφνίδιας επίθεσης από ένα κράτος ή μια τρομοκρατική ομάδα που χρησιμοποιεί την τεχνολογία, τους υπολογιστές και το διαδίκτυο για να καταστρέψει τη φυσική και ηλεκτρονική υποδομή του έθνους και να διαταράξει ζωτικές υπηρεσίες (Gordon & Ford, 2006: 13-20).

Η έννοια του φαινομένου της κυβερνοτρομοκρατίας είναι ασαφής γενικότερα. Η μία οπτική γωνία εξετάζει το φαινόμενο χρησιμοποιώντας την τεχνική αιτίου και αποτελέσματος και η άλλη το εξετάζει χρησιμοποιώντας τη διαδικτυακή δραστηριότητα του φαινομένου. Όσον αφορά την πρώτη προοπτική, γνωστή ως προοπτική αιτίου και αποτελέσματος, η κυβερνοτρομοκρατία αναδύεται όταν οι επιθέσεις σε υπολογιστές οδηγούν σε ένα περιβάλλον όπου παράγεται φόβος, όπως και μια παραδοσιακή τρομοκρατική πράξη. Η κυβερνοτρομοκρατία περιγράφεται ως "Εγκληματική πράξη που γίνεται με τη χρήση ηλεκτρονικών υπολογιστών και έχει ως αποτέλεσμα τη βία, το θάνατο ή την καταστροφή, δημιουργώντας ένα αίσθημα τρόμου που έχει ως στόχο να επηρεάσει την πολιτική μιας κυβέρνησης" με πιο απλό και συμπυκνωμένο τρόπο (Gordon & Ford, 2006: 13-20).

Επιπλέον, ένα άτομο πρέπει να πληροί τις ακόλουθες προϋποθέσεις προκειμένου να θεωρηθεί τρομοκράτης και οι δραστηριότητές του να κατηγοριοποιηθούν ως τρομοκρατικές:

1. Η πράξη του πρέπει να είναι προμελετημένη και να υποκινείται από ιδεολογικά συμφέροντα
2. Να πραγματοποιείται ενάντια σε αμάχους, από συγκεκριμένες ομάδες.
3. Να είναι ικανή να διασπείρει τον τρόμο με σκοπό να επηρεαστούν οι κυβερνόντες.

Η χρήση του διαδικτύου και άλλων μορφών τεχνολογίας επικοινωνίας αυξάνεται συνεχώς. Οι τρομοκράτες και οι εξτρεμιστές στρέφονται όλο και περισσότερο στο Διαδίκτυο για να εξαπολύουν επιθέσεις εναντίον ισχυρών κρατών του διεθνούς συστήματος, ιδίως των Ηνωμένων Πολιτειών, λόγω της προστασίας των συνόρων και των ανθρώπων. Λόγω των κενών ασφαλείας στη χρήση των υπολογιστών και του Διαδικτύου, οι τρομοκράτες μπορεί να έχουν την ευκαιρία να

αποκτήσουν περισσότερες γνώσεις σχετικά με τα συστήματα υπολογιστών και να συνάψουν συνεργασίες με το οργανωμένο έγκλημα (Gordon & Ford, 2006: 13-20).

1.4 Ασφάλεια Πληροφοριών

Η ασφάλεια των πληροφοριών αποσκοπεί στην προστασία των πόρων και των δεδομένων ενός πληροφοριακού συστήματος στο σύνολό του από κάθε βλάβη που θα μπορούσε να μειώσει την αξία τους. Επιπλέον, φιλοδοξεί να παρέχει αξιόπιστα δεδομένα στα οποία οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση όποτε χρειάζεται. Η ασφάλεια πληροφοριών μπορεί να θεωρηθεί ως μια διαδικασία τριών σταδίων από πρακτική άποψη (Μαυρίδης, 2015: 16-17).

- Πρόληψη, η οποία συνεπάγεται τη λήψη μέτρων για την αποφυγή των αρνητικών επιπτώσεων των αντιδράσεων
- Η ανίχνευση είναι η διαδικασία εντοπισμού συμπεριφορών και στη συνέχεια η εξέταση των συνθηκών, των ανθρώπων και των συμπεριφορών που οδήγησαν σε αυτές τις συμπεριφορές
- Η αποκατάσταση των πληγέντων πόρων και η διαχείριση των συνεχιζόμενων επιθέσεων αποτελούν την αντίδραση (Μαυρίδης, 2015: 16-17).

Όσον αφορά τις Σεχνολογίες Πληροφορίας και Επικοινωνιών αυτές αποσκοπούν:

α) «Προστασία Υπολογιστικών Συστημάτων (Computer Security): πρόληψη της μη εξουσιοδοτημένης χρήσης των πόρων του συστήματος υπολογιστών και άμυνα κατά της ακούσιας ή εκούσιας αποκάλυψης, τροποποίησης ή διαγραφής δεδομένων κατά την επεξεργασία και την αποθήκευση

β) «Προστασία Επικοινωνιών (Communication Security): είναι η διασφάλιση των πόρων του δικτύου και η υπεράσπιση των δεδομένων έναντι ακούσιας ή εκούσιας αποκάλυψης, τροποποίησης ή διαγραφής κατά τη μετάδοση μέσω δικτύων υπολογιστών.

Επιπλέον, η προστασία των πόρων και των δεδομένων βασίζεται σε σημαντικές πτυχές της ασφάλειας πληροφοριών, όπως (Μαυρίδης, 2015: 16-17):

i) «Εμπιστευτικότητα»: αναφέρεται στην προστασία των πληροφοριών από την αποκάλυψη όταν δεν έχει δοθεί άδεια.
ii) «Ακεραιότητα»: η προστασία των πληροφοριών από πιθανή αλλαγή, αλλοίωση ή διαγραφή χωρίς προηγούμενη άδεια για το σκοπό αυτό
iii) «Διαθεσιμότητα»: αναφέρεται στην ασφάλεια της εξουσιοδοτημένης πρόσβασης στην πληροφορία χωρίς καθυστέρηση ή παρεμπόδιση, είτε με σκοπό την αποκάλυψη είτε με σκοπό την τροποποίηση.
iv) «Πιστοποίηση»: Πραγματοποιήται επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής δεδομένων.
v) «Μη Άρνηση Αποδοχής»: Συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας και διασφαλίζει οτι μία συναλλαγή η οποία πραγματοποιήθηκε ηλεκτρονικά δεν μπορεί να αμφισβητηθεί από τα συμβαλλόμενα μέρη. Για παράδειγμα ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα.

Επιπλέον, η ασφάλεια στις ΤΠΕ εξαρτάται από τη λειτουργία συγκεκριμένων συστημάτων που εφαρμόζονται επιτυχώς εκτός από τα προαναφερθέντα χαρακτηριστικά. Ειδικότερα, εφαρμόζονται ο μηχανισμός "ταυτοποίησης" -ο οποίος αφορά τη διαδικασία ταυτοποίησης ενός προσώπου ενώπιον του συστήματος- και ο μηχανισμός "πιστοποίησης" -ο οποίος αφορά την επαλήθευση των στοιχείων ενός προσώπου που ανακοινώνει ένα πρόσωπο στο σύστημα. Ακολουθεί ο μηχανισμός "εξουσιοδότησης", ο οποίος αναφέρεται στην απόφαση σχετικά με την αποδοχή ή την απόρριψη του αιτήματος πρόσβασης ενός προσώπου σε ένα σύστημα μετά την αυθεντικοποίησή του, με βάση τα δικαιώματα πρόσβασης που έχουν ήδη χορηγηθεί και τη διαδικασία όσον αφορά τον έλεγχο σχετικά με την πρόσβαση στο σύστημα, και τέλος ο μηχανισμός "άρνησης πρόσβασης", ο οποίος αφορά την απόδοση ευθύνης για την εκτέλεση μιας ενέργειας στο σύστημα πέραν πάσης λογικής αμφιβολίας (Μαυρίδης, 2015: 17-18).

2. Ασύρματα Δίκτυα

Ο Ιταλός εφευρέτης G. Marconi έθεσε τα θεμέλια για τις σύγχρονες επικοινωνίες. Πρωτοστάτησε στην ασύρματη επικοινωνία χρησιμοποιώντας

ηλεκτρομαγνητικά κύματα για να μεταδώσει το γράμμα "S" στον κώδικα Μορς σε απόσταση 3 χιλιομέτρων. Η χρήση των ασύρματων επικοινωνιών θα είναι στάνταρ στη σημερινή και αυριανή ζωή. Το ραδιόφωνο, η τηλεόραση και οι δορυφορικές επικοινωνίες έχουν επηρεάσει τον τρόπο με τον οποίο λειτουργεί σήμερα η κοινωνία μας. Ο ρυθμός δεδομένων, η κινητικότητα και η φασματική αποδοτικότητα θα αυξηθούν μαζί με την ασύρματη τεχνολογία. Οι τεχνολογίες 1G και 2G χρησιμοποιούν μεταγωγή κυκλώματος, αλλά οι τεχνολογίες 2.5G και 3G χρησιμοποιούν τόσο μεταγωγή κυκλώματος όσο και μεταγωγή πακέτων. Οι τεχνολογίες λειτουργούν με τον ίδιο τρόπο όπως και οι διάδοχοι 3.5G έως 5G. Το αδειοδοτημένο φάσμα διαφέρει από το μη αδειοδοτημένο φάσμα εκτός από αυτά τα άλλα χαρακτηριστικά. Ενώ τεχνολογίες όπως το Wi-Fi, το Bluetooth και το WiMax χρησιμοποιούν το μη αδειοδοτημένο φάσμα, όλες οι εξελισσόμενες γενιές χρησιμοποιούν το αδειοδοτημένο φάσμα (Salah et al., 2021: 150-158).

2.1 Εξέλιξη Δικτύων

Πριν από το 1G, μόνο η φωνή μπορούσε να σταλεί μέσω ασύρματων δικτύων χρησιμοποιώντας αναλογικά συστήματα με μονοδιάστατη διαμόρφωση (SSB).

Οι ασύρματες επικοινωνίες μόνο για φωνή ήταν τυπικές στο 1G (1983). Το Bell Labs αποφάσισε να χρησιμοποιήσει αναλογικά συστήματα το 1966, επειδή η ψηφιακή ραδιοτεχνολογία ήταν πολύ ακριβή για ένα κινητό σύστημα υψηλής χωρητικότητας.

2G (1990): Οι ασύρματες επικοινωνίες μόνο για φωνή χρησιμοποιήθηκαν αποκλειστικά κατά τη διάρκεια αυτής της περιόδου. Το ευρωπαϊκό GSM χρησιμοποιούσε πολυπλεξία TDMA και ήταν ψηφιακή τεχνολογία. Από την πώληση της AT&T το 1980, κανένας ερευνητικός οργανισμός (όπως τα Bell Labs) δεν μπόρεσε να δημιουργήσει ένα ανώτερο σύστημα 2G που να είναι εξίσου αποτελεσματικό με το σύστημα 1G στη Βόρεια Αμερική. Το IS-54 εγκαταλείφθηκε καθώς ήταν δυσμενές. Το GSM ήταν τότε γνωστό ως 2G. Η αλλαγή από το 1G στο 2G σηματοδοτεί μια κρίσιμη μετάβαση από το αναλογικό στο ψηφιακό σύστημα (Salah et al., 2021: 150-158).

Όλες οι ασύρματες επικοινωνίες στο 2.5G (1995) επικεντρώνονται κυρίως στη φωνή υψηλής χωρητικότητας με περιορισμένη υπηρεσία δεδομένων. Στις ΗΠΑ εφαρμόστηκε ένα σύστημα CDMA με εύρος ζώνης 1,25 MHz.

3G (1999): Οι ασύρματες συνδέσεις φωνής και δεδομένων είναι διαθέσιμες σε αυτή τη γενιά. Σε αντίθεση με τις προηγούμενες γενιές τεχνολογιών, το 3G είναι το πρώτο παγκοσμίως τυποποιημένο σύστημα που παρήγαγε η ITU. Το WCDMA χρησιμοποιείται από το 3G με εύρος ζώνης 5 MHz. Υποστηρίζονται τόσο το TDD όσο και το FDD. Ως εκ τούτου, μπορούμε να αναφέρουμε ότι η μετάβαση από τα συστήματα που βασίζονται στη φωνή στα συστήματα που βασίζονται στα δεδομένα έγινε κατά τη διάρκεια της μετάβασης από τα συστήματα 2G στα συστήματα 3G.

4G (2013). (2013). Υπάρχουν δύο δίκτυα 4G. ο Το WiMAX δημιουργήθηκε στις ΗΠΑ χρησιμοποιώντας την ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM) και το σύστημα LTE, το οποίο δημιουργήθηκε μετά το WiMAX. Το εύρος ζώνης κάθε συστήματος είναι 20 MHz. Επομένως, μπορούμε να ισχυριστούμε ότι η μετάβαση από το 3G στο 4G αντιπροσωπεύει μια αλλαγή από αργές ταχύτητες δεδομένων για το Διαδίκτυο σε γρήγορες ταχύτητες δεδομένων για κινητά βίντεο.

5G (2021): Οι οργανισμοί τυποποίησης εξακολουθούν να εργάζονται για τον επίσημο ορισμό του 5G. Πρόκειται για ένα επαναστατικό σύστημα δεδομένων με εξαιρετικά υψηλές απαιτήσεις χωρητικότητας και ταχύτητας (Salah et al., 2021: 150-158).

2.2 Δίκτυα 5g- δίκτυα πέμπτης γενιάς

Στην τεχνολογία της κινητής τηλεφωνίας, η πέμπτη γενιά κινητών δικτύων, συχνά γνωστή ως 5G ή ασύρματα συστήματα 5ης γενιάς, θεωρείται το αποκορύφωμα της ασύρματης επικοινωνίας. Το καλώδιο δικτύου αποτελεί πλέον μια μακρινή ανάμνηση. Τα κινητά τηλέφωνα είναι χρήσιμα για διάφορα πράγματα εκτός από την επικοινωνία. Όσον αφορά την ευκολία κοινής χρήσης τηλεφώνων και δεδομένων, όλες οι προηγούμενες ασύρματες τεχνολογίες είναι "διασκεδαστικές", αλλά το 5G προσθέτει μια νέα διάσταση για να κάνει πραγματικά την κινητή ζωή πραγματικότητα. Αναμένεται ότι το νέο δίκτυο 5G θα βελτιώσει τις υπηρεσίες και τις εφαρμογές που

παρέχει. Σε αντίθεση με το 3G, το οποίο δίνει προτεραιότητα στον φορέα εκμετάλλευσης, και το 4G, το οποίο δίνει προτεραιότητα στην υπηρεσία, αυτή η τεχνολογία βλέπει τον χρήστη ως πρωταρχικό μέλημα. Λόγω της εκθετικής αύξησης της ζήτησης των χρηστών, η πολλαπλή πρόσβαση με διαίρεση δέσμης (BDMA), μια τεχνολογία πρόσβασης αιχμής, και η πολλαπλή πρόσβαση με τράπεζα φίλτρων πολλαπλών φορέων (FBMC) θα αντικατασταθούν από τα δίκτυα 5G. Στην έννοια BDMA, ο σταθμός βάσης αναθέτει μια ορθογώνια δέσμη για να συνδεθεί με τους κινητούς χρήστες. Η ποιότητα και η χωρητικότητα του συστήματος θα αυξηθούν ως αποτέλεσμα του τρόπου με τον οποίο αυτή η δέσμη που χρησιμοποιεί την τεχνολογία δέσμης θα διαιρείται με βάση τις τοποθεσίες των κινητών χρηστών.

Οι δυσκολίες και οι απαιτήσεις που προκύπτουν από τη γρήγορη εξέλιξη της τεχνολογίας, τις οποίες τα δίκτυα τέταρτης γενιάς δεν μπορούν να διαχειριστούν με επιτυχία, είναι αυτές που οδήγησαν στην ανάπτυξη των ασύρματων δικτύων επικοινωνίας πέμπτης γενιάς. Υψηλότερη χωρητικότητα, υψηλότερος ρυθμός μετάδοσης, χαμηλότερη καθυστέρηση, μαζική συνδεσιμότητα συσκευών και φυσικά φθηνότερο κόστος είναι μερικές από αυτές τις απαιτήσεις. Ενώ τα δίκτυα 5G είναι ταχύτερα από τα σημερινά, είναι πιο πολύπλοκα. Δεν είναι αδύνατο να αντικαταστήσουν το οικιακό WiFi προσφέροντας υψηλότερες ταχύτητες και καλύτερη κάλυψη, ακόμη και για ρυθμούς της τάξης των 10 Gpbs. Υπάρχουν επιχειρήματα για δεκαπλάσιες ταχύτητες σε σύγκριση με το 4G (LTE), οι οποίες θα επιτρέψουν στους καταναλωτές να κατεβάζουν ταινίες γρήγορα και να βιώνουν περιβάλλοντα εικονικής πραγματικότητας χωρίς την παραμικρή καθυστέρηση. Επειδή μπορεί να διαχειρίζεται αποτελεσματικότερα τις τεχνολογίες και να παρέχει στους χρήστες ευεργετική ακουστική, η τεχνολογία 5G έχει ένα πολλά υποσχόμενο μέλλον. Είναι πιθανό ότι η μελλοντική τεχνολογία θα κυριαρχήσει στη διεθνή αγορά (Salah et al., 2021: 150-158).

2.3 Καινοτομίες δικτύων 5g

Οι διακρίσεις μεταξύ του 5G και των παλαιότερων δικτύων πρέπει να γίνουν για να κατανοήσουμε γιατί είμαστε τώρα έτοιμοι να υποδεχτούμε τη νέα γενιά. Η επικράτηση των ασύρματων επικοινωνιών έχει αναμφίβολα αυξηθεί στη σύγχρονη εποχή σε ύψη που δεν θα μπορούσαμε ποτέ εύκολα να προβλέψουμε. Τα ασύρματα

δίκτυα χρησιμοποιούνται πλέον για τη σύνδεση διαφόρων τύπων υπολογιστών μεταξύ τους.

Οι πρωταρχικές διακρίσεις μεταξύ του 5G και των προηγούμενων γενεών δικτύων κινητής τηλεφωνίας περιλαμβάνουν:

- Πέρα από το κινητό διαδίκτυο, τα δίκτυα 5G παρέχουν ευρυζωνικές ασύρματες επικοινωνίες για το Διαδίκτυο των πραγμάτων.
- Σε σύγκριση με το 4G, τα δίκτυα 4,5G (LTE Advanced) αύξησαν τις ταχύτητες δεδομένων.
- Όλες οι υπηρεσίες IP (φωνή και δεδομένα), μια γρήγορη ευρυζωνική εμπειρία διαδικτύου και ενοποιημένες αρχιτεκτονικές και πρωτόκολλα δικτύου εισήχθησαν από τα δίκτυα 4G.
- Τα οικοσυστήματα κινητών εφαρμογών ήταν επιτυχημένα λόγω της πραγματικά πανταχού παρούσας εμπειρίας κινητού διαδικτύου που έφεραν τα δίκτυα 3.5G.
- Αν και τα δίκτυα 3G βελτίωσαν την εμπειρία του κινητού διαδικτύου, δυσκολεύτηκαν να υιοθετήσουν ευρέως τις υπηρεσίες δεδομένων.
- Με το GPRS και το EDGE, τα δίκτυα 2,5G και 2,75G, αντίστοιχα, βελτίωσαν τις υπηρεσίες δεδομένων.
- Οι ψηφιακές κυψελοειδείς υπηρεσίες φωνής, οι στοιχειώδεις υπηρεσίες δεδομένων (SMS, πλοήγηση στο Διαδίκτυο WAP) και οι υπηρεσίες περιαγωγής δικτύου εισήχθησαν από τα δίκτυα 2G.
- Οι αναλογικές υπηρεσίες φωνής έχουν πλέον κινητικότητα χάρη στα δίκτυα 1G.

Η επόμενη γενιά συνδεσιμότητας στο κινητό διαδίκτυο, ή δίκτυα 5G, παρέχει συνδέσεις σε smartphones και άλλες συσκευές με ταχύτερους ρυθμούς από ποτέ και με μεγαλύτερη αξιοπιστία. Το δίκτυο 5G θα είναι σε θέση να παρέχει συνδέσεις που θα είναι έτη φωτός ταχύτερες από τις υπάρχουσες συνδέσεις, με τυπικές ταχύτητες λήψης (περίπου 1GBps) να αποτελούν τον κανόνα, σύμφωνα με τις πιο πρόσφατες μελέτες. Ο κύριος στόχος του δικτύου 5G είναι η ενσωμάτωση ριζοσπαστικών τεχνολογιών που θα εγγυώνται αυξημένη χωρητικότητα, μειωμένη καθυστέρηση και αυξημένη εμπιστευτικότητα. Αυτές περιλαμβάνουν μια σειρά από τεχνολογίες αιχμής, όπως η μαζική MIMO, η επικοινωνία μεταξύ συσκευών και η εικονική διαχείριση λειτουργιών δικτύου (NFV) (Salah et al., 2021: 150-158).

Υπάρχουν διάφοροι εναλλακτικοί στόχοι για το 5G. Πρώτα απ' όλα, δεδομένου ότι η αύξηση των ρυθμών δεδομένων είναι ένας από τους κύριους στόχους του 5G, οι χρήστες θα πρέπει να αναμένουν ότι οι υπηρεσίες 5G θα είναι τουλάχιστον δέκα φορές ταχύτερες από το 4G. Επιπλέον, το 5G επιδιώκει την εξοικονόμηση ενέργειας εκτός από χρήματα. Το 5G θα μειώσει επίσης την καθυστέρηση και θα ενισχύσει τη χωρητικότητα του συστήματος. Όταν ολοκληρώνετε την πληκτρολόγηση μιας διεύθυνσης URL στον ιστότοπο του κινητού σας, η σελίδα χρειάζεται μερικά δευτερόλεπτα για να φορτώσει ως αποτέλεσμα δύο λόγων. Αυτό είναι ένα παράδειγμα ελαχιστοποίησης της καθυστέρησης. Ο χρόνος που απαιτείται για την επιβεβαίωση του αιτήματος και για τη μεταφορά όλων των κειμένων, των φωτογραφιών και των βίντεο στην κινητή συσκευή σας, αντίστοιχα. Ένα άλλο σημαντικό πλεονέκτημα του 5G είναι ότι θα επιτρέψει την ευρεία συνδεσιμότητα των συσκευών. Με άλλα λόγια, το 5G θα είναι σε θέση να υποστηρίζει πολλαπλές ευρυζωνικές συνδέσεις που θα μεταφέρουν gigabytes αιτούμενου εύρους ζώνης ανά πάσα στιγμή, καθώς και μαζικό MTC που θα συνδέει διάφορους αισθητήρες και μηχανήματα. Η επικοινωνία τύπου κρίσιμης μηχανής (MTC) είναι απαραίτητη για εφαρμογές όπως η εικονική πραγματικότητα που απαιτούν άμεση ανατροφοδότηση.

Σε μια ζώνη υψηλών συχνοτήτων του ασύρματου φάσματος, περίπου μεταξύ 30 και 300 GHz, θα λειτουργεί το δίκτυο 5G. Υψηλότερη ταχύτητα και εύρος ζώνης συνεπάγεται η υψηλότερη συχνότητα. Παρόλο που τα δεδομένα μπορούν να κινηθούν και να μεταφερθούν με πολύ γρήγορους ρυθμούς σε αυτό το φάσμα ηλεκτρομαγνητικών κυμάτων λόγω των χαμηλών συχνοτήτων του, δεν μπορούν να ταξιδέψουν τόσο μακριά όσο στα δίκτυα 4G. Είναι σημαντικό να σημειωθεί ότι επειδή οι τοίχοι, τα παράθυρα, οι οροφές και τα κτίρια μειώνουν αυτά τα κύματα, τα οποία έχουν επίσης υψηλή συχνότητα, είναι πολύ δύσκολο να περάσουν μέσα από αυτά. Περισσότερες συσκευές θα μπορούν να συνδέονται ταυτόχρονα στο ίδιο δίκτυο λόγω της υψηλότερης χωρητικότητας της νέας τεχνολογίας. Το δίκτυο 5G δεν προορίζεται μόνο για τη βασική χρήση κινητών τηλεφώνων. Οι τεχνολογικές εξελίξεις, όπως θερμοστάτες, αισθητήρες, οχήματα και ρομπότ, θα μπορούν να συνδεθούν σε δίκτυα πέμπτης γενιάς. Το παλαιότερο δίκτυο δεν διέθετε την απαραίτητη χωρητικότητα για τη διαχείριση του τεράστιου όγκου δεδομένων που μετέδιδαν οι συσκευές.

Η υστέρηση μεταξύ των συσκευών και του διακομιστή θα εξαφανιστεί χάρη στο 5G. Ωστόσο, αυτό σημαίνει ότι προκειμένου να αναπτυχθεί το 5G και να δοθεί η

ίδια κάλυψη, οι σημερινοί πάροχοι ασύρματου διαδικτύου θα πρέπει να ανακατασκευάσουν και να πολλαπλασιάσουν τις κεραίες, τοποθετώντας αυτές τις κεραίες σε κάθε φανάρι, σε κάθε πλευρά ενός κτιρίου και ενδεχομένως ακόμη και σε κάθε δωμάτιο. Ωστόσο, αυτό δεν συμβαίνει στα σημερινά δίκτυα 4G επειδή τα εμπόδια δεν αποτελούν σημαντικό ζήτημα και οι κεραίες μπορούν να τοποθετηθούν μακριά η μία από την άλλη. Αυτό δείχνει ότι ακόμη και όταν το δίκτυο πέμπτης γενιάς εισαχθεί, δεν θα πάρει τη θέση του προδρόμου του αλλά μάλλον θα τον συμπληρώσει - τουλάχιστον για τα πρώτα χρόνια μετά την εισαγωγή και τη χρήση του. Στην κινητή τηλεφωνία χρησιμοποιούνται ραδιοσυχνότητες, οι οποίες χωρίζονται σε ζώνες και καθεμία από τις οποίες έχει μοναδικές ιδιότητες. Ενώ το δίκτυο 5G θα λειτουργεί σε υψηλότερες ζώνες συχνοτήτων (30-90 GHz) χρησιμοποιώντας κύματα χιλιοστού (mmWaves), τα οποία έχουν μήκος κύματος μεταξύ 1 και 10 χιλιοστών, το δίκτυο 4G λειτουργεί σε ραδιοσυχνότητες κάτω των 6 GHz (Salah et al., 2021: 150-158).

3. Τεχνολογίες δικτύων 5g

Απαιτείται σημαντικός επανασχεδιασμός της κυψελοειδούς αρχιτεκτονικής 5G προκειμένου να ικανοποιηθούν οι απαιτήσεις των χρηστών και να ξεπεραστούν τα προβλήματα που είναι απαραίτητα για να χαρακτηριστεί σύστημα 5ης γενιάς. Τεχνικές όπως το SDN και το NFV πρέπει να χρησιμοποιηθούν προκειμένου να επιτευχθούν οι προαναφερθείσες απαιτήσεις. Λόγω της βελτιωμένης ευελιξίας και επεκτασιμότητας του 5G, οι πάροχοι υπηρεσιών θα εφαρμόσουν τις προαναφερθείσες τεχνολογίες καθώς και άλλες για την επίλυση πρόσθετων προβλημάτων (Salah et al., 2021: 150-158).

Νέες ραδιοσυχνότητες

Δύο ζώνες συχνοτήτων συνθέτουν τη διεπαφή αέρα NR (New Radio) για το 5G που έχει καθορίσει η 3GPP. Η FR2 (mmWave) και η FR1 (κάτω από 6GHz), η καθεμία με μοναδικά χαρακτηριστικά.

Massive MIMO (Multiple Input Multiple Output)

Οι μαζικές κεραίες MIMO χρησιμοποιούν πολλές κεραίες και MIMO πολλαπλών χρηστών για να ενισχύσουν την απόδοση του τομέα και την πυκνότητα χωρητικότητας. Κάθε κεραία μπορεί να διαθέτει στοιχεία ραδιοπομποδέκτη και ελέγχεται μεμονωμένα (Salah et al., 2021: 150-158).

Beamforming

Τα ραδιοκύματα κατευθύνονται σε έναν συγκεκριμένο στόχο χρήστη χρησιμοποιώντας διαμόρφωση δέσμης. Αυτό επιτυγχάνεται με την ανάμειξη υλικών με τρόπο που παρεμβαίνει εποικοδομητικά σε ορισμένα σήματα και καταστροφικά σε άλλα. Ως αποτέλεσμα βελτιώνονται οι ρυθμοί μεταφοράς δεδομένων και η ποιότητα του σήματος. Η πέμπτη γενιά ασύρματων δικτύων χρησιμοποιεί κεραίες σταδιακής συστοιχίας για τη διαμόρφωση δέσμης (Βλαχόπουλος, 2007).

SDN (Software Defined Networking)

Με τη χρήση της τεχνολογίας SDN, οι σταθμοί βάσης μπορούν να προγραμματίζονται και να διαχειρίζονται από έναν κεντρικό ελεγκτή. Η αρχιτεκτονική SDN αποτελείται από τρία στοιχεία: εφαρμογή, έλεγχος και υποδομή. Πρόκειται για μια στρατηγική για ασύρματα δίκτυα που επιτρέπει στους διαχειριστές να διοικούν και να ελέγχουν τους διακομιστές στο πιο βασικό επίπεδο λειτουργικότητας.

NFV (Network Function Virtualization)

Ο NFV είναι υπεύθυνος για την κληρονομικότητα. Με αυτό εννοούμε ότι το NFV αντιπροσωπεύει μια συλλογή λειτουργιών δικτύου που συνδυάζονται και ενσωματώνονται για να επιτρέψουν τη δημιουργία υπηρεσιών που προηγουμένως

ήταν δυνατές μόνο σε παλαιότερες γενιές δικτύων. Το NFV αντικαθιστά την παραδοσιακή εικονικοποίηση διακομιστών, η οποία θα μπορούσε να προγραμματίσει πολυάριθμες εικονικές μηχανές με ποικίλα λειτουργικά συστήματα, προγράμματα και λειτουργίες. Μεταδίδει εφαρμογές για δίκτυα ή επικοινωνίες, ειδικά αυτές που εκτελούνται σε εξειδικευμένες πλατφόρμες (Salah et al., 2021: 150-158).

UDD (Ultra Dense Deployments)

Οι απαιτήσεις της επόμενης τεχνολογίας 5G δεν μπορούν να καλυφθούν από το διαθέσιμο φάσμα. Το εύρος συχνοτήτων στο οποίο θα λειτουργούν τα δίκτυα 5G θα είναι διαφορετικό από εκείνο των προηγούμενων γενεών δικτύων. Η ευρεία ανάπτυξη μικρών κυψελών, οι οποίες θα συνυπάρχουν με Microcells, Macrocells και άλλα συστήματα όπως Wi-Fi, LTE/A και HSPA για τη δημιουργία ετερογενών δικτύων, αποτελεί κρίσιμο στοιχείο του 5G. Τα cells που προκύπτουν είναι ιδιαίτερα πυκνά. Επειδή αυτό έχει ως αποτέλεσμα τη μέγιστη αξιοποίηση του εύρους ζώνης και τη μείωση των απωλειών μετάδοσης, η συνακόλουθη πύκνωση των δικτύων είναι ζωτικής σημασίας.

Cloud Computing

Με τη βοήθεια του υπολογιστικού νέφους, οι χρήστες μπορούν να έχουν πρόσβαση σε ένα ευρύ φάσμα εικονικών πόρων. Πρόκειται για μια μέθοδο με την οποία οι πάροχοι υπηρεσιών παρέχουν στους καταναλωτές πρόσβαση σε εικονικούς πόρους. Το IaaS, το PaaS και το SaaS είναι τα τρία επίπεδα του υπολογιστικού νέφους (Salah et al., 2021: 150-158).

Millimeter Wave (mmWave)

Συζητήσαμε προηγουμένως τις πρόσθετες ραδιοσυχνότητες που διατίθενται από τα δίκτυα 5G καθώς και τις δύο κατηγορίες εκπομπής, FR1 και FR2. Η FR2 (mmWave), η οποία μεταδίδει δεδομένα με ρυθμό πολλαπλών giga bits ανά δευτερόλεπτο στη συσκευή του χρήστη, είναι μια πολλά υποσχόμενη τεχνολογία για τα δίκτυα 5G. Λειτουργεί στην περιοχή συχνοτήτων 30 GHz έως 300 GHz. Όταν η επικοινωνία D2D χρησιμοποιείται σε κυψελοειδή δίκτυα mmWave, μπορούν να

πραγματοποιηθούν περισσότερες άμεσες συνδέσεις ταυτόχρονα, αυξάνοντας τη χωρητικότητα του δικτύου (Βλαχόπουλος, 2007).

HetNets (Heterogenous Networks)

Η κατασκευή πολυάριθμων μικρών κυψελών, η οποία οδηγεί σε ετερογενή δίκτυα, είναι μια μέθοδος αντιμετώπισης της τεράστιας αύξησης της κίνησης στα ασύρματα δίκτυα. Αποτελούνται από μικρές κυψέλες με χαμηλή απόδοση ισχύος, αυξάνοντας την κάλυψη του σταθμού βάσης και τη χωρητικότητα του δικτύου.

D2D Communication (Device to Device)

Στα κινητά δίκτυα, η άμεση επικοινωνία μεταξύ χρηστών (D2D) περιγράφεται ως η επικοινωνία που πραγματοποιείται μεταξύ δύο χρηστών χωρίς την ανάγκη σταθμού βάσης ή πυρήνα δικτύου. Υπό ορισμένες συνθήκες, οι επικοινωνίες D2D μπορούν να βελτιώσουν σημαντικά τη φασματική απόδοση του δικτύου (Salah et al., 2021: 150-158).

4. Κυβερνοασφάλεια και 5g

Η ανάπτυξη του 5G, της πέμπτης γενιάς δικτύων κινητών επικοινωνιών, ενέχει απειλές για την ασφάλεια και η Ευρωπαϊκή Επιτροπή ενέκρινε την κοινή εργαλειοθήκη μέτρων μετριασμού που πέτυχαν τα κράτη μέλη της ΕΕ. Με τη χρήση της εργαλειοθήκης, τα κράτη μέλη συμφωνούν να προχωρήσουν από κοινού με βάση μια αμερόληπτη αξιολόγηση των εντοπισμένων κινδύνων και των λογικών στρατηγικών μετριασμού. Σύμφωνα με την Margarethe Westeyer, Εκτελεστική Αντιπρόεδρο για μια Ευρώπη έτοιμη για την ψηφιακή εποχή, η τεχνολογία αυτή υποστηρίζει την ιατρική ακριβείας, τα ολοκληρωμένα ενεργειακά συστήματα από όλες τις ανανεώσιμες πηγές και την εξατομικευμένη θεραπεία (Salah et al., 2021: 150-158).

Θετικά αποτελέσματα θα προκύψουν από αυτή την τεχνολογία, αλλά μόνο εάν οι χρήστες μπορούν να διασφαλίσουν την ασφάλεια των δικτύων τους, επιτρέποντας σε όλους να επωφεληθούν από τις τεχνολογικές εξελίξεις χωρίς να

θέσουν σε κίνδυνο την ασφάλεια της εσωτερικής αγοράς. Με έσοδα που αναμένεται να φθάσουν τα 225 δισεκατομμύρια ευρώ παγκοσμίως το 2025, η τεχνολογία 5G που αλλάζει τα δεδομένα αποτελεί θεμελιώδες στοιχείο της ανταγωνιστικότητας της Ευρώπης στην παγκόσμια αγορά και η ασφάλεια στον κυβερνοχώρο στον τομέα αυτό είναι απαραίτητη για τη διατήρηση της στρατηγικής ανεξαρτησίας της Ένωσης. Περιλαμβάνει δισεκατομμύρια διασυνδεδεμένα συστήματα και αντικείμενα, κρίσιμους τομείς όπως (Βλαχόπουλος, 2007):

• η ενέργεια
• οι μεταφορές
• οι τραπεζικές συναλλαγές
• η υγεία
• συστήματα βιομηχανικού ελέγχου που μεταφέρουν ευαίσθητες πληροφορίες και υποστηρίζουν συστήματα ασφαλούς λειτουργίας.

Ωστόσο, λόγω της πιο αποκεντρωμένης αρχιτεκτονικής, της έξυπνης υπολογιστικής ισχύος στην άκρη του δικτύου, της απαίτησης για περισσότερες κεραίες και της αυξημένης εξάρτησης από το λογισμικό, τα δίκτυα 5G παρουσιάζουν περισσότερες ευκαιρίες για επιθέσεις. Οι απειλές για την ασφάλεια στον κυβερνοχώρο επεκτείνονται και γίνονται όλο και πιο περίπλοκες. Ως αποτέλεσμα του γεγονότος ότι πολλές βασικές υπηρεσίες θα εξαρτώνται από το 5G, η διασφάλιση της ασφάλειας του δικτύου έχει ύψιστη στρατηγική σημασία για ολόκληρη την ΕΕ.

Προκειμένου να διασφαλιστεί η ασφάλεια των υποδομών 5G και της αλυσίδας εφοδιασμού 5G, η Επιτροπή θα συνεχίσει να είναι ενωμένη στο θέμα αυτό και θα ανταποκριθεί στα αιτήματα των κρατών μελών χρησιμοποιώντας, όπου χρειάζεται, όλα τα διαθέσιμα εργαλεία:

- κανονισμοί για την ασφάλεια στον κυβερνοχώρο και τις τηλεπικοινωνίες,
- συντονισμός σε επίπεδο ΕΕ στους τομείς της τυποποίησης και της πιστοποίησης,
- ένα σύστημα ρύθμισης των άμεσων ξένων επενδύσεων για τη διασφάλιση της ευρωπαϊκής αλυσίδας εφοδιασμού 5G,
- το εμπόριο των αμυντικών όπλων,
- κατευθυντήριες γραμμές διαγωνισμού,

- Κατά τη διάρκεια των δημόσιων συμβάσεων, βεβαιωθείτε ότι λαμβάνονται δεόντως υπόψη τα ζητήματα ασφάλειας.
- Χρηματοδοτικά προγράμματα της ΕΕ, διασφαλίζοντας ότι οι δικαιούχοι τηρούν τα απαραίτητα πρότυπα ασφαλείας (Salah et al., 2021: 150-158).

5. Ζητήματα απειλής και ασφάλειας

Το δίκτυο μας παρέχει μια πληθώρα γρήγορων πληροφοριών, μέσω του δικτύου θα μοιραστούμε τις πληροφορίες μας και μπορούμε να πούμε ότι το δίκτυο έχει γίνει μέρος της ζωής μας, φέρνει μεγάλη ευκολία στην εργασία μας, τη ζωή και τη μάθηση, αλλά με την εξαίρεση πέρα από αυτό, μας έχει επίσης δώσει πολλά προβλήματα. Ο αυξανόμενος αριθμός περιστατικών που σχετίζονται με την ασφάλεια πληροφοριών (IS), τα οργανωμένα εγκλήματα και οι απάτες phishing σημαίνουν ότι η IS αξίζει πολύ μεγαλύτερη προσοχή. Η ασφάλεια δικτύου θεωρείται γενικά ως η παροχή προστασίας στα όρια ενός οργανισμού, κρατώντας έξω τους εισβολείς (hackers). η ασφάλεια πληροφοριών, ωστόσο, επικεντρώνεται ρητά στην προστασία των πόρων δεδομένων από επιθέσεις κακόβουλου λογισμικού ή από απλά λάθη των ανθρώπων εντός ενός οργανισμού με τη χρήση τεχνικών πρόληψης απώλειας δεδομένων (DLP). Τα μέτρα ασφάλειας δικτύων είναι απαραίτητα για την προστασία των δεδομένων κατά τη μετάδοσή τους, επειδή σχεδόν όλες οι επιχειρήσεις, οι κυβερνητικοί και οι ακαδημαϊκοί οργανισμοί διασυνδέουν τα συστήματά τους με μια συλλογή δικτύων που αναφέρονται ως Διαδίκτυο (Acharya et al., 2013: 401-407).

5.1 Malware- Κακόβουλο Λογισμικό

Το κακόβουλο λογισμικό (malware), συντομογραφία των λέξεων κακόβουλο λογισμικό, είναι λογισμικό σχεδιασμένο για να βλάψει ή να αποκτήσει κρυφή

πρόσβαση σε ένα σύστημα υπολογιστή χωρίς τη συγκατάθεση του κατόχου του. Το κακόβουλο λογισμικό περιλαμβάνει υπολογιστικούς ιούς, σκουλήκια, δούρειους ίππους, κατασκοπευτικό λογισμικό, αθέμιτο διαφημιστικό λογισμικό, scareware, crimeware, τα περισσότερα rootkits και άλλο κακόβουλο και ανεπιθύμητο λογισμικό ή πρόγραμμα. Ιοί και σκουλήκια: Ο όρος ιός χρησιμοποιείται εδώ και πολύ καιρό γενικά για να περιγράψει οποιαδήποτε απειλή για τον υπολογιστή, αλλά στην πραγματικότητα αναφέρεται ειδικά σε κακόβουλο λογισμικό που εισάγει κακόβουλο κώδικα σε υπάρχοντα έγγραφα ή προγράμματα και στη συνέχεια εξαπλώνεται με διάφορα μέσα. Σήμερα, οι ιοί εξακολουθούν να αποτελούν μακράν τον πιο συνηθισμένο τύπο απειλής για την ασφάλεια του δικτύου, και πάνω από το 90 τοις εκατό των ιών εξαπλώνονται μέσω συνημμένων σε μηνύματα ηλεκτρονικού ταχυδρομείου. Τόσο οι ιοί όσο και τα σκουλήκια συχνά εργάζονται για να ανοίξουν νέες τρύπες στην ασφάλεια του δικτύου σας, προκειμένου να επιτρέψουν σε ακόμη πιο επικίνδυνες απειλές ασφαλείας να μολύνουν το δίκτυό σας (Acharya et al., 2013: 401-407).

5.2 Trojan Horses

Δούρειος ίππος είναι κάθε πρόγραμμα που καλεί τον χρήστη να το εκτελέσει, κρύβοντας ένα επιβλαβές ή κακόβουλο ωφέλιμο φορτίο. Το ωφέλιμο φορτίο μπορεί να επιδράσει άμεσα και μπορεί να οδηγήσει σε πολλές ανεπιθύμητες συνέπειες, όπως η διαγραφή των αρχείων του χρήστη ή η περαιτέρω εγκατάσταση κακόβουλου ή ανεπιθύμητου λογισμικού (Acharya et al., 2013: 401-407).

Οι δούρειοι ίπποι, σε αντίθεση με τους ιούς και τα σκουλήκια, δεν αυτοαναπαράγονται και δεν αναπαράγονται μολύνοντας άλλα αρχεία, αν και ορισμένοι μπορούν να μεταφέρουν ένα σκουλήκι ή έναν ιό. Αντ' αυτού, είναι ένα κομμάτι κώδικα προγραμματισμού μεταμφιεσμένο σε άλλο πρόγραμμα ή αρχείο. Οι χρήστες εξαπλώνουν τα Trojans εκτελώντας ή εγκαθιστώντας ένα ελκυστικό πρόγραμμα, όπως όμορφες προφυλάξεις οθόνης, διασκεδαστικά παιχνίδια ή άλλα προγράμματα που θεωρούν νόμιμα. Μαζί με αυτά τα προγράμματα, το Trojan εγκαθιστά ένα άλλο που προκαλεί προβλήματα. Κάποια από αυτά είναι μικροενοχλητικά, όπως αναδυόμενα παράθυρα ή αλλαγές στην αρχική σελίδα του χρήστη. Άλλα προκαλούν μεγαλύτερη ζημιά, όπως η διαγραφή αρχείων, η κλοπή πληροφοριών με την εγκατάσταση ενός keystroke logger ή το άνοιγμα μιας

κερκόπορτας για μη εξουσιοδοτημένους σκοπούς. Πολλά Trojans προσκαλούνται στους υπολογιστές όταν ένας χρήστης κάνει κλικ σε έναν κακό σύνδεσμο σε spam e-mail.

5.3 Rootkits

Μόλις εγκατασταθεί ένα κακόβουλο πρόγραμμα σε ένα σύστημα, είναι σημαντικό να παραμείνει κρυμμένο, ώστε να αποφύγει τον εντοπισμό και την απολύμανση. Το ίδιο ισχύει και όταν ένας ανθρώπινος εισβολέας εισβάλλει απευθείας σε έναν υπολογιστή. Οι τεχνικές που είναι γνωστές ως rootkits επιτρέπουν αυτή την απόκρυψη, τροποποιώντας το λειτουργικό σύστημα του κεντρικού υπολογιστή έτσι ώστε το κακόβουλο λογισμικό να είναι κρυμμένο από τον χρήστη (Acharya et al., 2013: 401-407).

5.4 Spam

Spam είναι η χρήση συστημάτων ηλεκτρονικών μηνυμάτων για την αποστολή ανεπιθύμητων μαζικών μηνυμάτων αδιακρίτως. Ανάλογα με την αναφερόμενη πηγή, τα ανεπιθύμητα μηνύματα αποτελούν το 70 έως 84% των καθημερινών μηνυμάτων ηλεκτρονικού ταχυδρομείου που αποστέλλονται σε όλο τον κόσμο. Όλο αυτό το spam έχει ως αποτέλεσμα την απώλεια παραγωγικότητας δισεκατομμυρίων δολαρίων και δημιουργεί μια συνεχώς αυξανόμενη ανάγκη για πόρους πληροφορικής για το φιλτράρισμα αυτής της ενοχλητικής και δυνητικά κακόβουλης απειλής (Acharya et al., 2013: 401-407).

5.5 Phising

Το "phishing" αναφέρεται σε μηνύματα ηλεκτρονικού ταχυδρομείου ανεπιθύμητης αλληλογραφίας που έχουν σχεδιαστεί για να εξαπατήσουν τους παραλήπτες ώστε να κάνουν κλικ σε έναν σύνδεσμο προς έναν ανασφαλή ιστότοπο. Συνήθως, οι απόπειρες phishing εκτελούνται για να υποκλέψουν πληροφορίες λογαριασμού για ιστότοπους ηλεκτρονικού εμπορίου όπως το eBay, επεξεργαστές πληρωμών όπως το PayPal ή ιστότοπους κανονικών χρηματοπιστωτικών ιδρυμάτων. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου phishing σας παρέχει έναν σύνδεσμο για να κάνετε κλικ, ο οποίος θα σας μεταφέρει σε μια σελίδα όπου μπορείτε να

καταχωρίσετε εκ νέου όλα τα στοιχεία του λογαριασμού σας, συμπεριλαμβανομένων των αριθμών πιστωτικών καρτών ή/και των κωδικών πρόσβασης. Φυσικά, οι ιστότοποι αυτοί δεν είναι ο πραγματικός ιστότοπος της τράπεζας, παρόλο που μοιάζουν με αυτόν.

Τα κινητά τηλέφωνα της εταιρείας σας μπορεί επίσης να μην είναι ασφαλή, καθώς τα μηνύματα SMS χρησιμοποιούνται πλέον συχνά ως ένας νέος τύπος phishing που ονομάζεται smishing. Μόλις το smishing είναι επιτυχές, άλλοτε απελευθερώνονται στο κινητό τηλέφωνο άλλα κακόβουλα προγράμματα, όπως Trojans. Αυτά τα Trojans δημιουργούν στη συνέχεια αθόρυβα μηνύματα κειμένου υψηλού κόστους, τα οποία επιβαρύνουν το λογαριασμό του αποστολέα. Ορισμένοι εγκληματίες χρησιμοποιούν επίσης το VoIP (Voice over internet protocol) για την αποστολή μηνυμάτων phishing. Αυτά προσπαθούν να μπερδέψουν τους ανθρώπους ώστε να καλέσουν τον παρεχόμενο αριθμό -συνήθως έναν αυτοματοποιημένο αριθμό κλήσης VoIP- και να αποκαλύψουν τα στοιχεία της πιστωτικής κάρτας, τα οποία καταγράφονται σε ηχητική μορφή.

Το phishing σε όλες τις ποικιλίες του είναι ένα τεράστιο και αυξανόμενο πρόβλημα για τους διαχειριστές ασφάλειας δικτύων και τους ιδιοκτήτες επιχειρήσεων. Καθώς όλοι γινόμαστε όλο και πιο διασυνδεδεμένοι και αποκτούμε πρόσβαση σε όλο και περισσότερες προσωπικές πληροφορίες μέσω δικτύων, οι ευκαιρίες για επιθέσεις από phishers γίνονται όλο και περισσότερες. Για την προστασία του δικτύου κάποιου, καθίσταται όλο και πιο σημαντικό να εκπαιδεύετε τους υπαλλήλους σας σχετικά με τους πιο συνηθισμένους τρόπους με τους οποίους οι χάκερ προσπαθούν να αλιεύσουν τις πληροφορίες των λογαριασμών σας (Acharya et al., 2013: 401-407).

5.6 Packet Sniffers

Οι ανιχνευτές πακέτων καταγράφουν ροές δεδομένων σε ένα δίκτυο, επιτρέποντας έτσι τη συλλογή ευαίσθητων δεδομένων όπως ονόματα χρηστών, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών. Το αποτέλεσμα, όπως είναι αναμενόμενο, είναι η απώλεια δεδομένων, εμπορικών μυστικών ή υπολοίπων διαδικτυακών λογαριασμών. Ειδικά για τους διαχειριστές δικτύων, ακόμη μεγαλύτερες απώλειες μπορεί να προκύψουν από αγωγές λόγω μη συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων. Τα packet sniffers λειτουργούν παρακολουθώντας και καταγράφοντας όλες τις πληροφορίες που προέρχονται και

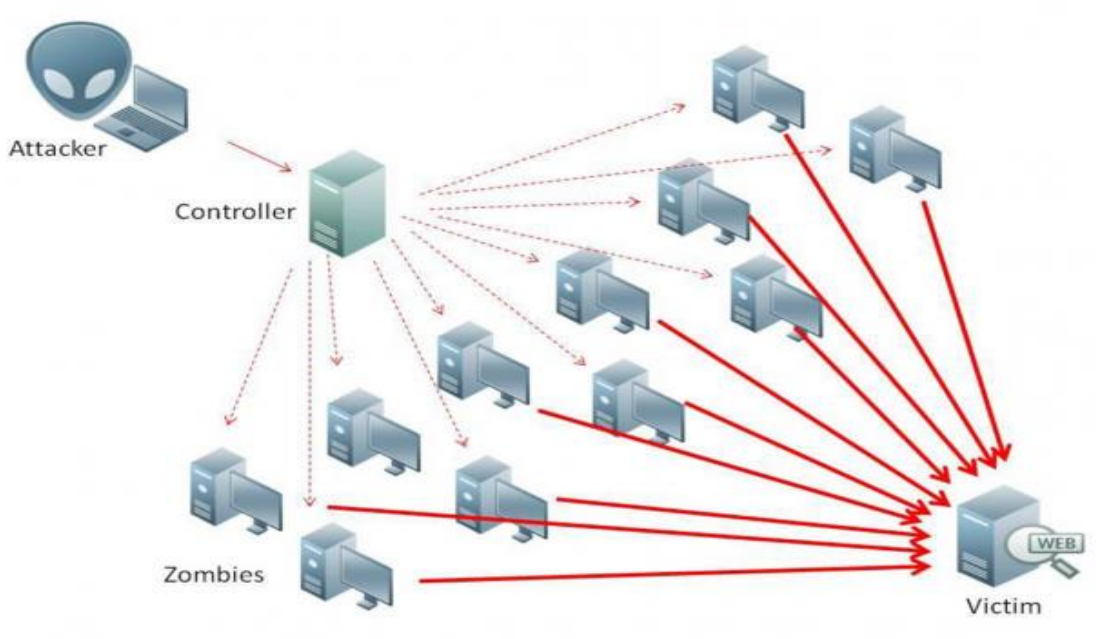
πηγαίνουν στον υπολογιστή σας μέσω ενός παραβιασμένου δικτύου. Έτσι, για να είναι αποτελεσματικός, ο ανιχνευτής πακέτων πρέπει πρώτα να έχει πρόσβαση στο δίκτυο που χρησιμοποιείτε. Ο πιο συνηθισμένος τρόπος για να γίνει αυτό είναι μέσω της χρήσης κάτι που ονομάζεται honeypots. Τα honeypots είναι απλά μη ασφαλή σημεία πρόσβασης wifi που εγκαθιστούν οι χάκερς και παγιδεύουν τους ανθρώπους για να τα χρησιμοποιήσουν. Συνήθως, αυτά τα honeypots εγκαθίστανται σε δημόσιους χώρους, όπως αεροδρόμια, και το δίκτυο wifi φέρει τον τίτλο "Free Public Wi-Fi". Οι ανυποψίαστοι χρήστες εγγράφονται στο κατεστραμμένο δίκτυο και ο packet sniffer παίρνει τις προσωπικές τους πληροφορίες όταν εισάγουν πληροφορίες όπως οι πληροφορίες της πιστωτικής τους κάρτας σε μια ιστοσελίδα (Acharya et al., 2013: 401-407).

5.7 Αποκέντρωση στο 5G

Τα δίκτυα πριν απο το 5G είχαν λιγότερα σημεία όπου χρησιμοποιείται υλικό, πράγμα το οποίο διευκόλυνε τους ελέγχους ασφαλείας και τη συντήρηση. Τα δυναμικά συστήματα πλέον που χρησιμοποιούνται στο 5G που βασίζονται κυρίως σε λογισμικό προσφέρουν πολύ περισσότερα σημεία δρομολόγησης της κυκλοφορίας. Για να μπορέσουν αυτά τα σημεία να είναι ασφαλείς και να εγγυηθουν στους κατόχους τους θα πρέπει να παρακολουθούνται διαρκώς. Το γεγονός αυτό εκτός του οτι είναι πολύ δύσκολο να ελεγχθεί είναι αρκετά επίφοβο να θέσει σε κίνδυνο και άλλα μέρη του δικτύου

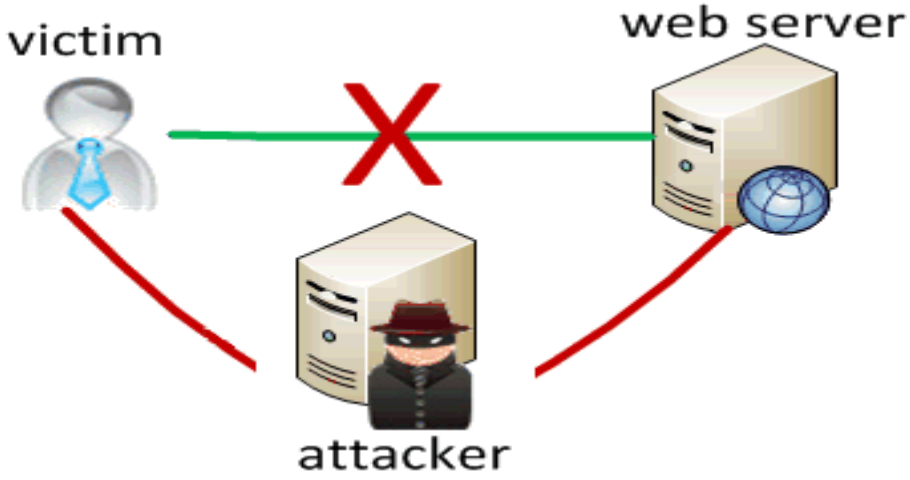
5.8 Ευπάθειες -Τύποι Επιθέσεων.

- **Botnet Attacks:** Μία τέτοιου τύπου επίθεση είναι μία μορφή κυβερνοεπίθεσης η οποία πραγματοποιείται απο μία ομάδα συνδεδεμένων συσκευών στο διαδίκτυο όπου όλες αυτές οι συσκευές ελέγχονται από έναν κακόβουλο παράγοντα. Όπως λέει και το όνομα της επίθεσης τα Botnet απαρτίζουν και το δίκτυο των συσκευών. Αρκετές φορές η έναρξη τέτοιων επιθέσεων ξεκινάει από εσωτερικό παράγοντα.



Εικόνα 1

- **Man in The Middle attacks:** Η συγκεκριμένη τεχνική κυβερνοεπίθεσης συγκαταλέγεται απο τις πρώτες. Η διαδικασία αυτής της επίθεσης πραγματοποιείται όταν κάποιος ο οποίος δεν έχει καμία εξουσιοδότηση παρεμβαίνει στην διαδικασία επικοινωνίας δύο αλλων ή και περισσότερων χρηστών που επικοινωνούν μεταξύ τους. Ο εισβολέας έχει την δυνατότητα να λειτουργεί ενεργητικά αλλοιώνοντας στοιχεία και περιεχόμενο της σύνδεσης ή και παθητικά πρακαλουθόντας και αντλώντας πληροφορίες της επικοινωνίας των άλλων χρηστών. Η εφαρμογή του 5G συνεπάγεται περισσότερα δίκτυα τοπικά ή και αστικά πράγμα το οποίο αυξανει τους πιθανούς κινδύνους της συγκεκριμένης επίθεσης.



Εικόνα 2

- **Location tracking and call interception:** Ο συγκεκριμένος τύπος παρακολούθησης τοποθεσίας και κλήσεων επιτυγχάνεται γνωρίζοντας πρωτοκολλα σελιδοποίησης μετάδοσης

5.9 Αρχές σχεδίασης για την ασφάλεια στο 5g

Οι ευρυζωνικές υπηρεσίες σε πραγματικό χρόνο, η συνδεσιμότητα των συσκευών IoT και η υψηλή κινητικότητα για τους χρήστες των συσκευών θα καταστούν δυνατές από το 5G με τρόπο εξαιρετικά αξιόπιστο και σε λογικές τιμές. Ένα νέο οικοσύστημα γνωστό ως 5G πιστεύεται ότι θα συνδέσει πρακτικά κάθε μέρος της κοινωνίας. Αυτό θα αποτελέσει σημαντική πρόκληση τόσο για τα υπάρχοντα όσο και για τα μελλοντικά δίκτυα, καθώς θα εισάγει ένα νέο σύνολο απειλών και τρωτών σημείων ασφαλείας που πρέπει να αντιμετωπιστούν. Για παράδειγμα, το 5G θα συνδέει βασικές υποδομές ενέργειας με το δίκτυο μέσω της σύνδεσης του δικτύου ηλεκτρικής ενέργειας, επομένως η ασφάλεια και οι παραβιάσεις σε αυτόν τον εξοπλισμό είναι ζωτικής σημασίας και δυνητικά καταστροφικές τόσο για τις υποδομές όσο και για την κοινωνία που εξυπηρετεί το 5G. Έτσι, ξεκινώντας από τα στάδια σχεδιασμού, θα πρέπει να λαμβάνεται υπόψη η ασφάλεια του 5G και των συστημάτων που συνδέονται μέσω αυτού (Ahmad et al., 2019).

Όπως αναφέρθηκε προηγουμένως, η έντονη χρήση των πόρων που βασίζονται στο νέφος, η εικονικοποίηση, ο διαχωρισμός του δικτύου και άλλες επερχόμενες τεχνολογίες του 5G θα έχουν ως αποτέλεσμα σημαντικά πλεονεκτήματα απόδοσης και ένα ευρύ φάσμα εφαρμογών. Ωστόσο, αυτές οι τροποποιήσεις εκθέτουν επίσης την αρχιτεκτονική ασφαλείας του σε πολυάριθμες νέες επιφάνειες επίθεσης και παρουσιάζουν πρόσθετους κινδύνους ασφαλείας. Αν και το 5G βασίζεται στις διαδικασίες ασφαλείας που χρησιμοποιήθηκαν από προηγούμενες τεχνολογίες κινητής τηλεφωνίας, το μοντέλο εμπιστοσύνης έχει επεκταθεί σημαντικά ως αποτέλεσμα της συμμετοχής περισσότερων μερών στη διαδικασία παροχής υπηρεσιών. Ο αριθμός των τελικών σημείων αυξάνεται δραματικά ως αποτέλεσμα του IoT και της αύξησης των χρηστών, με πολλές από αυτές τις εισροές κίνησης να μην παρακολουθούνται πλέον από ανθρώπους. Τα πρότυπα 3GPP για την ενισχυμένη ασφάλεια 5G περιλαμβάνουν μόνιμα αναγνωριστικά συνδρομητών (SUPI) για τη

διασφάλιση της ιδιωτικότητας του δικτύου, ενοποιημένη πιστοποίηση ταυτότητας για την αποσύνδεση της πιστοποίησης από τα σημεία πρόσβασης, κλιμακούμενα πρωτόκολλα πιστοποίησης για την υποστήριξη ασφαλών συναλλαγών και ευέλικτες πολιτικές ασφαλείας για την αντιμετώπιση περισσότερων περιπτώσεων χρήσης (Ahmad et al., 2019).

Οι φορείς εκμετάλλευσης θα πρέπει να παρακολουθούν και να αξιολογούν τακτικά τις επιδόσεις ασφαλείας καθώς η ανάπτυξη του 5G προχωρά και οι κρίσιμοι κόμβοι επιδόσεων γίνονται πιο εικονικοί. Για τη συμμόρφωση με τις βέλτιστες πρακτικές απαιτείται παρακολούθηση της ασφάλειας δικτύου από άκρο σε άκρο που καλύπτει την αρχιτεκτονική του συστήματος, τις συσκευές και τις εφαρμογές. Οι εκθετικές βελτιώσεις ταχύτητας στις οποίες έχουν συνηθίσει οι πελάτες με κάθε νέα γενιά δικτύων κινητής τηλεφωνίας θα παρασχεθούν αναμφίβολα από το 5G, αλλά η ταχύτητα είναι μόνο ένα συστατικό στοιχείο. Πολλοί έχουν χαρακτηρίσει το 5G ως την επόμενη βιομηχανική επανάσταση λόγω των προβλεπόμενων βελτιώσεων σε βιομηχανίες, όπως η γεωργία, η μεταποίηση και οι προσωπικές μεταφορές. Η πολυλειτουργική αρχιτεκτονική του, η οποία συνδυάζει MEC, massive MIMO NFV και μια αρχιτεκτονική πυρήνα βασισμένη σε υπηρεσίες προσανατολισμένες στο νέφος για την παροχή ενός νέου κύματος υπηρεσιών, βρίσκεται στο επίκεντρο αυτής της επανάστασης (Ahmad et al., 2019).

Λόγω των νέων συσκευών, υπηρεσιών και αναγκών που επέφεραν, συμπεριλαμβανομένης της ανάγκης για χαμηλή καθυστέρηση και κάλυψη υπηρεσιών σε πραγματικό χρόνο, κατέστησαν αναγκαίες νέες αρχές σχεδιασμού για το 5G. Η υψηλή ανθεκτικότητα και τα ανθεκτικά συστήματα είναι απαραίτητα, σύμφωνα με τα κριτήρια σχεδιασμού 5G του NGMN, τα οποία παρατίθενται στον παρακάτω πίνακα. Η ακύρωση παρεμβολών και η υιοθέτηση δυναμικών ραδιοπρωτοκόλλων είναι ζωτικής σημασίας για το ραδιόφωνο, μια φθηνή και πυκνή ανάπτυξη. Οι απαιτήσεις του δικτύου ποικίλλουν και επικεντρώνονται κυρίως στην ενσωμάτωση νέας τεχνολογίας. Αξιοποιώντας τις τεχνολογίες NFV και SDN, οι λειτουργίες του δικτύου θα τοποθετούνται δυναμικά. Ο στόχος είναι να μειωθεί η χρήση ξεπερασμένων δικτύων και να εφαρμοστούν νέες διεπαφές μεταξύ των τεχνολογιών ραδιοπρόσβασης (RAT) και του πυρήνα (Ahmad et al., 2019). Επιπλέον, ο σχεδιασμός του δικτύου θα πρέπει να διευκολύνει την υιοθέτηση διαδικασιών και χαρακτηριστικών ασφαλείας, ανάλογα με τις ανάγκες. Το SDN και η δυνατότητα που προσφέρει να διαχωρίζει το επίπεδο ελέγχου από το επίπεδο προώθησης δεδομένων

θα απαιτηθεί για την απλούστευση της λειτουργίας και της διαχείρισης. Το επίπεδο ελέγχου διαχειρίζεται τους πόρους του δικτύου, ενώ παράλληλα παρακολουθεί ολόκληρο το δίκτυο χρησιμοποιώντας συνδεδεμένες εφαρμογές. Η αξιοποίηση αυτών των συνδεδεμένων εφαρμογών στο δίκτυο, μαζί με την κεντρική διαχείριση του δικτύου, εγείρει ορισμένες σοβαρές ανησυχίες για την ασφάλεια. Εκτός από το SDN, θα αναπτυχθούν και άλλες τεχνολογίες 5G, όπως το NFV και το network slicing, που εγείρουν ανησυχίες για την ασφάλεια. Αυτό είναι πολύ σημαντικό και θα πρέπει να ληφθεί υπόψη στις αρχές σχεδιασμού των συστημάτων.

Λαμβάνοντας υπόψη τις πρωταρχικές τεχνολογίες ενεργοποίησης του 5G, τις κεραίες MIMO, το SDN, το NFV και τις έννοιες υπολογιστικού νέφους όπως το Multi-access Edge Computing (MEC), οι ανησυχίες για την ασφάλεια στο 5G μπορούν να περιγραφούν με ακρίβεια (Ahmad et al., 2019).

5.9.1 Massive MIMO

Θα ξεκινήσουμε συζητώντας τις τεράστιες προκλήσεις ασφάλειας MIMO. Μία από τις βασικές τεχνολογίες για το 5G είναι το massive MIMO. Ο σταθμός βάσης του αποτελείται από πολλές κεραίες, ώστε να μπορούν να υποστηριχθούν πολλοί τελικοί χρήστες χρησιμοποιώντας την ίδια ζώνη συχνοτήτων. Η χρήση μεγάλου αριθμού κεραιών έχει πολλά οφέλη, όπως η επέκταση της κάλυψης, η βελτίωση της ενεργειακής απόδοσης και η χρήση τους για διάφορους άλλους σκοπούς. Η μαζική MIMO έχει αδυναμίες ασφαλείας που επιτρέπουν τόσο παθητική όσο και ενεργητική υποκλοπή. Ο στόχος της παθητικής υποκλοπής είναι να σταματήσει η μετάδοση των σημάτων. Κανένα σήμα δεν αποστέλλεται από τον παθητικό εισβολέα από μόνος του. Η ενεργητική υποκλοπή περιλαμβάνει την αποστολή σημάτων στον χρήστη-στόχο για να παρεμποδίσει την ικανότητά του να μεταδίδει. Μια ενεργητική επίθεση αναφέρεται ως επίθεση παρεμβολής εάν ο μοναδικός στόχος της είναι να παρεμποδίσει τη νόμιμη μετάδοση. Η αλλοίωση πιλότου (pilot spoofing), μια άλλη διαδεδομένη τεχνική, περιλαμβάνει τον επιτιθέμενο που προσποιείται ότι είναι ο εξουσιοδοτημένος χρήστης. Ο σταθμός βάσης αποκτά πληροφορίες για την κατάσταση του καναλιού μέσω της διαδικασίας εκτίμησης του καναλιού με βάση τα σήματα πιλότου που αποστέλλονται από τους

εξουσιοδοτημένους χρήστες, τα οποία στη συνέχεια χρησιμοποιούνται για την προκωδικοποίηση της μετάδοσης (Ahmad et al., 2020).

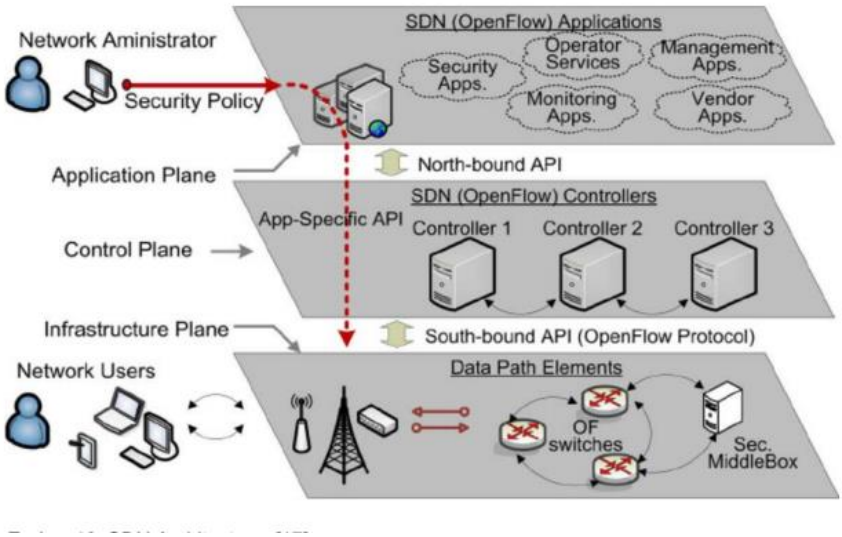
Ο επιτιθέμενος επιδιώκει να παραπλανήσει το σταθμό βάσης κατά τη διάρκεια μιας επίθεσης εναντίον του, παρέχοντας το πανομοιότυπο πιλοτικό σήμα. Ως αποτέλεσμα, ο σταθμός βάσης μπερδεύεται και σχεδιάζει λανθασμένα την προκωδικοποίηση της εκπομπής, γεγονός που βοηθά τον επιτιθέμενο και διαστρεβλώνει το κανάλι μεταξύ του σταθμού βάσης και του εξουσιοδοτημένου χρήστη. Οι επιθέσεις παρεμβολής είναι πιο δύσκολο να αντιμετωπιστούν από τις επιθέσεις παραποίησης για έναν τεράστιο δέκτη MIMO. Αντί για τη διεξαγωγή μιας επίθεσης παραποίησης, ο επιτιθέμενος επιδιώκει να παράγει τις περισσότερες παρεμβολές. Το γεγονός ότι πολλές κεραίες στα συστήματα μαζικής MIMO είναι αφιερωμένες σε έναν μόνο χρήστη τα καθιστά γενικά απρόσβλητα από τις επιθέσεις παθητικής υποκλοπής. Ωστόσο, ο επιτιθέμενος μπορεί ακόμα να εκμεταλλευτεί την εγγύτητα των χρηστών, την υψηλή συσχέτιση καναλιών ή τις αδυναμίες της εκτίμησης καναλιών ως άμυνα. Ένας από τους απλούστερους στόχους για επιθέσεις ασφαλείας ήταν το βήμα εκτίμησης καναλιού στο MIMO. Επιθέσεις παρεμβολής μπορούν επίσης να εξαπολυθούν χρησιμοποιώντας ανακριβείς πληροφορίες για την κατάσταση του καναλιού. Ακολουθεί ένας κατάλογος με ορισμένες από τις μεγάλες συστάσεις ασφαλείας MIMO. Το σύστημα πρέπει να προστατεύεται από τις ουσιαστικές ανησυχίες ασφάλειας που εμφανίζονται για να μπορέσει το MIMO να προσφέρει τα πλήρη οφέλη του. Μια μέθοδος ανίχνευσης είναι η αποστολή τυχαίων πιλοτικών σημάτων ώστε να είναι δυνατή η ανίχνευση ενεργών υποκλοπών. Σε αυτήν, ο σταθμός βάσης μπορεί να αναγνωρίσει τον εισβολέα από τον νόμιμο χρήστη που μεταδίδει μια σειρά τυχαίων συμβόλων (Ahmad et al., 2020).

Το μειονέκτημα αυτής της μεθόδου είναι ότι απαιτεί επιπλέον επιβάρυνση για τη μετάδοση πρόσθετων τυχαίων ακολουθιών. Μια άλλη τεχνική για τον εντοπισμό της ενεργής υποκλοπής είναι η κατασκευή του διαμορφωτή δέσμης έτσι ώστε το δείγμα που λαμβάνει από τον αυθεντικό χρήστη να ισούται με μια προκαθορισμένη τιμή. Ο νόμιμος χρήστης θα το ανιχνεύσει αυτό, καθώς θα δει μια μειωμένη τιμή όταν υπάρχει παρείσακτος. Η ενεργή υποκλοπή μπορεί να ανιχνευθεί από σταθμούς βάσης που συνεργάζονται μεταξύ τους. Σε αυτές τις περιπτώσεις, διάφοροι σταθμοί βάσης μπορούν να επικοινωνούν πληροφορίες, παρέχοντας την ευκαιρία να καθορίσουν αμοιβαία το βαθμό της νόμιμης μόλυνσης που προκαλείται από τους πιλότους. Για τον εντοπισμό ενεργών επιθέσεων υποκλοπής, μπορούν επίσης να χρησιμοποιηθούν

τεχνικές μηχανικής μάθησης ("Machine Learning", ML). Η μαζική MIMO επιτρέπει στο σταθμό βάσης να παρέχει υπηρεσίες σε πολλούς χρήστες ταυτόχρονα. Ακόμη και με την ανάπτυξη ισχυρών συστοιχιών κεραιών για την παρακολούθηση πληροφοριών, μια επίθεση είναι ακόμη δυνατή. Προτείνεται η προσέγγιση του στρώματος ασφαλείας του συστήματος ασφαλούς μετάδοσης με εναλλασσόμενο σύμβολο αρχικής φάσης ως άμυνα κατά αυτού του σεναρίου. Η θεμελιώδης ιδέα πίσω από αυτό είναι η τυχαία περιστροφή της φάσης του αρχικού σήματος, προκειμένου να μπερδευτεί ο εισβολέας, ενώ επιτρέπει στους εξουσιοδοτημένους χρήστες να αναγνωρίσουν σωστά την περιστροφή της φάσης και να εκτελέσουν τις απαραίτητες κατάλληλες αντίστροφες λειτουργίες, προκειμένου να ανακτήσουν την αρχική μετάδοση. Για την καταπολέμηση των προσπαθειών παρεμβολής σε τεράστιο uplink MIMO, προτείνεται ένας δέκτης ανθεκτικός στις παρεμβολές (Ahmad et al., 2020).

5.9.2 SDN

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, το SDN συγκεντρώνει τον έλεγχο του δικτύου σε πλατφόρμες λογισμικού ελέγχου του δικτύου και διαχωρίζει το επίπεδο προώθησης από το επίπεδο ελέγχου του δικτύου. Οι εφαρμογές χρησιμοποιούνται στο καθορισμένο από λογισμικό δίκτυο για την επικοινωνία με τις συσκευές προώθησης και τον έλεγχο των λειτουργιών. Με τον τρόπο αυτό επιτυγχάνεται απλότητα στον έλεγχο, τη διαχείριση και τη λειτουργία του δικτύου και επιταχύνεται η καινοτομία στην υλοποίηση των λειτουργιών του δικτύου. Η αρχιτεκτονική SDN αποτελείται από τρία λειτουργικά επίπεδα με διασυνδέσεις μεταξύ τους (Ahmad et al., 2020). Ο σχεδιασμός τριών επιπέδων του OpenFlow, μιας υλοποίησης SDN, περιλαμβάνει μεταγωγείς OpenFlow, ελεγκτές και εφαρμογές. Το παρακάτω διάγραμμα απεικονίζει την αρχιτεκτονική SDN.



Εικόνα 3: Αρχιτεκτονική SDN. Πηγή: Google Scholar

Τα ζητήματα ασφάλειας με το SDN καλύπτονται παρακάτω. Οι εφαρμογές που εγκαθίστανται στο επίπεδο εφαρμογών μπορούν να υλοποιήσουν λειτουργίες δικτύου. Οι εφαρμογές που χρησιμοποιούν SDN μπορούν να διαχειρίζονται το δίκτυο σύμφωνα με τις ανάγκες τους. Ωστόσο, το SDN έχει ορισμένα ζητήματα ασφάλειας, τα περισσότερα από τα οποία έχουν επισημανθεί σε σχέση με το OpenFlow. Για παράδειγμα, η κεντρική διαχείριση του δικτύου καθιστά την πλατφόρμα ελέγχου έναν καλό στόχο για επιθέσεις DoS. Επιπλέον, όταν κρίσιμες εφαρμογές παραβιάζονται από κακόβουλο λογισμικό, το δίκτυο μπορεί να αντιμετωπίσει κινδύνους ασφαλείας. Αφού εξετάσουμε κάθε ζήτημα ασφάλειας SDN, θα παρέχουμε επίσης τις διορθώσεις ασφαλείας που έχουν προταθεί. Η ασφάλεια του SDN είναι ένα πολύπλευρο ζήτημα που καλύπτει τόσο την ασφάλεια του SDN λόγω των εγγενών ευπαθειών του σε απειλές ασφαλείας όσο και το πώς το SDN, με τον κεντρικό έλεγχο του δικτύου και την ενισχυμένη ορατότητα και τον έλεγχο των ροών κυκλοφορίας, μπορεί να αξιοποιηθεί για τη βελτίωση της ασφάλειας του δικτύου. Θα δώσουμε ιδιαίτερη προσοχή στα μέτρα ασφαλείας που έχουν προταθεί ως τρόπος για να γίνει το SDN και κάθε επίπεδο που το απαρτίζει πιο ασφαλές (Ahmad et al., 2020).

5.9.3 Προκλήσεις SDN

Το SDN καινοτομεί στα δίκτυα επικοινωνίας, αλλά εισάγει επίσης αρκετά κενά ασφαλείας. Τα δύο κύρια χαρακτηριστικά του SDN είναι η διαχείριση του δικτύου με βάση το λογισμικό και ένα συγκεντρωτικό έξυπνο δίκτυο. Η πλειονότητα των λειτουργιών του δικτύου στο SDN υλοποιείται ως εφαρμογές, πράγμα που σημαίνει ότι εάν επιτραπεί η πρόσβαση σε μια κακόβουλη εφαρμογή, έχει τη δυνατότητα να βλάψει σοβαρά το δίκτυο. Τα ανοικτά API, ο ακατάλληλος έλεγχος ταυτότητας, η έλλειψη μηχανισμών εμπιστοσύνης και οι στρατηγικές εξουσιοδότησης εφαρμογών μπορούν να συμβάλουν σε ζητήματα ασφάλειας που επιφέρουν οι εφαρμογές. Όπως αναγνωρίζεται, πριν επιτραπεί στις εφαρμογές SDN να λειτουργούν το δίκτυο, θα πρέπει να προσδιοριστούν λύσεις για τα προαναφερθέντα ζητήματα ασφάλειας (Dangi et al., 2022). Μέτρα ασφαλείας για το επίπεδο εφαρμογών SDN: Στο SDN δεν θα πρέπει να επιτρέπεται η πρόσβαση σε κακόβουλο λογισμικό, στο δίκτυο ή στο επίπεδο ελέγχου του δικτύου. Υπάρχουν διάφορες συστάσεις σχετικά με τον τρόπο διεξοδικής εξέτασης των εφαρμογών SDN πριν τους επιτραπεί η πρόσβαση στις διαμορφώσεις του επιπέδου ελέγχου του δικτύου. Οι εφαρμογές μπορούν να λειτουργούν μόνο εντός των ορίων των δηλωμένων προνομίων του PermOF χάρη στην αυστηρή δομή εξουσιοδότησης. Το PermOF είναι φτιαγμένο για να δίνει σε ένα άλλο πρόγραμμα έλεγχο δικαιωμάτων ανάγνωσης, εγγραφής, ειδοποίησης και ελέγχου δικαιωμάτων με βάση το σύστημα προνομίων. Ως αποτέλεσμα, υπερασπίζεται τις πλατφόρμες ελέγχου από κακόβουλο λογισμικό. Άλλα μοντέλα αδειοδότησης εφαρμογών SDN υπάρχουν για να εγγυηθούν ότι μόνο αξιόπιστες εφαρμογές έχουν πρόσβαση στις δυνατότητες του επιπέδου ελέγχου. Παρόμοια με αυτό, το FortNOX είναι ένας πυρήνας επιβολής ασφάλειας που υλοποιεί δικαιώματα βάσει ρόλων για κάθε εφαρμογή OpenFlow και προτείνεται ως άμυνα κατά των απατεώνων εφαρμογών. Ο ελεγκτής Rose-Mary προτείνει ένα τελικό σχήμα αδειών που, στην ουσία, διασφαλίζει ότι η λειτουργία του ελεγκτή είναι θωρακισμένη από επιβλαβή προγράμματα (Dangi et al., 2022). Ζητήματα ασφάλειας με τους ελεγκτές SDN: Λόγω της κεντρικής λειτουργίας λήψης αποφάσεων, το επίπεδο ελέγχου του SDN (όπως ο ελεγκτής OpenFlow) αποτελεί πρωταρχικό στόχο για πειρατεία δικτύου ή άλλες κακόβουλες δραστηριότητες. Οι επιθέσεις DoS και οι κατανεμημένες επιθέσεις DoS αποτελούν τους κύριους κινδύνους. Ωστόσο, η χρήση του κεντρικού επιπέδου ελέγχου του OpenFlow έχει ακόμη περισσότερα προβλήματα ασφάλειας. Οι εφαρμογές ελέγχου, η ορατότητα του ελεγκτή και η επεκτασιμότητα του ελεγκτή, για

παράδειγμα, μπορούν όλα να χρησιμοποιηθούν ακούσια για να επηρεάσουν την ασφάλεια του δικτύου συνολικά (Dangi et al., 2022).

Λύσεις ασφαλείας για το επίπεδο ελέγχου (control plane) του SDN: Το επίπεδο ελέγχου διαδραματίζει κρίσιμη λειτουργία, επομένως υπάρχουν διάφορες ιδέες και στρατηγικές για τη βελτίωση της ασφάλειάς του. Η ασφάλεια του αρχικού ελεγκτή προβολέων αυξάνεται από τον ενισχυμένο ελεγκτή προβολέων. Συμπεριλαμβάνοντας ένα ασφαλές προγραμματιζόμενο API βόρειας κατεύθυνσης στον ελεγκτή SDN, ο ελεγκτής SE-Floodlight προσθέτει μηχανισμούς διαχωρισμού προνομίων στο επίπεδο ελέγχου SDN, προκειμένου να το καταστήσει πιο ασφαλές. Επιβεβαιώνοντας τους κανόνες ροής που δημιουργούνται από την εφαρμογή, χρησιμεύει ως γέφυρα μεταξύ των επιπέδων εφαρμογής και δεδομένων. Για την ασφάλεια του ελεγκτή SDN από κακόβουλες εφαρμογές, ο ελεγκτής ROSEMARY είναι ένα ισχυρό λειτουργικό σύστημα δικτύου. Το AVANT-GUARD έχει την ικανότητα να καθορίζει όρια στις αιτήσεις ροής στο επίπεδο ελέγχου, προκειμένου να αμυνθεί έναντι των επιθέσεων Dos αλλά και των προβλημάτων κλιμάκωσης του ελεγκτή. Υπάρχουν διάφορες μέθοδοι για την ενίσχυση της ασφάλειας του επιπέδου ελέγχου έναντι των επιθέσεων DoS και Distributed DoS (DDoS), συμπεριλαμβανομένων των αυτοοργανωμένων χαρτών. Το κατανεμημένο επίπεδο ελέγχου, η τοποθέτηση του ελεγκτή, ο πλεονασμός του ελεγκτή και ο αντιδραστικός σε αντίθεση με τον προληπτικό έλεγχο των κανόνων ροής και των ενημερώσεων είναι άλλες στρατηγικές για την ενίσχυση της αντίστασης του ελεγκτή σε προβλήματα ασφάλειας (Dangi et al., 2022).

5.9.4 NFV

Μεταφέροντας τις λειτουργίες δικτύου σε εφαρμογές λογισμικού, το NFV, το οποίο βασίζεται στην ιδέα της εικονικοποίησης, διαχωρίζει τις λειτουργίες δικτύου από το υποκείμενο ιδιόκτητο υλικό. Χωρίς τη χρήση λειτουργικού υλικού, είναι σε θέση να παρέχει λειτουργίες δικτύου βάσει ζήτησης σε οποιαδήποτε περιοχή του δικτύου. Η ασφάλεια των δεδομένων των χρηστών, των υπηρεσιών και του ίδιου του δικτύου έχουν αντιμετωπίσει ζητήματα ασφάλειας ως αποτέλεσμα της χρήσης του. Τα ζητήματα ασφάλειας με το NFV καλύπτονται εδώ. Η ικανότητα μετακίνησης λειτουργιών ή υπηρεσιών από μια τοποθεσία σε μια άλλη ή από έναν πόρο σε έναν

άλλο θα παρουσιάσει μια σειρά από προκλήσεις ασφάλειας με την εισαγωγή του NFV. Η χειροκίνητη διαμόρφωση των εικονικών συστημάτων ή των VNF, η οποία μπορεί να οδηγήσει σε δυναμικές παραβιάσεις της ασφάλειας λόγω της αυξημένης πολυπλοκότητας με την ανάπτυξη του συστήματος, αποτελεί ανησυχία καθώς αυξάνεται ο αριθμός των υπηρεσιών ή των εικονικών λειτουργιών (Dangi et al., 2022).

Επιπλέον, η αύξηση των VNF δημιουργεί σοβαρές ανησυχίες σχετικά με την κλοπή της κυκλοφορίας, την κλοπή υπηρεσιών και την παράνομη πρόσβαση σε δεδομένα. Επιπλέον, τα εικονικά συστήματα ή τα συστήματα NFV έχουν εγγενή ζητήματα ασφάλειας. Θα συζητήσουμε τις προτεινόμενες διορθωτικές λύσεις ασφάλειας για κάθε ζήτημα ασφάλειας, αφού αναλύσουμε τα ίδια τα ζητήματα ασφάλειας. Το network slicing, μια τεχνική εικονικοποίησης, μπορεί να βελτιώσει σημαντικά την ασφάλεια των χρηστών. Με βάση τις προτεραιότητες ασφαλείας της υπηρεσίας και του δικτύου, το network slicing χρησιμοποιείται για τον διαχωρισμό της κίνησης διαφόρων υπηρεσιών ή τμημάτων δικτύου. Τα κατανεμημένα VNF μπορούν να χρησιμοποιηθούν για τη βελτίωση της διαθεσιμότητας, της κλίμακας και την άμυνα έναντι επιθέσεων DoS και DDoS. Ενισχύοντας τη νοημοσύνη αυτοάμυνας, οι VNF μπορούν να αυξήσουν την ασφάλεια στα δίκτυα 5G. Ένα από τα κύρια πλεονεκτήματα του 5G σε σχέση με τα παλαιότερα δίκτυα είναι ο τεμαχισμός του δικτύου (Dangi et al., 2022).

Προβλήματα με τα εικονικά συστήματα: Είναι αμφίβολο ότι τα εικονικά συστήματα που χρησιμοποιούν το ίδιο συστατικό του δικτύου θα απαιτούν το ίδιο επίπεδο προστασίας. Ως εκ τούτου, φαίνεται λογικό ότι τα ίδια μέτρα ασφαλείας δεν μπορούν να χρησιμοποιηθούν σε ολόκληρο το σύστημα. Ένας διακομιστής που εκτελεί μια εικονική μηχανή η οποία διαχωρίζεται σε διάφορες ζώνες, η καθεμία με διαφορετικό επίπεδο προστασίας, είναι ένα παράδειγμα αυτού. Κάθε ζώνη που έχει έναν συγκεκριμένο βαθμό ασφάλειας δεν μπορεί να μεταφερθεί σε άλλον φυσικό διακομιστή, επειδή αυτός ο διακομιστής μπορεί να έχει διαφορετικό επίπεδο ασφάλειας που δεν είναι συμβατό με το επίπεδο της ζώνης αυτής. Ωστόσο, οι πολλές αλυσιδωτές υπηρεσίες που προσφέρονται από το NFV θα καταστήσουν τον προσδιορισμό της υποκείμενης αιτίας των κινδύνων ασφαλείας ακόμη πιο δύσκολο (Harald, 2021).

Λύσεις ασφαλείας για εικονικά συστήματα: Τα εικονικά συστήματα έχουν πολλά πλεονεκτήματα ασφάλειας, παρά το γεγονός ότι η διαχείρισή τους είναι

δύσκολη. Για παράδειγμα, ένα εικονικό σύστημα μπορεί εύκολα να μετατοπιστεί για να μειωθεί ο αντίκτυπος μιας επίθεσης. Προτείνεται ένας διαχειριστής πολιτικής για την επιβολή μιας πολιτικής ασφαλείας σε δυναμικά περιβάλλοντα VNF, προκειμένου να αντιμετωπιστούν οι δυσκολίες στη διασφάλιση της σταθερότητας των κανόνων ασφαλείας σε εικονικά δίκτυα. Οι χρήστες μπορούν να σχεδιάζουν και να επιβάλλουν τις δικές τους απαιτήσεις εντός του δικτύου χρησιμοποιώντας το στοιχείο λογισμικού NFV, αποφεύγοντας περίπλοκες διαδικασίες ασφαλείας (Harald, 2021).

5.9.5 Cloud

Μικρές και μεγάλες επιχειρήσεις μπορούν να έχουν πρόσβαση σε υπολογιστικούς πόρους και υπηρεσίες κατά παραγγελία χάρη στο υπολογιστικό νέφος, το οποίο βελτιστοποιεί τη χρήση των διαθέσιμων πόρων και επιτρέπει ένα υψηλότερο επίπεδο αφαίρεσης των υποκείμενων μηχανισμών από την πλευρά του πελάτη. Τα τεχνολογικά μεγαθήρια σήμερα έχουν αγκαλιάσει το νέφος, το χρησιμοποιούν και αναπτύσσονται χάρη στις δυνατότητές του. Μία από τις βασικές εφαρμογές του υπολογιστικού νέφους στο 5G είναι η μαζική επικοινωνία τύπου μηχανής. Ένας τεράστιος αριθμός διασυνδεδεμένων μηχανών που δημιουργούν ένα δίκτυο αισθητήρων και ενεργοποιητών χρησιμοποιείται στις μαζικές επικοινωνίες τύπου μηχανής για την υποστήριξη ενός τεράστιου αριθμού φθηνών και χαμηλής ισχύος συσκευών. Εδώ, φαίνεται ότι υπάρχει ανάγκη για υπολογιστικό νέφος που επιτρέπει την ανταλλαγή δεδομένων σε πραγματικό χρόνο μεταξύ των συσκευών, καθώς και για υπολογιστικό νέφος που παρέχει σε συσκευές χαμηλής αποθηκευτικής ικανότητας πρόσβαση σε εικονικό αποθηκευτικό χώρο στο νέφος (Harald, 2021).

Μια άλλη σημαντική εφαρμογή του υπολογιστικού νέφους είναι το MEC (Multi-Access Edge Computing), το οποίο είναι ζωτικής σημασίας για τα μελλοντικά δίκτυα κινητής τηλεφωνίας όπως το 5G. Το MEC επιτρέπει την επέκταση του νέφους και των υπολογιστικών δυνατοτήτων εντός του RAN στην άκρη των κινητών δικτύων. Ως αποτέλεσμα, οι πάροχοι περιεχομένου μπορούν να έχουν άμεση πρόσβαση σε ραδιοδεδομένα με ελάχιστη καθυστέρηση και μεγάλο εύρος ζώνης. Ωστόσο, όλες αυτές οι τεχνολογίες ενέχουν σημαντικούς κινδύνους για την ασφάλεια. Η τεχνολογία που χρησιμοποιείται στο υπολογιστικό νέφος, όπως η εικονικοποίηση, η δικτύωση και οι υπηρεσίες που χρησιμοποιούνται σε αυτό, ευθύνονται σε μεγάλο βαθμό για τις

ανησυχίες ασφαλείας του. Είναι σαφές ότι τα τυπικά μέτρα ασφαλείας δεν είναι σε θέση να διασφαλίσουν το νέφος λόγω των εικονικών, ευρέως διασκορπισμένων πόρων και της ποικιλίας των υπηρεσιών του. Επειδή το υπολογιστικό νέφος χρησιμοποιεί μια σειρά από τεχνολογίες, παρουσιάζει επίσης μια σειρά από προβλήματα ασφαλείας που απαιτούν εξειδικευμένες λύσεις. Υπάρχουν πολυάριθμοι τρόποι για την αντιμετώπιση των απειλών ασφαλείας του υπολογιστικού νέφους. Για παράδειγμα, η ασφάλεια της εικονικοποίησης και των εικονικών λειτουργιών δικτύου (VNF) που βασίζονται στο νέφος επηρεάζει άμεσα την ασφάλεια του νέφους (Harald, 2021).

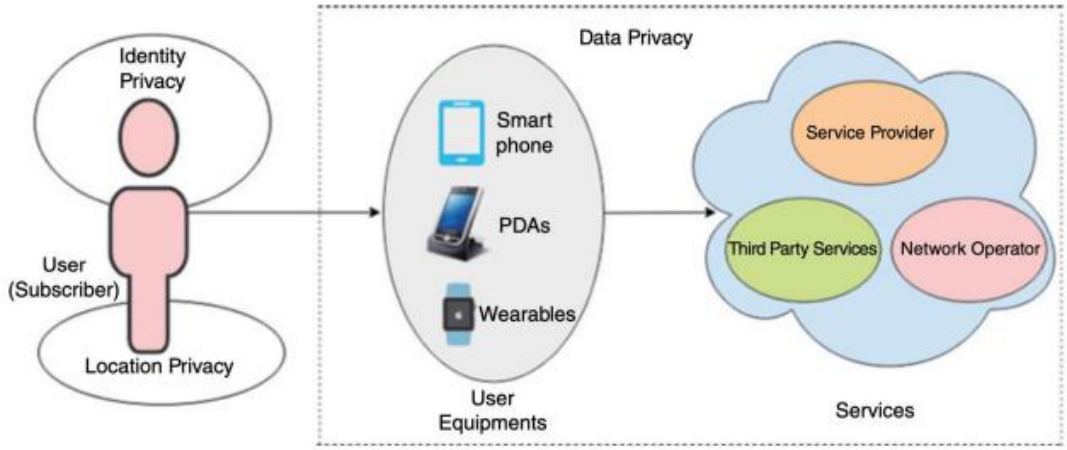
5.9.6 Απειλές και λύσεις ασφάλειας από Insiders & ιδιωτικότητα δεδομένων

Επιθέσεις εκ των έσω (Insider attacks): Οι επιθέσεις εκ των έσω αποτελούν σοβαρή απειλή για ολόκληρο το νέφος, επειδή περιλαμβάνουν ουσιαστικά επιθέσεις που ξεκινούν από τους εργαζόμενους του παρόχου υπηρεσιών. Αυτοί οι εργαζόμενοι έχουν πρόσβαση στους πραγματικούς διακομιστές που φιλοξενούν τα δεδομένα των χρηστών. Όπως είναι σαφές, η ακατάλληλη χρήση και διαχείριση αυτών των δεδομένων από αυτή την ομάδα ανθρώπων που υποτίθεται ότι είναι έμπιστοι, αποτελεί σοβαρή απειλή για το σύννεφο στο σύνολό του (Harald, 2021).

Λύσεις ασφαλείας για την επίθεση εκ των έσω (Insider attack): Από κοινωνική και τεχνική άποψη, η αντιμετώπιση των ευπαθειών από επιθέσεις εκ των έσω στα δίκτυα 5G που βασίζονται στο νέφος είναι δύσκολη. Παρόλο που το CPS εργάζεται για να παρέχει στους καταναλωτές ασφαλείς διεπαφές και API, η πιθανότητα τα δεδομένα στο νέφος να χρησιμοποιηθούν και να καταχραστούν από εξουσιοδοτημένο προσωπικό του παρόχου υπηρεσιών είναι μια σοβαρή ανησυχία. Η διαρροή δεδομένων και η απώλεια δεδομένων είναι δύο φυσικά περιστατικά που περιπλέκουν περαιτέρω το πρόβλημα. Μια τεχνική μετριασμού από αυτή την άποψη είναι η απαίτηση για πιο αξιόπιστα αντίγραφα ασφαλείας και πολλαπλές δυνατότητες δημιουργίας αντιγράφων ασφαλείας σε διάφορες τοποθεσίες και πλατφόρμες. Η εφαρμογή κατάλληλων ελέγχων ελέγχου και ελέγχων ιστορικού ρουτίνας, μαζί με ψηφιακές χρονικές σφραγίδες και υπογραφές στα δεδομένα cloud, θα μπορούσε να συμβάλει στη μείωση της πιθανότητας κακής χρήσης και κατάχρησης δεδομένων cloud από εξουσιοδοτημένους εσωτερικούς χρήστες για άλλες σκόπιμες επιθέσεις εκ των έσω (Nelson, 2021).

Ένα ευρύ φάσμα νέων χρήσεων και εφαρμογών θα καταστεί δυνατό με την τεχνολογία πέμπτης γενιάς (5G). Αυτό υποδηλώνει ότι ένας σημαντικός όγκος ιδιωτικών δεδομένων θα μεταδίδεται μέσω των δικτύων 5G. Τα δεδομένα διατρέχουν τεράστιο κίνδυνο ως αποτέλεσμα της ανάπτυξης εργαλείων εξόρυξης δεδομένων, τα οποία καθιστούν απλούστερη την εξαγωγή πληροφοριών για την προστασία Μια ποικιλία αξιόπιστων πληροφοριών θα πρέπει να προστατεύονται από μέτρα ασφαλείας στο δίκτυο 5G τόσο για τους ανθρώπινους όσο και για τους αυτοματοποιημένους χειριστές (Nelson, 2021).

Με την κατανόηση των ιδιοτήτων συγκεκριμένων υπηρεσιών, η τεχνολογία 5G θα παρέχει επίσης στους καταναλωτές εξατομικευμένες υπηρεσίες δικτύου. Ως αποτέλεσμα, διαφορετικές υπηρεσίες στο δίκτυο 5G ενδέχεται να έχουν διαφορετικές απαιτήσεις προστασίας της ιδιωτικής ζωής. Επίσης, η τεχνολογία 5G καθιστά δυνατή την εφαρμογή προτύπων απορρήτου προσανατολισμένων στις υπηρεσίες. Για παράδειγμα, ορισμένες εφαρμογές υγειονομικής περίθαλψης θα απαιτούν υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής για τις πληροφορίες υγείας των χρηστών. Επίσης, ένα υψηλότερο επίπεδο ανωνυμίας είναι απαραίτητο στην περίπτωση ορισμένων κρίσιμων βιομηχανικών διαδικασιών. Ωστόσο, ορισμένες εφαρμογές, όπως η αναζήτηση δεδομένων τοποθεσίας, μπορεί να χρειάζονται μόνο ένα ελάχιστο επίπεδο προστασίας της ιδιωτικής ζωής. Όπως υποδεικνύεται στην παρακάτω εικόνα, διαχωρίσαμε τις ιδέες της προστασίας της ιδιωτικής ζωής των χρηστών σε τρεις κατηγορίες για μια πιο εστιασμένη κατανόηση: την προστασία των δεδομένων, την προστασία της θέσης και την προστασία της ταυτότητας (Nelson, 2021).



Εικόνα 4

Εικόνα 5: Χρήστης και ασφάλεια δεδομένων. Πηγή: Google Scholar

Η πιθανότητα διαρροής προσωπικών δεδομένων είναι αρκετά υψηλή, επειδή υπάρχουν πολλές έξυπνες και διαφορετικές συσκευές που συνδέονται μέσω της τεχνολογίας 5G. Χωρίς τη συγκατάθεσή τους, οι πάροχοι υπηρεσιών διατηρούν και χρησιμοποιούν τα προσωπικά δεδομένα των πελατών τους. Σε ορισμένες περιπτώσεις, ο πάροχος υπηρεσιών αποθηκεύει τις πληροφορίες των χρηστών για τα δικά του αγαθά προτού τις μοιραστεί με άλλες επιχειρήσεις. Αυτό επιτρέπει στις τελευταίες να εξετάζουν τα δεδομένα και να εντοπίζουν τάσεις, όπως για παράδειγμα ποιο από τα προϊόντα τους είναι πιο κατάλληλο για έναν συγκεκριμένο χρήστη. Σε ορισμένες περιπτώσεις, είναι ακόμη και επωφελές για την επιχείρηση να συλλέγει ορισμένα από τα προσωπικά δεδομένα του χρήστη προκειμένου να αναπτύξει νέα αγαθά και υπηρεσίες (Nelson, 2021).

Ωστόσο, οι πάροχοι υπηρεσιών θα πρέπει να είναι πιο σαφείς σχετικά με το πώς και γιατί χρησιμοποιήθηκαν τα δεδομένα των χρηστών. Πρέπει επίσης να δίνουν απαντήσεις σε ζητήματα όπως το ποιες πληροφορίες ελήφθησαν, πώς αποθηκεύτηκαν και πού φυλάχθηκαν. Πριν από την εγκατάστασή τους, ορισμένες εφαρμογές για κινητά, όπως αυτές για Android, απαιτούν συγκεκριμένες πληροφορίες. Τις περισσότερες φορές, οι πληροφορίες για τις οποίες μια εφαρμογή ζητά άδεια έχουν ελάχιστη σχέση με τις υπηρεσίες που προσφέρει. Ενδέχεται να υπάρχουν και άλλες χρήσεις για τα δεδομένα αυτά εκτός από αυτές που έχουν γνωστοποιήσει οι δημιουργοί της εφαρμογής. Στις μέρες μας, οι σελίδες κοινωνικής δικτύωσης είναι οι πιο δημοφιλείς πλατφόρμες για την ανταλλαγή δημόσιων και ιδιωτικών πληροφοριών από τους χρήστες. Η πραγματοποίηση ζωντανών συνομιλιών κειμένου, φωνής και βίντεο, καθώς και η κοινή χρήση ή η μεταφόρτωση ιδιωτικών φωτογραφιών είναι δημοφιλείς τρόποι για να ενημερώσετε τους άλλους για τις παρούσες ενεργοποιήσεις σας. Αυτό το είδος της συνεχούς και απρόσκοπτης σύνδεσης αναμένεται να επιτρέψει το 5G. Οι μελλοντικές τεχνολογίες πρέπει να περιλαμβάνουν συστήματα IoT που βασίζονται στο 5G, προκειμένου να παρέχουν ένα ευρύ φάσμα ψηφιακών υπηρεσιών. Στο τέλος, αυτό θα παράγει συνεχώς τεράστιους όγκους δεδομένων. Τεράστιος όγκος δεδομένων θα χρησιμοποιηθεί όταν το IoT γίνει κοινός τόπος. Οι ταχύτητες μεταφοράς δεδομένων θα βελτιωθούν χάρη στο 5G, αυξάνοντας τον κίνδυνο εχθρικών επιθέσεων (Nelson, 2021).

Παρόμοια με αυτό, η φορητή τεχνολογία παράγει μεγάλο όγκο δεδομένων λόγω των αισθητήρων που παρακολουθούν και συλλέγουν συνεχώς δεδομένα του χρήστη, όπως η φυσική κατάσταση, ο καρδιακός ρυθμός, το βάρος, το ύψος κ.λπ. Χωρίς τη συγκατάθεση του χρήστη, τρίτοι είναι σε θέση να αναλύσουν αυτά τα δεδομένα και να εξάγουν πρόσθετα χαρακτηριστικά από αυτά. Όταν ένας τρίτος, πάροχος υπηρεσιών ή άλλος κακόβουλος εισβολέας επιχειρεί να αποκτήσει πρόσβαση στα προσωπικά δεδομένα ενός χρήστη χωρίς την άδεια του χρήστη, προκύπτουν κίνδυνοι για την ιδιωτικότητα των δεδομένων. Για παράδειγμα, κάποιος μπορεί απλώς να εκτιμήσει το καθημερινό μοτίβο του καταναλωτή παρακολουθώντας τη δραστηριότητά του όταν χρησιμοποιεί τα προσωπικά του δεδομένα. Σε ορισμένες περιπτώσεις, αυτό μπορεί να είναι επιζήμιο, επειδή είναι απλό να παρακολουθεί κανείς τις δραστηριότητες κάποιου. Ο κλάδος της υγειονομικής περίθαλψης, όπου πρόκειται για ευαίσθητα ιατρικά δεδομένα, μπορεί να χρησιμεύσει ως άλλο σημαντικό παράδειγμα. Ο ασθενής συχνά θέλει να περιορίσει την πρόσβαση σε επιλεγμένα άτομα, όπως γιατρούς, συγκεκριμένα μέλη της οικογένειας ή γνωστούς. Ωστόσο, οι πληροφορίες ενδέχεται να αποκτήσουν πρόσβαση από μη εξουσιοδοτημένους χρήστες ή κακόβουλους χρήστες που θα τις χρησιμοποιούσαν για αθέμιτους σκοπούς (Salah et al., 2021).

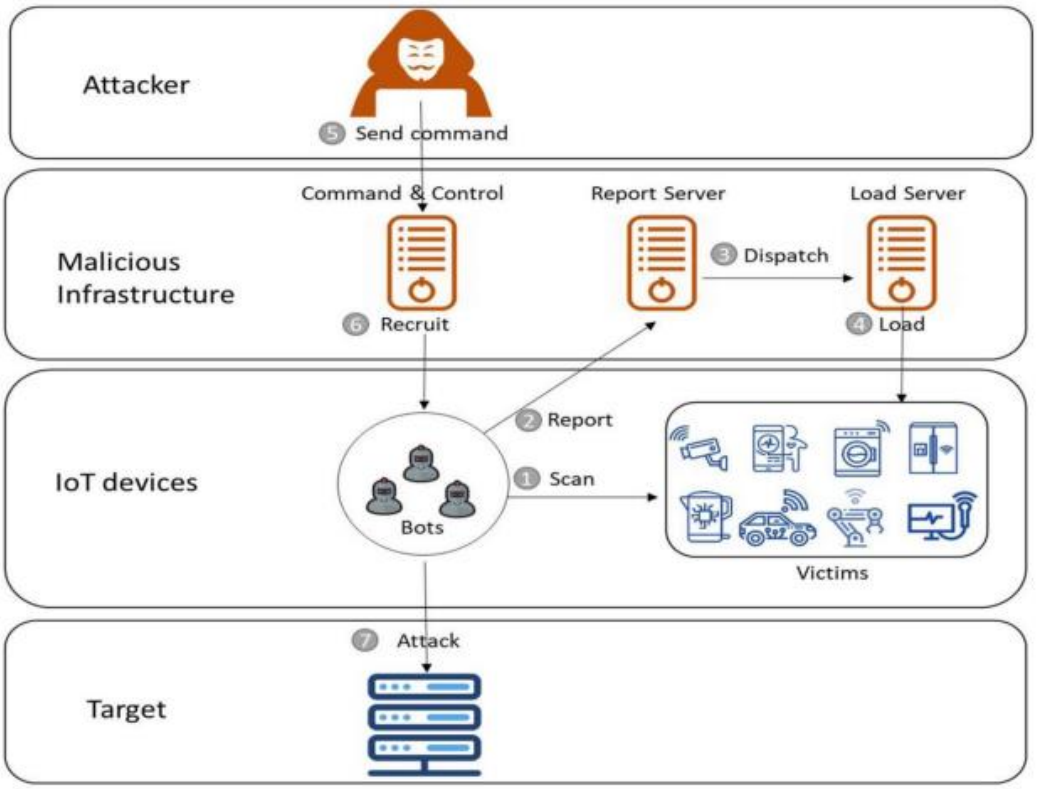
Πολλές φορές στα δίκτυα 5G, η χρήση της συγκεκριμένης τεχνικής πρόσβασης επηρεάζει τις ανάγκες προστασίας της ιδιωτικής ζωής. Διαφορετικά δίκτυα πρόσβασης 5G θα μοιράζονται δεδομένα χρηστών και διάφοροι προμηθευτές θα παρέχουν τα λειτουργικά δεδομένα του δικτύου. Τα διασκορπισμένα δεδομένα του χρήστη, τα οποία μπορεί να είναι προσβάσιμα σε οποιοδήποτε σημείο του δικτύου, μπορούν να αναλυθούν από τρίτους με τη χρήση αλγορίθμων εξόρυξης δεδομένων για την απόκτηση προσωπικών πληροφοριών. Για τα δίκτυα 5G, απαιτούνται αυστηρότερες λύσεις προστασίας της ιδιωτικής ζωής των δεδομένων λόγω της πιθανότητας τέτοιων συμβάντων. Κατά την επισημοποίηση και την ανάπτυξη πολιτικών τεχνολογίας 5G, είναι ζωτικής σημασίας η δημιουργία ισχυρών διαδικασιών προστασίας δεδομένων (Salah et al., 2021).

Επιπλέον, οι πάροχοι υπηρεσιών πρέπει να περιγράφουν τον τρόπο με τον οποίο συλλέγονται και εφαρμόζονται τα δεδομένα στις διάφορες υπηρεσίες. Το απόρρητο των χρηστών και τα δεδομένα που χρησιμοποιούνται από τους παρόχους υπηρεσιών θα πρέπει να είναι ισορροπημένα, ώστε οι επιχειρήσεις να μπορούν να αναπτύσσουν καινοτόμες και επωφελείς εφαρμογές για τον χρήστη, διασφαλίζοντας

παράλληλα ότι δεν διακυβεύεται το απόρρητο των χρηστών. Θα πρέπει να θεσπιστούν μηχανισμοί ελέγχου ώστε να διευκολύνεται η παρακολούθηση κάθε δραστηριότητας που λαμβάνουν διάφορες οντότητες. Οι πρακτικές συλλογής, διατήρησης και διαγραφής δεδομένων των παρόχων υπηρεσιών ή άλλων μερών θα πρέπει να εξετάζονται στο πλαίσιο των προσεγγίσεων ελαχιστοποίησης των δεδομένων (Salah et al., 2021).

5.9.7 Επιθέσεις DDoS σε 5g και προστασία

Οι επιτιθέμενοι ενδέχεται να χρησιμοποιήσουν τις δυσκολίες που δημιουργούν οι νέες τεχνολογίες IoT και 5G για κακόβουλους σκοπούς, καθώς θα συνδέσουν πολλές καθημερινές ανθρώπινες ρουτίνες με τα δίκτυα επικοινωνίας και θα επιταχύνουν την παγκοσμιοποίηση. Θα προκύψουν σημαντικές προκλήσεις στον τομέα της ασφάλειας. Από την πρώτη γενιά μέχρι σήμερα, τα δίκτυα κινητής τηλεφωνίας είχαν πάντα τα δικά τους προβλήματα. Τα προβλήματα θα είναι περισσότερα και πιο σύνθετα από εκείνα των προηγούμενων γενεών όταν πρόκειται για την τεχνολογία 5G, η οποία θα προσφέρει νέες υπηρεσίες και θα χρησιμεύσει ως η κύρια πλατφόρμα επικοινωνίας για το Διαδίκτυο των πραγμάτων. Πολλές συσκευές IoT περιέχουν ελαττώματα στο λειτουργικό σύστημα, το λογισμικό, το υλικό και την αρχιτεκτονική τους. Η ανάπτυξη επιθέσεων άρνησης παροχής υπηρεσιών (DoS) και κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS), οι οποίες λαμβάνουν χώρα όταν παραβιάζεται ο εξοπλισμός IoT, είναι μία από τις πιο συχνές παραβιάσεις του εξοπλισμού IoT. Οι επιθέσεις που προκαλούν άρνηση παροχής υπηρεσιών εμποδίζουν τους εξουσιοδοτημένους χρήστες να χρησιμοποιούν μια συγκεκριμένη υπηρεσία. Μια επίθεση DoS προέρχεται συχνά από μία μόνο πηγή, η οποία είναι ένας διακομιστής ή ένα σύστημα υπολογιστή, ενώ μια επίθεση DDoS χρησιμοποιεί πολλαπλά συστήματα και μπορεί να είναι ακόμη και παγκοσμίως κατανεμημένη και αποκεντρωμένη (Storck & Duarte, 2020).



Εικόνα 6: Δίκτυο IoT. Πηγή: Google Scholar

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: Αποφεύγουμε να χρησιμοποιούμε μακροσκελείς, πολύπλοκους κωδικούς πρόσβασης σε αυτή τη συσκευή λόγω των περιορισμών υλικού στη μνήμη RAM και ROM.

- Προσαρμοσμένα λειτουργικά συστήματα: Η διαμόρφωση και η λειτουργικότητα του λειτουργικού συστήματος είναι βάναυσα περιορισμένες ώστε να ανταποκρίνονται στις ανάγκες και τη χρήση αυτού του εξοπλισμού (Storck & Duarte, 2020).

-Ελλιπής υποστήριξη: Πολλά από αυτά τα κομμάτια εξοπλισμού δεν λαμβάνουν πλήρη υποστήριξη, συμπεριλαμβανομένης της κατασκευής, των απαραίτητων αναβαθμίσεων και της αντικατάστασης με νέο εξοπλισμό (Storck & Duarte, 2020).

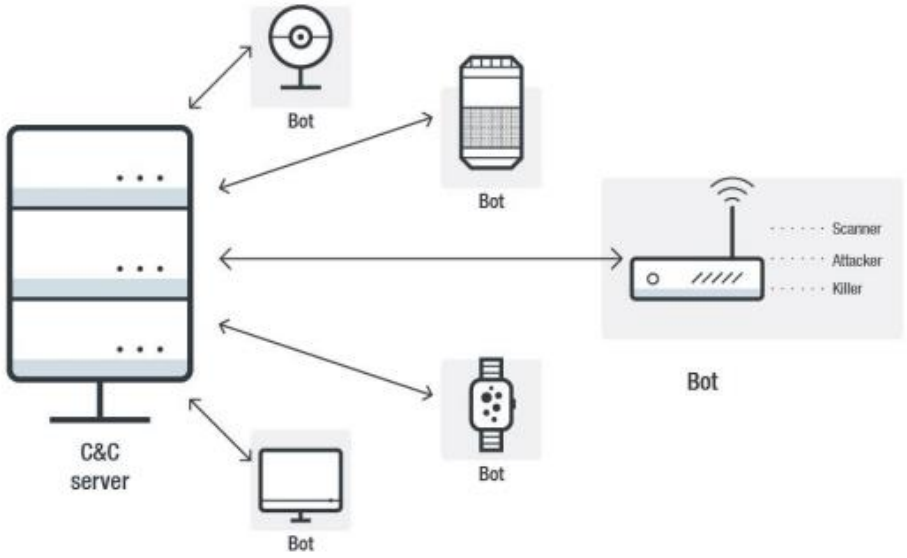
- Αδύναμη ή καθόλου κρυπτογράφηση: Χρησιμοποιούνται αδύναμες τεχνικές κρυπτογράφησης λόγω της αξιοποίησης φθηνού υλικού και σπάνιων πόρων.

Η έλλειψη κρυπτογράφησης στην αρχή της διαδικασίας αποκαλύπτει αρκετές φορές πληροφοφορίες της συσκευής σε μη εξουσιοδοτημένα άτομα οι οποίες πληροφορίες μπορούν να χρησιμοποιηθούν για στοχευμένες επιθέσεις IoT προκαλώντας σοβαρές ζημιές. Οι hackers μέσω της επεξεργασίας αυτών των πληροφοριών είναι σε θέση να γνωρίζουν ποιες ακριβώς συσκευές είναι συνδεδεμένες την εκάστοτε χρονική στιγμή στο δίκτυο. Επιπρόσθετες λεπτομέρειες σχετικά με τύπο του λειτουργικού συστήματος καθώς και τον τύπο της συσκευής είναι μεγάλο και σημαντικό πλεονέκτημα για τους hackers προκειμένου να σχεδιάσουν με όσο το δυνατόν μεγαλύτερη ακρίβεια την επίθεσή τους ώστε να αυξήσουν την ακρίβεια και την αποτελεσματικότητα της επιτυχίας της επίθεσής τους.

Η αφθονία των συσκευών IoT, η απομακρυσμένη προσβασιμότητα και η τεράστια γεωγραφική περιοχή συμβάλλουν στην αύξηση των μολύνσεων από συσκευές IoT. Οποιοδήποτε είδος συσκευής IoT μπορεί να αξιοποιηθεί εξ αποστάσεως και να μετατραπεί σε bot. Σε αυτές τις συσκευές του Διαδικτύου των Πραγμάτων (IoT) χρησιμοποιούνται συνήθως οι υπηρεσίες Telnet, SSH και Web. Αυτές οι υπηρεσίες διασφαλίζονται αποκλειστικά με όνομα χρήστη και κωδικό πρόσβασης, κάτι που έχει μειονεκτήματα και είναι εύκολα ευάλωτο σε παραβίαση. Επιπλέον, ένας μεγάλος αριθμός αυτών των συσκευών βρίσκεται στην περιφέρεια ενός τοπικού ιδιωτικού LAN. Σε περίπτωση εισβολής και ενώ ελέγχεται από χάκερς, το ιδιωτικό τοπικό δίκτυο είναι ουσιαστικά επίσης μολυσμένο και ευάλωτο (Storck & Duarte, 2020).

Επιπλέον, οι επιθέσεις DDoS μπορούν ευκολότερα να εκμεταλλευτούν την κινητικότητα του εξοπλισμού IoT. Ο επιτιθέμενος σε αυτό το σενάριο μπορεί να αλλάξει γρήγορα τη θέση του, καθυστερώντας την ανίχνευση και τον εντοπισμό της επίθεσης (εγκληματολογική έρευνα). Με βάση αυτό το χαρακτηριστικό, ένας επιτιθέμενος θα μπορούσε να αναπτύξει έναν αριθμό Command & Operate Servers με δυνατότητες κινητικότητας στη θέση ενός C&C (Command & Control Server) για τον έλεγχο του botnet. Επιπλέον, οι εν λόγω διακομιστές περιλαμβάνουν αρκετές κάρτες

διασύνδεσης δικτύου (NIC), οι οποίες επιτρέπουν στον επιτιθέμενο να δημιουργεί νέες συνδέσεις σε δίκτυα 4G και 5G. Ως αποτέλεσμα, ο επιτιθέμενος μπορεί να διαχειριστεί το δίκτυο botnet χρησιμοποιώντας ένα δίκτυο φορητών διακομιστών C&C με πολλές διευθύνσεις IP. Ως αποτέλεσμα, η φυσική τοποθεσία και η διεύθυνση προέλευσης του διακομιστή εντολών και ελέγχου θα αλλάζουν. Η παρακάτω εικόνα δείχνει πώς ένας χάκερ απέκτησε πρόσβαση στο δίκτυο IoT και απέκτησε πολλά bots. Στη συνέχεια, το θύμα θα δεχθεί επίθεση και η υπηρεσία θα τερματιστεί, ως απάντηση σε εικονικά αιτήματα, όπως η κίνηση HTTP, το TCP SYN, τα ερωτήματα DNS, τα αιτήματα ICMP και τα αιτήματα SIP (Session Initiation Protocol), μεταξύ άλλων. Αυτά τα bots μπορούν να αγοραστούν για πολύ λίγα χρήματα στην αγορά του σκοτεινού ιστού για ποικίλες χρήσεις (Zhang et al., 2020).



Εικόνα 7: Επίθεση από hacker. Πηγή: Google Scholar

Σε αυτή την περίπτωση, ο επιτιθέμενος έχει μια άλλη επιλογή για τον έλεγχο των διακομιστών C&C: ένα απομακρυσμένο πρόγραμμα. Στη συνέχεια, μπορεί να ρυθμίσει κάθε διακομιστή C&C να δίνει εντολές στο botnet του με αυτόν τον τρόπο. Εάν ο επιτιθέμενος αποκρύψει τις διευθύνσεις IP των διακομιστών εντολών και ελέγχου του και κρύψει τους διακομιστές του πίσω από ένα δίκτυο TOR (The Onion Router), τότε αυτή η τεχνική μπορεί να είναι αρκετά επικίνδυνη (Zhang et al., 2020). Όσον αφορά τα μέτρα ασφαλείας, το 5G διαθέτει κάποιες άμυνες για την προστασία του συστήματός του. Παρουσιάζει την ιδέα του "Network Slicing", κατά την οποία το δίκτυο χωρίζεται σε μικρότερα τμήματα για γρήγορη αντίδραση στις επιθέσεις.

Επιπλέον, προσφέρει ελέγχους που καθιστούν διαφανή για τους διαχειριστές του δικτύου τον τρόπο με τον οποίο συμπεριφέρεται μια εφαρμογή, ώστε να μπορούν να παρέμβουν για τη διαφύλαξη του δικτύου. Ο παρακάτω κατάλογος περιλαμβάνει μερικές προτάσεις για την άμυνα κατά των επιθέσεων DDoS στο περιβάλλον IoT.

Προσέγγιση με χρήση μηχανικής μάθησης (ML). Μια μέθοδος, για παράδειγμα, αποφεύγει τις επιθέσεις με τη χρήση μιας αυτοματοποιημένης λύσης Deep Packet Inspection (DPI) που μπορεί να εντοπίσει ακόμη και μη αναγνωρισμένες επιθέσεις τόσο στην εισερχόμενη όσο και στην εξερχόμενη κυκλοφορία. Αυτή η μέθοδος είναι γρήγορη και δεν απαιτεί την κατασκευή ακριβών υποδομών (Zhang et al., 2020).

SaaS (ασφάλεια ως υπηρεσία): Οι πάροχοι υπηρεσιών νέφους προσφέρουν μια συγκεκριμένη κατηγορία υπηρεσιών, γνωστή ως SaaS (Security as a Service). Επιτρέπει στις επιχειρήσεις και στους παρόχους υπηρεσιών να υπερασπίζονται το δίκτυο από διαδικτυακές απειλές. Προσέγγιση φιλτραρίσματος κίνησης με επίγνωση της ενθυλάκωσης: Αυτή η προσέγγιση ενσωματώνει τον μηχανισμό φιλτραρίσματος στην αρχιτεκτονική ασφάλειας 5G και κάνει χρήση του DPI (Deep Packet Inspection).

Αυτόματη εξαγωγή υπογραφών (ASE). Με τη δυναμική εξαγωγή των υπογραφών άγνωστων ιών και σκουληκιών που διατρέχουν το δίκτυο χωρίς την ανάγκη ανθρώπινης παρέμβασης, η λειτουργία ASE μειώνει το χρόνο απόκρισης για την ανίχνευση κακόβουλου λογισμικού. Αλγόριθμοι κρυπτογράφησης: Αυτοί οι αλγόριθμοι είναι ταχύτεροι από τους παλαιότερους αλγόριθμους και είναι ικανοί να προστατεύουν τα δίκτυα IoT.

Ασφάλεια των δρομολογητών: Οι συσκευές IoT δεν εκτελούν λογισμικό ασφαλείας. Ως πύλη που επιτρέπει την επικοινωνία των συσκευών μεταξύ τους στο Διαδίκτυο, ο δρομολογητής που συνδέει τις συσκευές μπορεί να προσφέρει ένα βελτιωμένο σύστημα ασφαλείας. Η κατασκευή ασφαλών δρομολογητών αποτελεί κορυφαία προτεραιότητα για τους κατασκευαστές δρομολογητών (Zhang et al., 2020).

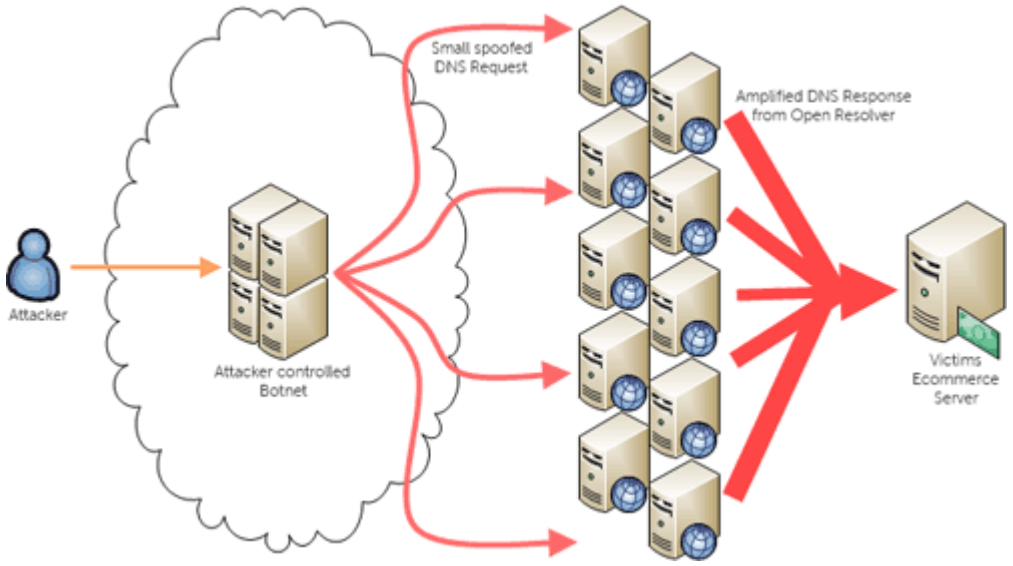
Διαχείριση συσκευών και ασφαλής εκκίνηση: Η ασφάλεια του IoT μπορεί να ενισχυθεί με την επιβεβαίωση της θέσης των συσκευών και της πλατφόρμας στην οποία χρησιμοποιούνται.

Ο έλεγχος πρόσβασης για τους πόρους των συσκευών IoT παρέχεται μέσω της εξουσιοδότησης και του ελέγχου πρόσβασης.

Εφαρμόζεται στο επίπεδο εφαρμογής, όπως η κρυπτογράφηση από άκρο σε άκρο ή ο έλεγχος ταυτότητας δύο παραγόντων (Two Factor Authentication) (Zhang et al., 2020).

Τέλος υπάρχουν τρεις κύριοι τύποι της συγκεκριμένης επίθεσης:

- **Network-centric or volumetric attacks:** Αυτό που συμβαίνει σε μία τέτοια επίθεση είναι να στέλνουν πολλαπλά πακέτα με δεδόμενα σε έναν πόρο ο οποίος είναι και στόχος με αποτέλεσμα αυτός να μην μπορεί να ανταποκριθεί και να επεξεργαστεί τα δεδομένα καταναλώνοντας αρκετά μεγάλο διαθέσιμο εύρος ζώνης.
- **Protocol Attacks :** Οι επιθέσεις πρωτοκόλλου αυτό που κάνουν είναι να χρησιμοποιούν ελλατώματα στα πρωτόκολλά τους για να κατακλύσουν και να προκαλέσουν κατάρευση στο πόρο-στόχο. Χρησιμοποιούνται συνήθως τα πρωτόκολλα του network layer ή του transport layer. Ενα παράδειγμα μίας τέτοιας επίθεσης είναι όταν κάποιος στέλνει στις διευθύνσης IP ενός πόρου-στόχου ένα μεγάλου όγκου πακέτων αρχικής αίτησης σύνδεσης χρησιμοποιώντας πλαστές IP διευθύνσεις. Αυτό προκαλεί πρόβλημα στο Πρωτόκολλο Ελέγχου Μετάδοσης το οποίο δεν μπορεί να ολοκληρωθεί λόγω της ακατάπαυστης εισροής νέων αιτημάτων.
- **Application Layer:** Σε αυτό το επίπεδο οι βάσεις δεδομένων και οι υπηρεσίες δικτύων υπερφορτώνονται με μεγάλο όγκο κλήσεων εφαρμογών. Λόγου αυτού του γεγονότος παρατηρείται και η συγκεκριμένη επίθεση της άρνησης εξυπηρέτησης. Ένα παράδειγμα μίας τέτοιας επίθεσης είναι μία επίθεση στο (HTTP) πρωτόκολλο μεταφοράς υπερκείμένου όταν ανανεώνονται πολλές ιστοσελίδες την ίδια χρονική στιγμή επανηλημένα.



Εικόνα 8

Συμπεράσματα

Λόγω του γεγονότος ότι το 5G χρησιμοποιεί πολυάριθμες καθιερωμένες και παραδοσιακές τεχνολογίες δικτύου και διαθέτει αρχιτεκτονική που επιτρέπει την ενσωμάτωση ποικίλων προηγμένων μέτρων ασφαλείας, είναι εγγενώς πιο ασφαλές από οποιοδήποτε προηγούμενο δίκτυο κινητής τηλεφωνίας. Ωστόσο, δημιουργεί σοβαρό πρόβλημα ασφάλειας λόγω των αλλαγών στο λογισμικό, του κατακερματισμού του δικτύου, του πολλαπλασιασμού των νέων προμηθευτών στην αλυσίδα εφοδιασμού και του αυξημένου αριθμού κινητών συσκευών και σταθμών βάσης. Παρά την εξαιρετική εργασία σε επίπεδο προτύπων για την ασφάλεια του 5G, εξακολουθούν να υπάρχουν σημαντικές ανησυχίες. Για να διασφαλίσουν τα δίκτυά τους, οι φορείς εκμετάλλευσης του 5G θα πρέπει να επανεξετάσουν και να εφαρμόσουν με συνέπεια τις συστάσεις κατά 3GPP και GSMA. Οι αλλαγές στην πολιτική ασφαλείας θα πρέπει να αποτελούν μέρος μιας ενδελεχούς διαδικασίας. Είναι σημαντικό να διεξάγεται επαλήθευση τόσο πριν όσο και μετά την εγκατάσταση. Με άλλα λόγια, η ασφάλεια του 5G υπερβαίνει την απλή ύπαρξη της κατάλληλης αρχιτεκτονικής ή τεχνολογίας ασφαλείας. Απαιτεί την ανάπτυξη ροών εργασίας, διαδικασιών και ομαδικής συνεργασίας. Μπορεί να είναι εξίσου εύκολο να παραβιάσει κανείς το 5G όπως είναι να παραβιάσει το Διαδίκτυο. Η δικτύωση που καθορίζεται από το λογισμικό (SDN) και η εικονικοποίηση λειτουργιών δικτύου (NFV) αποτελούν τα θεμέλια του δικτύου 5G (Zhang et al., 2020).

Τα πρωτόκολλα HTTP και REST API χρησιμοποιούνται ευρέως στις αρχιτεκτονικές SDN και NFV. Το Διαδίκτυο χρησιμοποιεί συχνά αυτά τα δύο πρωτόκολλα και είναι εξοικειωμένο με αυτά. Κάθε εχθρικός χρήστης έχει πρόσβαση σε εργαλεία για τον εντοπισμό και την εκμετάλλευση ευπαθειών, οι οποίες μπορεί να έχουν απροσδόκητα αποτελέσματα. Η διαχείριση θα γίνει ακόμη πιο δύσκολη εάν το SDN και το NFV χρησιμοποιηθούν για την τμηματοποίηση του δικτύου στο 5G. Η ευελιξία των δικτύων 5G έρχεται σε βάρος της μεγαλύτερης πολυπλοκότητας, η οποία αυξάνει την πιθανότητα λαθών ρύθμισης και παραλείψεων ασφαλείας.

Επιπλέον, τα δισεκατομμύρια συνδεδεμένα gadgets του IoT αποτελούν σοβαρή απειλή από botnets. Οι επιθέσεις κατά του IoT γίνονται όλο και πιο συχνές. Η διανομή κακόβουλου λογισμικού είναι εύκολα επεκτάσιμη, ωστόσο η προστασία των συσκευών είναι ανεπαρκής. Οι κίνδυνοι για την ασφάλεια των πληροφοριών συνήθως μειώνονται με κάθε διαδοχική γενιά δικτύων κινητής τηλεφωνίας. Κατά το σχεδιασμό της αρχιτεκτονικής του δικτύου 5G, ελήφθησαν υπόψη τα ζητήματα ασφάλειας με τα πρωτόκολλα SS7 και Diameter (τα οποία είχαν εμφανιστεί στα δίκτυα 2G, 3G, 4G και LTE). Παρά τα πολυάριθμα χαρακτηριστικά ασφαλείας στα δίκτυα 5G, η μακροχρόνια ασφάλεια θα είναι δυνατή μόνο με τη σκληρή δουλειά των τηλεπικοινωνιακών φορέων, οι οποίοι είναι υπεύθυνοι για την εφαρμογή των καλύτερων προτύπων στην πράξη, και τη συμμετοχή των χρηστών. Έχει γίνει σημαντικός όγκος έρευνας σχετικά με τον τρόπο αύξησης της ασφάλειας των δικτύων 5G (Zhang et al., 2020).

Στο πλαίσιο αυτής της προσπάθειας μελέτης αναπτύχθηκαν πολλές ενδιαφέρουσες προτάσεις που μπορούν να χρησιμοποιηθούν για τη δημιουργία ασφαλέστερων δικτύων 5G. Ως αποτέλεσμα της νέας και διαρκώς αναπτυσσόμενης τεχνολογίας που χρησιμοποιούν τα δίκτυα 5ης γενιάς, προκύπτουν πάντα νέες απειλές για την ασφάλεια, επομένως η συνεχής έρευνα στον τομέα αυτό είναι απαραίτητη. Η ασφάλεια των δικτύων 6ης γενιάς έχει ήδη τεθεί προς συζήτηση, παρά το γεγονός ότι τα δίκτυα 5ης γενιάς βρίσκονται ακόμη σε ανάπτυξη και δεν έχουν ακόμη διερευνηθεί εκτενώς. Η ασφάλεια των δικτύων 5G θα χρησιμεύσει αναμφίβολα ως θεμέλιο για την ασφάλεια των δικτύων επόμενης γενιάς, όπως είναι χαρακτηριστικό σε κάθε μετάβαση γενιάς. Όπως κάθε νέα γενιά δικτύων, έτσι και η έκτη θα έχει το μερίδιό της σε θέματα ασφάλειας, πολλά από τα οποία θα προκληθούν από τις τεχνολογίες που αποτελούν το θεμέλιό της, όπως η τεχνολογία κατανεμημένων βιβλίων (DLT), η κατανεμημένη AI/ML, η επικοινωνία ορατού φωτός (VLC) κ.λπ. Για να καταστούν τα δίκτυα 6ης γενιάς αξιόπιστα και ασφαλή στη χρήση, θα πρέπει να διερευνηθούν και να αντιμετωπιστούν διεξοδικά όλες αυτές οι προκλήσεις.

Βιβλιογραφία

Acharya, H. S., Dutta, S. R., & Bhoi, R. (2013). Network and Information Security Issues. *International Journal of Innovative Research and Development (ISSN 2278–0211)*, *2*(2), 400-406.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. *IEEE Communications Surveys & Tutorials*, *21*(4), 3682-3722.

Ahmad, W. S. H. M. W., Radzi, N. A. M., Samidi, F. S., Ismail, A., Abdullah, F., Jamaludin, M. Z., & Zakaria, M. (2020). 5G technology: Towards dynamic spectrum sharing using cognitive radio networks. *IEEE Access*, 8, 14460-14488.

Dangi, R., Lalwani, P., Choudhary, G., You, I., & Pau, G. (2022). Study and investigation on 5G technology: A systematic review. *Sensors*, *22*(1), 26.

Gordon, S. and Ford, R. (2006). "On the definition and classification of cybercrime", *Journal in Computer Virology*, vol. 2, no. 1, pp. 13-20. Available: 10.1007/s11416-006-0015-z.

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

Nelson Machado Junior (2021). *A Brief Introduction To 5G Technology*, https://medium.com/the-shadow/a-brief-introduction-to-5gtechnologyb50c0f453f4

Pham, Q. V., Fang, F., Ha, V. N., Piran, M. J., Le, M., Le, L. B., ... & Ding, Z. (2020). A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art. *IEEE Access*, *8*, 116974-117017.

N. Provos, M. Rajab and P. Mavrommatis, (2009). "Cybercrime 2.0", *Communications of the ACM*, vol. 52, no. 4, pp. 42-47. Available: 10.1145/1498765.1498782.

Salah, I., Mabrook, M. M., Hussein, A. I., & Rahouma, K. H. (2021). Comparative study of efficiency enhancement technologies in 5G networks-A survey. *Procedia Computer Science*, *182*, 150-158.

Storck, C. R., & Duarte-Figueiredo, F. (2020). A survey of 5G technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles. *IEEE access*, *8*, 117593-117614.

Zhang, J., Björnson, E., Matthaiou, M., Ng, D. W. K., Yang, H., & Love, D. J. (2020). Prospective multiple antenna technologies for beyond 5G. *IEEE Journal on Selected Areas in Communications*, *38*(8), 1637-1660.

Ιωάννης Δημ. Ιγγλεζάκης, (2021). *Δίκαιο Πληροφορικής*, εκδόσεις Σάκκουλα.

Κωνσταντίνος Βλαχόπουλος, (2007). *Ηλεκτρονικό Έγκλημα -Μορφές, Πρόληψη, Αντιμετώπιση,* Νομική Βιβλιοθήκη.

(CISA, 2020)

(CISA, 2021)

(COSMOTE, 2022)

Jason Glassberg, (2019, September 5). What will 5G mean for business cybersecurity?. *The business Journals.*

William,Stallings.(2006).*CRYPTOGRAPHY AND NETWORK SECURITY*.(4th ed.). USA: Pearson Education Incorporation as Prentice Hall.

Ιάκωβος, Στ. Βενιέρης.(2013). *ΔΙΚΤΥΑ ΕΥΡΕΙΑΣ ΖΩΝΗΣ: Τεχνολογίες και Εφαρμογές με Έμφαση στο Διαδίκτυο.*.Ελλάδα: Εκδόσεις Τζιόλα.

Φίλιππος, Κωνσταντίνου, & Αθανάσιος, Κανατάς, & Πάντος, Γεώργιος.(2013). *ΣΥΣΤΗΜΑΤΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ*.(2η εκ.). Ελλάδα: Εκδόσεις Παπασωτηρίου.

Γεώργιος, Κ. Καραγιαννίδης, & Κοραλία, Ν. Παππή. (2018). ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ. (4η εκ.). ΕΛΛΑΔΑ: Εκδόσεις Τζιόλα.

JYRKI T. J. PENTTINEN. (2019). 5G EXPLAINED Security and Deployment of Advanced Mobile Communications. USA: 2019 John Wiley & Sons Ltd.

Σύνδεσμοι:

- https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf [1]
- https://www.youtube.com/watch?v=yhs8bGmfJ4g&t=503s&ab_channel=COSMOTE [2]
- https://www.cisa.gov/5g-library [3]
- https://www.bizjournals.com/bizjournals/how-to/technology/2019/09/what-will-5g-mean-for-business-cybersecurity.html [4]
- https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons [5]