Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ιδιωτικότητα σε Έξυπνους Ψηφιακούς Βοηθούς (Smart Virtual Assistants)

Αλέξανδρος Χριστοφή

Επιβλέπων Καθηγητής

Σταύρος Σιαήλης

Νοέμβριος 2021

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Ιδιωτικότητα σε Έξυπνους Ψηφιακούς Βοηθούς (Smart Virtual Assistants)

Αλέξανδρος Χριστοφή

Επιβλέπων Καθηγητής
Σταύρος Σιαήλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών Μεταπτυχιακού Προγράμματος Σπουδών Ασφάλειας Υπολογιστών και Δικτύων από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Νοέμβριος 2021

Περίληψη

Η εργασία αυτή μελετά τις προκλήσεις που υπάρχουν όσον αφορά την ιδιωτικότητα που υπάρχει κατά την χρήση Έξυπνων Ψηφιακών Βοηθών (ΕΨΒ) που υπάρχουν ως επί τον πλείστων στα σπίτια των χρηστών. Ανεξάρτητα με τα μέτρα και τους κανονισμούς που επιβάλλονται συνεχώς για την αντιμετώπιση αυτών των ανησυχιών, οι πληροφορίες που έρχονται στην κατοχή τέτοιων συσκευών θα μπορούσαν να προκαλέσουν προβλήματα όσον αφορά την ιδιωτικότητα και τη ψηφιακή ζωή του χρήστη, εκθέτοντας ευαίσθητες πληροφορίες.

Με τη χρήση ενός ΕΨΒ και συγκεκριμένα του Google Nest Mini 2nd generation, έγινε εκτέλεση μερικών πειραμάτων με σκοπό τη συλλογή πληροφορίων και της διερεύνησης των δεδομένων που μαζεύονται και στέλνονται/μεταδίδονται από τη συσκευή. Επίσης μέσω υλοποίησης αλγόριθμων εκμάθησης μηχανής (Machine Learning) για την ταξινόμηση των κρυπτογραφημένων δεδομένων που στάλθηκαν μέσω του δικτύου και μέσω SLC (Supervised Learning Classifiers) γίνεται προσπάθεια υπολογισμού της κάθε εντολής που δόθηκε από τον χρήστη. Μέσα από τα αποτελέσματα φαίνεται η δυνατότητα τέτοιων μεθόδων να εξάγουν κάποια προσωπικά δεδομένα παρόλο που τα δεδομένα είχαν διαδοθεί κρυπτογραφημένα.

Summary

This dissertation studies the privacy challenges that IoT and connected devices introduce. The main focus is on Virtual Personal Assistants, which are progressively being established in homes. The privacy of these devices is still an issue that has not been solved and its implications could threat the sensitive information of everyday users. Despite the measures and regulations that have been enforced to address these concerns, the personal information that smart home devices collect and transmit could induce exposures that are crucial for the preservation of digital identity and privacy.

An experimental study was carried out using a Google Nest Mini 2nd generation device in order to collect and investigate the data that the device receives and transmits. By using Machine Learning algorithms, attempts have been made to classify the encrypted data that the device collects and through Supervised Learning Classifiers predict which queries were made by the user. The results show the capabilities of such techniques to expose personal information, regardless of the encryption of the data that are being transmitted.

Περιεχόμενα

1. Εισαγωγή

Η πρόοδος της τεχνολογίας και των έξυπνων οικιακών συσκευών έχει δημιουργήσει έναν διασυνδεδεμένο κόσμο για πρώτη φορά στα χρονικά. Τα δεδομένα πλέον θεωρούνται από τους πιο πολύτιμους πόρους τα τελευταία χρόνια. Η μαζική αυτή συλλογή δεδομένων έχει οδηγήσει πολλές εταιρείες σε τεράστια ανάπτυξη και αύξηση των κερδών τους, δημιουργώντας όμως μεγάλες ανησυχίες σχετικά με το σκοπό που χρησιμοποιούν τα δεδομένα αυτά. Με αφορμή διάφορα περιστατικά που έχουν λάβει μέρος τα τελευταία χρόνια έχει δημιουργηθεί μια γενική δυσπιστία για το πως οι εταιρείας διαχειρίζονται και εάν διατηρούν ασφαλή τα προσωπικά δεδομένα που συλλέγουν.

Η χρήση των έξυπνων συσκευών έχει καθιερωθεί στην καθημερινότητά μας, ξεκινώντας από smartphone, smartwatches, smart TV, μέχρι έξυπνα αυτοκίνητα, έξυπνα σπίτια, έξυπνα δίκτυα και τελικά έξυπνες πόλεις. Αυτή η αλληλεπίδραση με έξυπνες συσκευές παράγει τεράστιο όγκο δεδομένων που συνήθως οι εταιρείες συλλέγουν και χρησιμοποιούν για να βελτιώσουν την εμπειρία των χρηστών για τα προϊόντων τους. Ωστόσο, τις περισσότερες φορές, τα δεδομένα πωλούνται και σε διαφημιστικές εταιρείες για να χρησιμοποιηθούν για πιο βελτιωμένη και στοχευμένη διαφήμιση.

Σε αυτήν την αναφορά, η εστίαση είναι στις έξυπνες οικιακές συσκευές και, συγκεκριμένα, στους Έξυπνους Ψηφιακούς Βοηθούς (ΕΨΒ). Η ικανότητα ενός ΕΨΒ να παρέχει χρήσιμες πληροφορίες και ακόμη και να ελέγχει πολλές έξυπνες συσκευές μέσω φωνητικών εντολών κάνει τη ζωή του χρήστη πολύ πιο εύκολη. Η τεχνολογία έδωσε τη δυνατότητα στους ανθρώπους να έχουν πρόσβαση σε κάθε είδους πληροφορίες, επικοινωνία, ειδήσεις, μέσα ενημέρωσης και ψυχαγωγία μέσω των δακτύλων τους. Σε έναν κόσμο που κινείται συνεχώς γρήγορα, αυτή η ικανότητα περνά από τα δάχτυλα των ανθρώπων στη χρήση της φωνής τους. Η διαχρονική ανάγκη της ανθρωπότητας να βρει τρόπους να κάνει περισσότερα με λιγότερη προσπάθεια ώθησε για μια ακόμη τεχνολογική βελτίωση. Η μεγαλύτερη ανησυχία σχετικά με τη χρήση των ΕΨΒ επικεντρώνεται στη συλλογή προσωπικών πληροφοριών και στην πιθανή παραβίαση του απορρήτου.

Σκοπός της έρευνας είναι να μελετήσει πόσο εύκολο είναι για ένα κακόβουλο χρήστη να παρακολουθήσει και να συλλέξει πληροφορίες για ένα χρήστη ΕΨΒ. Με τη διεξαγωγή πειραματικών διαδικασιών θα μελετηθεί ποιες πληροφορίες μπορεί να μαζέψει ο θύτης για να δημιουργήσει ένα προφίλ για τον ανυποψίαστο χρήστη και έπειτα να προχωρήσει σε περαιτέρω επιθέσεις.

Οι ευαίσθητες πληροφορίες αυτές είναι πολύ εύκολο να ανιχνευτούν από ένα κακόβουλο χρήστη που βρίσκεται στο ίδιο δίκτυο με το θύμα, αφού αποτελούν δεδομένα τα οποία δεν κρυπτογραφούνται κατά την αλληλεπίδραση με τη συσκευή.

2. Ανασκόπηση

Σε αυτό το κεφάλαιο, μελετάται η χρήση των ΕΨΒ και εξετάζονται τα ζητήματα απορρήτου σχετικά με τη χρήση τους σε οικιακά δίκτυα. Επιπλέον, διερευνώνται ορισμένα περιστατικά και απειλές που έχουν ήδη αναφερθεί.

2.1 Η ανάγκη για Προσωπικούς Έξυπνους Βοηθούς

Από τη πρώτη στιγμή που ανακαλύφτηκαν οι Η/Υ, ο άνθρωπος είχε ως στόχο την αλληλεπίδραση μαζί τους χρησιμοποιώντας φωνητικές εντολές ή ακόμα και με διάλογο. Ακόμα και πριν μερικές δεκαετίες ένας διάλογος με συνομιλητή έναν Η/Υ φάνταζε σενάριο επιστημονικής φαντασίας. Παρόλα αυτά, πολλά προϊόντα αναπτύχθηκαν τα τελευταία χρόνια και συνεχίζουν να αναπτύσσονται, όπου επέφεραν στη καθημερινότητα μας συσκευές όπως τους φωνητικούς βοηθούς (voice assistants), με πάρα πολλά χαρακτηριστικά να προστίθενται συνεχώς στις δυνατότητες τους. Έχουν εγκατασταθεί στη καθημερινότητα μας και έχουν κάνει τις ζωές μας πολύ πιο άνετες, εκτελώντας περισσότερες διαδικασίες σε πιο λίγο χρόνο και πιο αποτελεσματικά έχοντας ως άμεσο επακόλουθο τη ραγδαία αύξηση αγοράς τέτοιων συσκευών από τους χρήστες.
Αποτελεί πρωταρχικό στόχο λοιπόν οι Έξυπνοι Ψηφιακοί Βοηθοί (ΕΨΒ) να είναι ασφαλείς και να διατηρούν την ιδιωτικότητα του χρήστη εφόσον έχουν πρόσβαση σε ευαίσθητα και προσωπικά δεδομένα. Παρά τους κανονισμούς και τα μέτρα που επιβάλλονται συνεχώς, τα προσωπικά δεδομένα που συλλέγονται και μεταδίδονται από κάθε συσκευή μπορεί να εκτεθούν έχοντας καίρια σημασία στη διατήρηση του απορρήτου του χρήστη και της ψηφιακής του ταυτότητας (Abd, et al., 2019).

2.1.1 Τι είναι οι Έξυπνοι Ψηφιακοί Βοηθοί

Έξυπνοι Ψηφιακοί Βοηθοί (ΕΨΒ) είναι πράκτορες λογισμικού (software agents) όπου ερμηνεύουν την ομιλία από τον άνθρωπο και απαντούν επίσης με ομιλία .Το Echo/Alexa της Amazon, το Google Home/Assistant, το Apple's Siri και το Cortana της Microsoft αποτελούν τους πιο γνωστούς έξυπνους φωνητικούς βοηθούς (smart voice assistants) και είναι συνήθως εγκατεστημένοι σε κινητά τηλέφωνα, ηχεία σπιτιού και προσωπικούς υπολογιστές. Τα λογισμικά τους βρίσκονται σε συνεχή εγρήγορση και περιμένουν να ακούσουν τη λέξη κλειδί για να 'ξυπνήσουν' και να εκτελέσουν τις εντολές που δίνει ο χρήστης (Hoy, 2018). Οι χρήστες έχουν τη δυνατότητα να εκτελέσουν διάφορες λειτουργίες με φωνητικές εντολές. Αφού η συσκευή ακούσει τη λέξη κλειδί και ξεκινήσει να ηχογραφεί αυτά που λέει ο χρήστης στέλνει τις πληροφορίες σε ένα εξειδικευμένο server όπου επεξεργάζεται και ερμηνεύει τις εντολές του χρήστη. Ανάλογα με την εντολή που είχε δοθεί, ο server θα δώσει στο voice assistant τις απαραίτητες πληροφορίες για να έρθουν πίσω στο χρήστη. Πολλές συσκευές I-o-T (Internet of Things) πλέον κατασκευάζονται για να μπορούν επίσης να ελέγχονται με φωνητικές εντολές και ως επακόλουθο ο αριθμός των υπηρεσιών (services) που υποστηρίζουν φωνητικές εντολές να αυξάνεται ραγδαία (Hoy, 2018).

2.1.2Τι μπορούν να κάνουν οι Έξυπνοι Ψηφιακοί Βοηθοί

Υπάρχουν αρκετές εταιρείες που κατασκευάζουν τα δικά τους προϊόντα και το κάθε ένα από αυτά περιέχει τα δικά του χαρακτηριστικά, παρόλο που οι δυνατότητες τους και οι υπηρεσίες που μπορούν να παρέχουν σε σύγκριση με άλλες εταιρείες κυμαίνονται στα ίδια επίπεδα.

Το Google Nest το οποίο χρησιμοποιείται σε αυτή την έρευνα, έχει τις πιο κάτω δυνατότητες (Google, 2021):

- Έχει επαφή με τα μέσα μαζικής ενημέρωσης. Μπορεί να παίξει μουσική, να εκφωνήσει τελευταία νέα από έμπειρες πυγές, να απεικονίσει νέα (με την

προϋπόθεση ότι υποστηρίζεται με Chromecast), να παίξει δημοφιλής podcasts, να παίξει ραδιοφωνικούς σταθμούς, να παίξει αποθηκευμένη μουσική άλλης συσκευής χρησιμοποιώντας Bluetooth, να διαβάσει ακουστικά βιβλία από το Google Play Books και να κάνει κοινή χρήση με μέλη της οικογένειας ή φίλους.

- Μπορεί να ελέγχει τηλεοράσεις και ηχεία με τη δυνατότητα να ανοίξει, να τα κλίσει και να παίξει YouTube TV. Εφόσον η τηλεόραση υποστηρίζεται με Chromecast τότε θα μπορούσε να απεικονίσει στη τηλεόραση ταινίες και τηλεοπτικές εκπομπές, να παίξει videos από το YouTube, να απεικονίσει προσωπικές φωτογραφίες που βρίσκονται στη Google βιβλιοθήκη (US μόνο), να παίξει ακουστικό περιεχόμενο σε ηχεία και τηλεοράσεις, να παίξει συγχρονισμένη μουσική ταυτόχρονα σε πολλά έξυπνα ηχεία και να δήξει τη πρόβλεψη του καιρού στη τηλεόραση.
- Μπορεί να δίνει πληροφορίες για τη κίνηση στους δρόμους, χρησιμοποιώντας μια ρουτίνα που σχετίζεται με υπενθυμίσεις, καθημερινά νέα ημερολόγιου και καιρικές συνθήκες, κοιτάζοντας κοντινά μέρη και πληροφορίες για αυτά, να καταχωρήσει γεγονότα που θα γίνουν στο μέλλον, να κρατά χρονόμετρο να δώσει πληροφορίες για ενδεχόμενες αεροπορικές πτήσεις που ίσως ενδιαφέρουν τον χρήστη και τέλος μπορεί να ενωθεί με τρίτα προγράμματα εκτελώντας ανάλογες λειτουργίες.
- Μπορεί επίσης να κρατά λίστες, να παραγγέλνει υλικά αγαθά, να βρίσκει συνταγές, να πραγματοποιεί κλήσεις, να δημιουργεί shortcuts, να προωθεί μηνύματα σε άλλα ηχεία που είναι συνδεδεμένα στο σπίτι και να στέλνει πληροφορίες στο κινητό τηλέφωνο.
- Μπορεί να ελέγχει, έξυπνες συσκευές που βρίσκονται μέσα στο δίκτυο, online services και τρίτες έξυπνες συσκευές, να μεταδίδει την εικόνα από κάμερες ασφαλείας.
- Μπορεί επίσης με τη δοκιμή ερωτήσεων να αποκαλυφτεί κάτι το οποίο δεν γνωρίζουμε. Τέλος μπορεί να παίζει παιχνίδια γνώσεων και να πει αστεία ή ιστορίες.

Επιπρόσθετα σε αυτά μπορούν να προστεθούν διαφορετικά χαρακτηριστικά σε κάθε συσκευή το οποία ονομάζονται ‘‘skills’’ και μπορούν να αυξήσουν τις δυνατότητες της συσκευής συνδέοντας την με άλλες συσκευές μέσω φωνητικών εντολών. Οι δεξιότητες αυτές αναπτύσσονται συνήθως από τρίτους προγραμματιστές με παρόμοιο τρόπο που φτιάχνονται τα προγράμματα και τα έξυπνα κινητά τηλέφωνα (Hoy, 2018). Για παράδειγμα το Google Assistant μπορεί να επικοινωνήσει με διάφορα εργαλεία τα οποία επιτρέπουν στο χρήστη να δημιουργήσει τις δικές του δεξιότητες που θέλει να προσθέσει στη συσκευή.

2.1.3 Αρχιτεκτονική

Ένα χαρακτηριστικό του οικοσυστήματος όπου οι ΕΨΒ λειτουργούν είναι ότι οι δυνατότητες του δεν περιορίζονται σε μια φυσική συσκευή αλλά σε όλες τις συσχετισμένες τεχνολογίες. Η λειτουργίες των προσωπικών έξυπνων βοηθών μπορούν να χωριστούν σε διαφορετικά στάδια από τα οποία το κάθε ένα από αυτά μπορεί να αποτελέσει πιθανό στόχο επίθεσης από έναν επιτιθέμενο (CUELLAR, 2020).

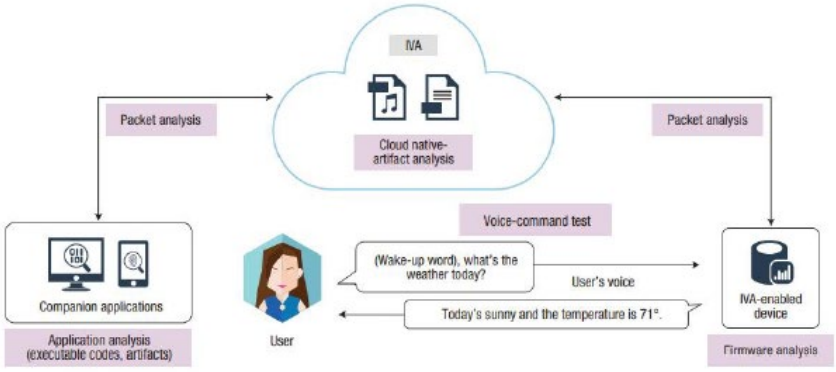
Το πρώτο στάδιο είναι η επικοινωνία μεταξύ των χρηστών και των συσκευών. Οι συσκευές αυτές έχουν ενσωματωμένους δέκτες και πολύ πιθανόν διαμεσολαβητές ομιλίας όπου καταγράφουν τις εκφράσεις του χρήστη. Η συσκευή για να μπορεί να χρησιμοποιηθεί πρέπει να είναι ενωμένη με το διαδίκτυο και έπειτα να βρίσκεται συνέχεια σε αναμονή έτσι ώστε όταν ακούσει τη λέξη κλειδί (κάθε εταιρεία έχει τις δικές τις λέξεις κλειδιά, στην έρευνα αυτή που χρησιμοποιείται το Google Nest mini οι λέξεις κλειδιά είναι ‘Hey Google’ και ‘Okay Google’) να ‘ξυπνήσει’ και να μπορεί να καταγράψει τις φωνητικές εντολές που δίνει ο χρήστης, οι οποίες γίνονται από αναλογικές εντολές σε ψηφιακές για να αναλυθούν από τη συσκευή.

Στο δεύτερο στάδιο αφού η φωνητική εντολή του χρήστη έχει ήδη μετατραπεί σε ψηφιακή καταγραφή, αποστέλλεται από τη συσκευή στο διακόπτη-δρομολογητή (switch-router) του σπιτιού και στη συνέχεια στις cloud υπηρεσίες της εταιρείας για περαιτέρω ανάλυση.

Σε ένα τρίτο στάδιο, η ψηφιακή καταγραφή αποστέλλεται στο cloud για να μελετηθεί από το Natural Language Process (NLP) και να αναλύσει τον τρόπο ομιλίας/έκφρασης του χρήστη και να ανταποκριθεί στις εντολές του. Καταγράφοντας στο cloud, το NLP εξετάζει τη σημαντικότητα από πηγές που βρίσκονται στο διαδίκτυο και τη βάση δεδομένων της συσκευής έτσι ώστε να μπορεί να δώσει τη πιθανότερο καταλληλότερη απάντηση.

Κατά το τέταρτο στάδιο οι χρήστες οι οποίοι είναι συνδεδεμένοι με το παροχέα υπηρεσίας cloud μπορούν να αλληλοεπιδράσουν με τη συσκευή ή ακόμα και να δουν καταγραφές της εφαρμογής.

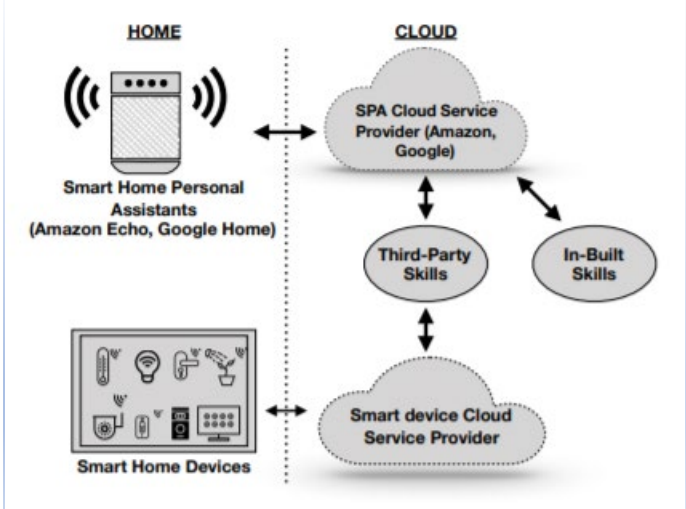
Στο πέμπτο στάδιο, η εταιρεία που έχει το cloud αναθεωρεί εάν υπάρχει εγχώρια εφαρμογή που να μπορεί να εκπληρώσει το αίτημα του χρήστη. Σε αυτή τη περίπτωση επεξεργάζεται το αίτημα του χρήστη και δίνεται η καλύτερη δυνατή απάντηση πίσω στην έξυπνη συσκευή. Εάν για κάποιο λόγο δεν υπάρχει εγχώρια εφαρμογή σε διαθεσιμότητα, οι ΕΨΒ στέλνουν το αίτημα σε τρίτες εφαρμογές.



Εικόνα 1 (Hyunji, et al., 2017): Εικόσύστημα ΕΨΒ 1

Στη περίπτωση όπου ο σκοπός του έξυπνου βοηθού είναι να ελέγχει άλλες έξυπνες συσκευές, οι πληροφορίες στέλνονται συγκεκριμένα στα cloud αυτών που διαχειρίζονται τις έξυπνες συσκευές για να αναλύσουν τα αιτήματα[Εικόνα 2].

Ο αισθητήρας ή η έξυπνη συσκευή λαμβάνει το αίτημα και το εκτελεί.



Εικόνα 2 (Abd, et al., 2019)

2.2 Ιδιωτικότητα και Ασφάλεια

Οι συσκευές IoT (Internet of Things) έχουν καθιερωθεί σε διάφορους ευαίσθητους τομείς και έχουν επίσης αλλάξει τον τρόπο με τον οποίο συλλέγουν και επεξεργάζονται τις πληροφορίες, ως εκ τούτου διάφοροι νόμοι και κανονισμοί πρέπει να διασφαλίζουν τη προστασία του απορρήτου του χρήστη (Rachelle, et al., 2017). Μια από τις πιο σημαντικές αλλαγές στον τομέα αυτό είναι η θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR). Το GDPR τέθηκε επίσημα σε ισχύ στις 25 Μαΐου 2018 και αντικατέστησε την Οδηγία Προστασίας Δεδομένων του 1995. Ο κύριο στόχος του GDPR είναι η θεσμοθέτηση νόμων που να προστατεύουν τα απόρρητα δεδομένα πολιτών της ΕΕ και να επαναπροσδιορίζει τους ρόλους στη διαδικασία και τη διαχείριση δεδομένων σε εταιρείες προκειμένου να διασφαλιστεί η προστασία του απορρήτου. Μερικές από τις αλλαγές που έφερε το GDPR είναι η διεύρυνση του ορισμού για τα ευαίσθητα δεδομένα με αρχές όπως το Privacy by Design και άλλα δικαιώματα όπως το δικαίωμα πρόσβασης (Right of Access), δικαίωμα ενημέρωσης (Right to be informed) και δικαίωμα στη λήθη (Right to be Forgotten). Οποιαδήποτε εταιρεία ή οργανισμός δεν συναινεί στους κανονισμούς του GDPR μπορεί να επιβάλει σημαντικό πρόστιμο.

Η χρήση και αυτοματοποίηση των συσκευών IoT όπου ανταλλάσσονται πληροφορίες και δεδομένα για λογαριασμό των χρηστών δημιουργεί σοβαρούς κινδύνους παραβίασης του ελέγχου των προσωπικών πληροφοριών που παρέχει το GDPR (Junwoo, et al., 2017). Η αρχή Privacy by Design θα μπορούσε να συμβάλει στη αύξηση της εμπιστοσύνης των χρηστών (Wachter, 2018). Όσον αφορά τη διαφάνεια και τη συναίνεση των χρηστών, υπάρχουν προτάσεις για την ηλεκτρονική επικοινωνία των χρηστών που θα μπορούν να απαντούν ηλεκτρονικά και να εκφράσουν τις επιλογές τους για απόρρητο.

Αξιοσημείωτο πως οι ΕΨΒ έχουν ενσωματωμένες τεχνολογίες για αναγνώριση φωνητικών εντολών, αυτόματα τους δίνεται το δικαίωμα να ηχογραφούν φωνητικές εντολές και διαλόγους. Εφόσον οι εντολές και οι συζητήσεις παράγουν τεράστια μάζα ευαίσθητων και μη, πληροφορίων, αυτό δεν περνά ανεκμετάλλευτο από τις αρμόδιες εταιρείες αφού μαζεύουν και αναλύουν όλες αυτές τις πληροφορίες. Η συλλογή και η ανάλυση που γίνεται μπορεί να έχει ως στόχο τη βελτιστοποίηση των λειτουργιών των συσκευών, παρόλα αυτά όμως οι ευαίσθητες πληροφορίες που αφορούν το κάθε χρήστη θα είναι εκτεθειμένες στους νόμους του GDPR ή σε χειρότερες περιπτώσεις παραβιάσεις των. Ως εκ τούτου, ενδείξεις για το ποιες πληροφορίες αποθηκεύει ένας ΕΨΒ και πως τις χρησιμοποιεί, επιβάλλονται με κάποιους κανονισμούς για να υπάρχει έλεγχος μέχρι το σημείο που είναι εφικτό (Gray, 2016).

2.2.1 Ιδιωτικότητα στους Προσωπικούς Έξυπνους Βοηθούς

Οι ΕΨΒ ενισχύονται από τεχνολογίες αναγνώρισης ομιλίας, έχοντας ως άμεσο δικαίωμα την καταγραφή φωνητικών εντολών και συνομιλιών. Πιο πάνω έχει αναλυθεί πως λειτουργεί η αρχιτεκτονική ενός ΕΨΒ και πως τα δεδομένα καταλήγουν στις εταιρείες. Αυτό επιτρέπει στις εταιρείες να συλλέγουν και να αναλύουν τεράστιες ποσότητες προσωπικών δεδομένων.

Η συλλογή δεδομένων και φωνητικών εντολών που δίνονται από τον χρήστη επιτρέπουν στην αναγνώριση ομιλίας να μπορεί να βελτιώνεται με την πάροδο του χρόνου, να

προσαρμόζεται στα μοτίβα ομιλίας και την προφορά του χρήστη εκτελώντας γλωσσική ανάλυση. Ωστόσο, η συλλογή τέτοιων δεδομένων μπορεί να καταλήξει σε πιθανές παραβιάσεις του απορρήτου και να βάλει σε κίνδυνο το προσωπικά δεδομένα των χρηστών. Επιπλέον αποθήκευση φωνητικών εντολών του χρήστη εμπίπτει στην προστασία των βιομετρικών στοιχείων από τον GDPR και στο πλαίσιο του νόμου περί απορρήτου. Επομένως, μια σαφής ένδειξη στον χρήστη για το πότε μια συσκευή ΕΨΒ μεταδίδει και αποθηκεύει δεδομένα εξωτερικά επιβάλλεται από τους κανονισμούς και μπορεί να βοηθήσει στη βελτίωση της εμπιστοσύνης του καταναλωτή (Gray, 2016).

Σε συνέχεια των πιο πάνω η κατοχή τέτοιων ιδιωτικών πληροφοριών καθιστά τις συσκευές πιθανό στόχο για κακόβουλους χρήστες με σκοπό να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες του θύματος, οι οποίες στη συνέχεια μπορούν να χρησιμοποιηθούν για περαιτέρω κακόβουλες ενέργειες. Όπως περιεγράφηκε πιο πάνω οι ΕΨΒ μεταφέρουν πληροφορίες σε διαφορετικά επίπεδα, στα οποία για κάθε ένα από αυτά μπορούν να υπάρξουν διαφορετικές απειλές. Υπάρχουν τεχνικές που μπορούν να αναγνωρίσουν μοτίβα σε κρυπτογραφημένα δεδομένα και να οδηγήσουν σε αναγνώριση της κατάστασης της συσκευής ή για ποιο λόγο χρησιμοποιείται η συσκευή από τον χρήστη.

3. Σχετική Έρευνα

Η συλλογή και η κατοχή ιδιωτικών πληροφοριών καθιστά τις συσκευές ΕΨΒ πιθανό στόχο για κακόβουλους χρήστες που θα μπορούσαν να αποκτήσουν ευαίσθητες πληροφορίες σχετικά με τα θύματα, οι οποίες στη συνέχεια μπορούν να χρησιμοποιηθούν για περαιτέρω κακόβουλες ενέργειες. Οι ΕΨΒ μεταφέρουν τις πληροφορίες του χρήστη σε διαφορετικά επίπεδα και για κάθε ένα από αυτά μπορούν να βρεθούν διαφορετικές απειλές. Αυτή η ενότητα προσφέρει μια επισκόπηση γνωστών επιθέσεων στο σύστημα ΕΨΒ και τα τρωτά σημεία που εκμεταλλεύονται.

Ο Πίνακας 1 δείχνει μια επισκόπηση των πιο σχετικών επιθέσεων που έγιναν σε προηγούμενες έρευνες και εκμεταλλεύονται συγκεκριμένα σημεία στην αρχιτεκτονική (Jide, et al., 2020). Διαπιστώθηκε ότι οι περισσότερες επιθέσεις στοχεύουν τα ακόλουθα στοιχεία της αρχιτεκτονικής:

(1) Συσκευή χρήστη: Υπάρχει ένα ευρύ φάσμα επιθέσεων που στοχεύουν αυτό το σημείο της αρχιτεκτονικής.

Πιο συγκεκριμένα:

i) εκμετάλλευση αδύναμου ελέγχου ταυτότητας και

ii) επίθεση σε υποκείμενες και ολοκληρωμένες τεχνολογίες.

(2) Συσκευή ΕΨΒ στο σύννεφο (cloud) παρόχου υπηρεσιών SPA: Υπάρχει μια επίθεση που στοχεύει αυτό το σημείο της αρχιτεκτονικής και εκμεταλλεύεται την ακατάλληλη απόκρυψη πληροφοριών της κυκλοφορίας πακέτων δικτύου των ΕΨΒ.

(3) Σύννεφο παρόχου υπηρεσιών ΕΨΒ: Υπάρχουν επίσης αρκετές επιθέσεις σε αυτό το σημείο της αρχιτεκτονικής που στοχεύει στοιχεία του cloud. Εντοπίστηκαν έργα που εκμεταλλεύονται

i) Ευπάθειες ML και

ii) υποκείμενες τεχνολογίες.

(4) Δεξιότητες Ιστού τρίτου μέρους: Επιθέσεις που στοχεύουν σε αυτό το σημείο της αρχιτεκτονικής χρήστη που εκμεταλλεύεται λανθασμένες αντιλήψεις για το σύστημα ΕΨΒ.

Δεν φαίνεται να βρέθηκαν επιθέσεις που να στοχεύουν αρχιτεκτονικά στοιχεία που αφορούν απομακρυσμένη πρόσβαση μέσω κινητού και Ιστού ή από άλλες συνδεδεμένες έξυπνες συσκευές.

Επίθεση	Weak Authentication			Weak Authorization			Profiling		Adversarial AI		Integrated Techs.		
	Wake up Word	Always Listening	Synthesized Speech	Payment Auth.	Multiuser Environ.	External Party	Traffic Analysis	Uncont. Infer,	ML	NLP Vul	Skills	Cloud	Smart Devices
Side Channel	√	√		√									√
Behavioral Profiling							√						
Attack on Voice Models using Adversarial samples	√	√							√				
Skill Squatting & Masquerading									√	√	√		

Πίνακας 1. Κατηγοριοποίηση επιθέσεων προηγούμενων ερευνών (Jide, et al., 2020).

Επιπρόσθετα επιθέσεις ανάλυσης της κυκλοφορίας και πιο συγκεκριμένα επιθέσεις στο πρωτόκολλο SSL 3.0 (Aveek, et al., 2016) που έδειξαν πως η διεύθυνση URL ενός αιτήματος HTTP GET διαρρέει στο SSL επειδή τα κρυπτογραφημένα κείμενα αποτυγχάνουν να συγκαλύψουν το μήκος απλού κειμένου.

Σε άλλη έρευνα αναλύθηκαν σε πειραματικό στάδιο οι ρυθμοί αποστολής και λήψης της κίνησης SSL μεταξύ του Echo (amazon) και μιας μεμονωμένης ηλεκτρονικής διεύθυνσης του amazon.com. Η επισκεψιμότητα SSL συσχετίστηκε αισθητά με τις αλληλεπιδράσεις χρηστών. Εφόσον ένας εισβολέας σε επίπεδο δικτύου μπορούσε να αναγνωρίσει τη συγκεκριμένη ροή IP ότι προέρχεται από μια Echo συσκευή, οι αιχμές της κυκλοφορίας SSL έδειξαν ξεκάθαρα πότε σημειώθηκαν αλληλεπιδράσεις με τους χρήστες. Σε ορισμένους, αυτό μπορεί να μην φαίνεται να αποτελεί ευπάθεια απορρήτου, επειδή τα περιεχόμενα των ερωτήσεων είναι κρυπτογραφημένα. Ωστόσο, απλά μαθαίνοντας τις ώρες της ημέρας που οι πελάτες αλληλοεπιδρούν με μια συγκεκριμένη συσκευή θα μπορούσε να κατέληγε σε ανεπιθύμητες διαφημιστικές καμπάνιες (Noah, et al., 2017).

Ήδη από το 2004, έχει παρατηρηθεί η χρήση τεχνικών Μηχανικής Μάθησης για την ταξινόμηση της κυκλοφορίας που είναι σε θέση να αναγνωρίζουν και να ταξινομούν κρυπτογραφημένη κίνηση δικτύου σε πραγματικό χρόνο (Nguyen & Armitage, 2008) (Gu, et al., 2011). Τέτοιες τεχνικές μπορούν να αναγνωρίσουν μοτίβα σε κρυπτογραφημένα δεδομένα και να οδηγήσουν σε αναγνώριση της κατάστασης της συσκευής ή εάν ένας χρήστης χρησιμοποιεί τη συσκευή αυτή τη στιγμή για να ακούσει μουσική ή να πραγματοποιήσει αγορές στο διαδίκτυο.

Στις αρχές του 2017, υπήρξαν άλλες αναφορές σχετικά με τη χρήση μη κρυπτογραφημένων πακέτων δικτύου που επιτρέπουν τη μεταφορά δεδομένων εικόνας υλικολογισμικού και θα μπορούσαν να παρέχουν σε μη εξουσιοδοτημένους φορείς τη δυνατότητα να αναθεωρήσουν, να κατανοήσουν και ενδεχομένως να εκμεταλλευτούν τις λειτουργίες της συσκευής (micakisa, 2017).

Κατά τη διάρκεια του ίδιου έτους, άλλες αναφορές υποδεικνύουν ότι η πρόσβαση στο ενσωματωμένο API ήταν δυνατή χωρίς έλεγχο ταυτότητας ή κρυπτογράφηση και κατέστη δυνατή η εκτέλεση εντολών που μπορούσαν να αλλάξουν τον όγκο των συναγερμών, να

ενεργοποιήσουν την πρόσβαση Beta-Firmware, να επανεκκινήσουν τη συσκευή, να συνδεθούν σε άλλη Δίκτυο Wi-Fi και να διαγράψουν αμέσως τα δεδομένα πρόσβασης Wi-Fi (Morgenstern, 2017).

4. Ερευνητικές Μέθοδοι

Σε αυτό το κεφάλαιο περιγράφονται οι διάφορες φάσεις της πειραματικής διαδικασίας που υλοποιήθηκε και αναλυτικές λεπτομέρειες της κάθε φάσης. Οι πειραματικές μέθοδοι είχαν ως στόχο να μελετήσουν τη συμπεριφορά των έξυπνων προσωπικών βοηθών όταν δέχονται σαν είσοδο διάφορα ερωτήματα από τον χρήστη. Περιγράφονται οι πιο τεχνικές λεπτομέρειες του πειράματος και πως αυτά τα δεδομένα χρησιμοποιήθηκαν για περεταίρω ανάλυση. Επιπρόσθετα παρουσιάζεται μια σύντομη ανάλυση στα δεδομένα που συλλέχθηκαν και πιθανούς κινδύνους που μπορεί να επιφέρουν. Τέλος δίνεται μια επεξήγηση στους αλγόριθμους Supervised Learning Classifiers που χρησιμοποιήθηκαν κατά τη πειραματική διαδικασία.

4.1 Επισκόπηση και Περιγραφή

Κατά τη διάρκεια της πειραματικής διαδικασίας χρησιμοποιήθηκε το Google Home Nest Mini 2nd generation (GHNM). Για την εγκατάσταση του GHNM ακολουθήθηκε τη τυπική διαδικασία που απαιτεί η συσκευή, συμπεριλαμβανομένου του ότι έγινε αποδοχή, στους Όρους και Προϋποθέσεις (Terms and Conditions) της Google αλλά και επιπρόσθετα η πρόσβαση στα δεδομένα τοποθεσίας, άλλα προγράμματα (Spotify), περιηγητές (browsers), σε άλλες συσκευές και σε προσωπικά αποτελέσματα (personal results) όπως ημερολόγιο, ηλεκτρονικό ταχυδρομείο, επαφές και πληρωμές. Δεν δόθηκε πρόσβαση της Google, στο να κρατά τις δραστηριότητες/εντολές του χρήστη σε περιηγητές και προγράμματα (web and app activity), και σε εξατομικευμένες διαφημίσεις. Οι υπόλοιπες ρυθμίσεις ακολουθήθηκαν όπως ήταν προκαθορισμένες από τη συσκευή.

4.2 Διασύνδεση Δικτύου

Η διασύνδεση του GHNM για την πειραματική διαδικασία έγινε ακριβώς όπως θα γινόταν από ένα μέσο χρήστη που θα ήθελε να χρησιμοποιήσεις ένα ΕΨΒ στο σπίτι του. Το τοπικό δίκτυο (LAN – Local Area Network) αποτελείται από ένα δρομολογητή (router) που λειτουργεί σαν πύλη (gateway) παρέχοντας σύνδεση στο διαδίκτυο. Για την παρακολούθηση όλων των πακέτων που στάλθηκαν μέσω του δικτύου καθ' όλη τη διάρκεια των πειραμάτων, έγινε σύνδεση του Η/Υ με τον δρομολογητή μέσω ενός σύρματος 'ethernet' και το GHNM ήταν συνδεδεμένο στο διαδίκτυο μέσω του Wi-fi σήματος που έκπεμπε ο δρομολογητής. Για να περιορίσω τη κίνηση του δικτύου κατά την διάρκεια των πειραμάτων καμία άλλη συσκευή δεν ήταν συνδεδεμένη στο τοπικό δίκτυο.

Ο Η/Υ ήταν εξοπλισμένος με το 'Wireshark', ένα εργαλείο ανοικτού κώδικα (open-source) που συλλέγει και αναλύει τα πακέτα που μεταδίδονται μέσα στο δίκτυο. Χρησιμοποιείται συνήθως για την αντιμετώπιση προβλημάτων δικτύου, εκπαίδευση, ανάλυση δεδομένων και για ανάπτυξη πρωτοκόλλων λογισμικού και επικοινωνιών. Επιπρόσθετα στις ρυθμίσεις του εργαλείου επιλέχθηκε όπως ήταν προεπιλεγμένο το "promiscuous mode" για να λαμβάνει και να χρησιμοποιεί όλα τα πακέτα, αφού η λειτουργία αυτή επιτρέπει τη λήψη όλων των εισερχόμενων και εξερχόμενων πακέτων ακόμα και αν η προέλευση τους ή ο προορισμός τους είναι διαφορετικά από τη διεύθυνση του Σημείου Πρόσβασης (Access Point).

4.3 Πειραματική εκτέλεση εντολών

Για τη συλλογή των πληροφοριών το πείραμα έλαβε δράση σε περίοδο 15 ημερών όπου συλλέγονταν τα δεδομένα σε διαφορετικές ώρες τη κάθε ημέρα. Οι εντολές δίνονταν μέσα από ηχογραφημένες φωνητικές εντολές και η ίδιες ηχογραφήσεις χρησιμοποιούνταν ξανά όταν επαναλαμβάνονταν τα ερωτήματα.

Κατά τη πειραματική διαδικασία επιλέχθηκαν μερικές εντολές από αυτές που προτείνει η Google μέσα από τη επίσημη σελίδα τους για τις δυνατότητες που έχει το GHNM. Οι εντολές που μπορεί ένας χρήστης να δώσει στο GHNM χωρίζονται σε διάφορες κατηγορίες και υποκατηγορίες. Για την πειραματική διαδικασία επιλέχθηκε σημαντικός αριθμός εντολών (30) οι οποίες παρουσιάζονται πιο κάτω σε πίνακα καθώς και σε ποια κατηγορία ανήκουν [Πίνακας 2].

Τα περισσότερα ερωτήματα που γίνονται στη πειραματική διαδικασία περιλαμβάνουν ερωτήσεις και ζητούν πληροφορίες που είναι πιθανές να ρωτηθούν στη καθημερινότητα ενός μέσου χρήστη. Κάποια άλλα ερωτήματα απαιτούν πιο ευαίσθητες πληροφορίες όπως τοποθεσία και σύνδεση με προσωπικούς λογαριασμούς (όπως Spotify). Η πληροφορίες αυτές δίνονται στο GHNM μέσω της εφαρμογής στο κινητό τηλέφωνο του χρήστη.

Κατηγορία	**Υπο-Κατηγορία**	**Εντολή**
Watch or listen to media	***Music***	Hey Google, play music on Spotify.
		Hey Google, play music from Youtube.
		Hey Google, stop music.
	News	Hey Google What's the latest news in technology?
		Hey Google, What's the latest in economy?
		Hey Google, What's the latest in sports?
Plan your day	***Traffic***	Hey Google, How long will take to drive to work?
		Hey Google, How long will take to go to work by bike?
		Hey Google, How is the traffic like?
	Weather	Hey Google, What is the weather like?
		Hey Google, Is it going to rain tomorrow?
		Hey Google, What's the weather forecast for next week?
	Calendar	Hey Google, Add an alarm for 10am tomorrow.
		Hey Google, What's my alarms for tomorrow?
		Hey Google, Cancel all my alarms for tomorrow.
Get answers	***Facts and info***	Hey Google, How tall is Barrack Obama?
		How far is the sun?
		Hey Google, What's the smallest country in Europe?
	Calculations	Hey Google, What's the 5th root of 97?
		Hey Google, What is 15% of 92?
		Hey Google, What is 10 times 24?
		Hey Google, What's "good morning" in French?

	Translation	Hey Google, How do you say "hello" in Greek?
		Hey Google, What's "good night" in Chinese?
	Currency and Unit conversion	Hey Google, How many euros is a dollar?
		Hey Google, 2 gallons are how many litres?
		Hey Google, What is 5 inches in meters?
	Sports	Hey Google, What are the Premiere League standings?
		Hey Google, When is Liverpool playing?
		Hey Google, Who is the best tennis player in the world?

Πίνακας 2: Εντολές

4.4 Συλλογή πληροφοριών

Μέσω του εργαλείου 'Wireshark' το οποίο περιλαμβάνει όλες τις πληροφορίες για τη κίνηση του δικτύου που στάλθηκε και λήφθηκε κατά τη διάρκεια των διαδικασιών. Κάθε μέρα πριν την εκτέλεση εντολών γινόταν η διενέργεια ενός ελέγχου ταχύτητας του δικτύου (speed-test) για το λόγο ότι η ταχύτητα του δικτύου μπορεί να επηρεάσει/καθυστερήσει τη κίνηση του δικτύου και κατ' επέκταση τις πληροφορίες που απαιτούνται από το GHNM. Οι παράμετροι που συλλέγονται και εξετάζονται κατά τη διάρκεια του πειράματος είναι:

I. Ταχύτητα δικτύου
II. Διεύθυνση (IP address) του αποστολέα και του παραλήπτη (source and destination)
III. Μέγεθος πακέτου δικτύου
IV. Πρωτόκολλο που χρησιμοποιείται
V. Πεδία πρωτοκόλλου
VI. Τοπική ώρα

Για την αυτοματοποίηση της διαδικασίας χρησιμοποιήθηκε 'script' το οποίο δέχεται σαν είσοδο τα .pcap αρχεία που συλλέχθηκαν από το Wireshark (σε 'promiscuous mode'), και εξάγει τις πιο πάνω πληροφορίες ορίζοντας το αρχείο όπου θα γίνει η καταγραφή των δεδομένων που . Οι ηχογραφημένες εντολές βρίσκονται όλες σε μια μόνο ηχογράφηση όπου δίνονται οι εντολές σειριακά και ταυτόχρονα γίνεται και η συλλογή των πακέτων.

4.5 Ανάλυση δεδομένων

Η ανάλυση έχει σκοπό τη μελέτη και επεξεργασία των μη-επεξεργασμένων δεδομένων που μεταφέρονται μέσα στο δίκτυο και συλλέγονται από το Wireshark, τα οποία συλλέχθηκαν κατά τη πειραματική διαδικασία. Για την ταξινόμηση των δεδομένων χρησιμοποιείται μια επισκόπηση μεθόδων και αλγορίθμων εκμάθησης μηχανής (Machine Learning) που μελετήθηκαν και δοκιμάστηκαν για την ταξινόμηση των δεδομένων.

4.5.1 Κίνηση και Πρωτόκολλα δικτύου

Στη φάση συλλογής δεδομένων συλλέχθηκαν αρχεία από το Wireshark για μια περίοδο 15 ημερών. Κάθε αρχείο συμπεριλαμβάνει όλα τα δεδομένα που χρησιμοποιούνται και εξάγονται από τη πειραματική διαδικασία. Μια σύντομη στατιστική ανάλυση φαίνεται πιο κάτω σε ένα από τα καταγεγραμμένα αρχεία, όπου φαίνονται κάποια στατιστικά για τα πακέτα και τα πρωτόκολλα σε μία πειραματική διαδικασία. Πανομοιότυπες τάσεις παρατηρούνται και στα υπόλοιπα αρχεία της συλλογής.

Αρχικά, όπως φαίνεται πιο κάτω εμφανίζονται τα ποσοστά των πακέτων βασισμένα σε IPv6 πρωτόκολλα και IPv4 (Εικόνα 3). Υπάρχει ένας πολύ μικρός αριθμός πακέτων με IPv6 διευθύνσεις για αυτό το λόγο θα δοθεί έμφαση στα πακέτα αυτά παρά μόνο στις IPv4 διευθύνσεις. Σε μερικές μετρήσεις η πλειοψηφία των πακέτων φαίνεται να είναι UDP πακέτα, κάτι που δεν ισχύει για όλα τα αρχεία. Στη περίπτωση που φαίνεται πιο κάτω υπάρχουν περίπου ίσος αριθμός TCP και UDP πακέτων. Υπάρχει επίσης ένας μικρός αριθμός πακέτων που δεν είναι TCP ούτε UDP και αυτά είναι συνήθως πακέτα ICMP και IGMP που χρησιμοποιούνται σαν βοηθητικά για τη διαχείριση του δικτύου. Τα δεδομένα που πραγματικά μεταφέρονται (χωρίς τα headers) μέσα από τα πακέτα TCP (δηλαδή το payload) είναι κρυπτογραφημένα. Ως εκ τούτου κάποια στατιστικά μπορούν να φανούν χρήσιμα κατά την ανάλυση και ταξινόμηση των δεδομένων που έχουν συλλεχθεί.

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IP Protocol Types	702				0.0031	100%	0.2800	82.290
UDP	345				0.0015	49.15%	0.1700	42.655
TCP	349				0.0015	49.72%	0.2800	82.290
NONE	8				0.0000	1.14%	0.0100	35.238

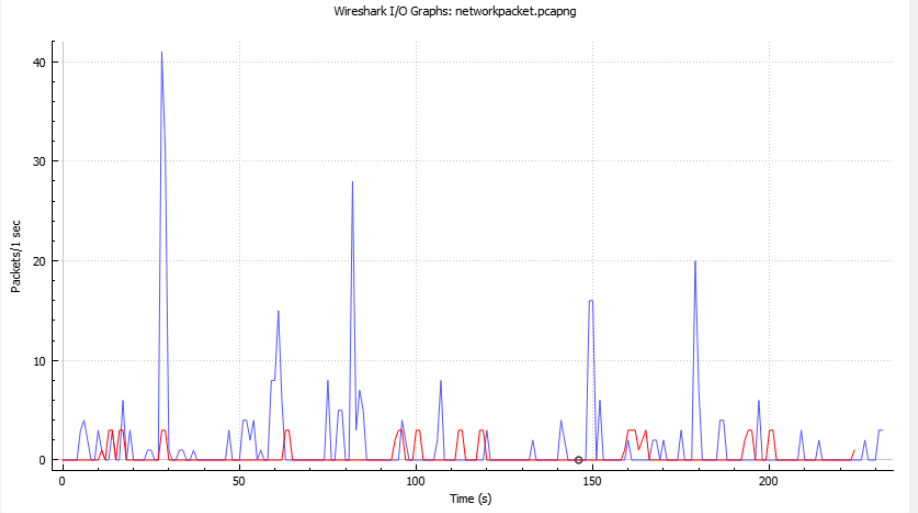
Εικόνα 3: IPv4 Protocols

Σε συνέχεια της ανάλυσης της κίνησης του δικτύου και της εξαγωγής στατιστικών, παρατηρήθηκε η έντονη παρουσία του πρωτοκόλλου MDNS στα πακέτα που στέλνονταν μέσα στο δίκτυο. Μια πιο λεπτομερής εικόνα της χρήσης των πρωτοκόλλων φαίνεται πιο κάτω [Εικόνα 4]. Το MDNS πρωτόκολλο θα αναλυθεί περισσότερο στην επόμενη υπό-ενότητα εφόσον περιέχει πληροφορίες οι οποίες μπορεί να φανούν πολύ χρήσιμες κατά την ανάλυση και να προξενήσουν διάφορους κινδύνους.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	833	100.0	220552	7560	0	0	0
Ethernet	100.0	833	5.3	11662	399	0	0	0
Logical-Link Control	14.5	121	2.7	6034	206	0	0	0
Spanning Tree Protocol	14.0	117	1.9	4095	140	117	4095	140
Cisco Discovery Protocol	0.5	4	0.7	1556	53	4	1556	53
Internet Protocol Version 6	1.2	10	0.2	400	13	0	0	0
User Datagram Protocol	1.2	10	0.0	80	2	0	0	0
DHCPv6	1.2	10	0.4	872	29	10	872	29
Internet Protocol Version 4	84.3	702	6.4	14072	482	0	0	0
User Datagram Protocol	41.4	345	1.3	2760	94	0	0	0
Simple Service Discovery Protocol	29.2	243	35.1	77305	2650	243	77305	2650
Multicast Domain Name System	9.8	82	14.8	32729	1121	82	32729	1121
Domain Name System	1.0	8	0.4	802	27	8	802	27
Data	1.4	12	0.2	404	13	12	404	13
Transmission Control Protocol	41.9	349	32.6	71956	2466	271	50587	1734
Transport Layer Security	9.5	79	29.4	64831	2222	78	64526	2212
Internet Group Management Protocol	1.0	8	0.0	64	2	8	64	2

Εικόνα 4: Protocol Hierarchy

Γραφικά, τα παραπάνω στατιστικά στοιχεία μπορούν να παρατηρηθούν πιο κάτω [Εικόνα 5]. Στο γράφημα, τα πακέτα ανά δευτερόλεπτο φαίνονται σε αναλογία με το χρόνο που έχει περάσει από τη στιγμή παραλαβής του πακέτου. Τα πακέτα TCP εμφανίζονται με κόκκινο και τα πακέτα MDNS με μπλε και καλύπτουν το μεγαλύτερο μέρος του γραφήματος. Οι άκρες του γραφήματος υποδεικνύουν το χρονοδιάγραμμα των εντολών και των ανταποκρίσεων.



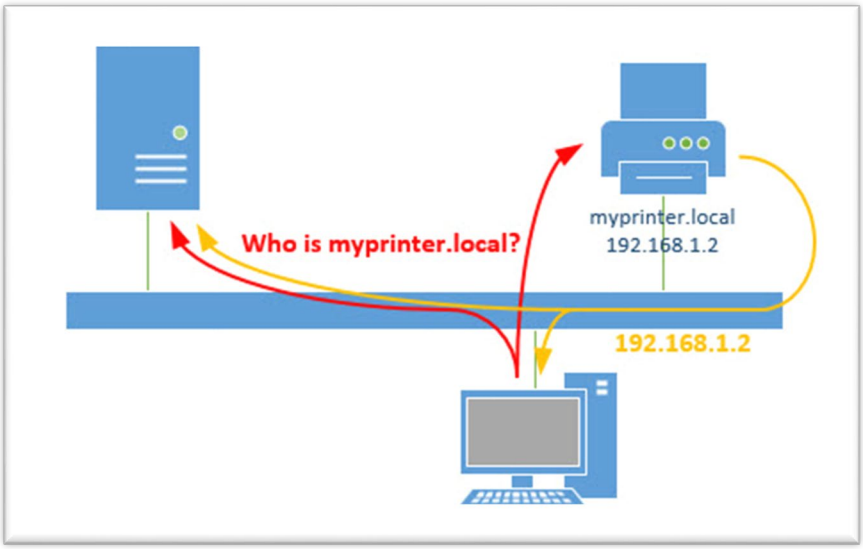
Εικόνα 5

4.5.2 MDNS πρωτόκολλο

Σε αυτό το κεφάλαιο, θα δοθεί περισσότερη έμφαση στο πρωτόκολλο MDNS και σε γνωστές απειλές και επιθέσεις που μπορούν να διεκπεραιωθούν μέσω του πρωτοκόλλου αυτού.

Το πρωτόκολλο MDNS (Multicast DNS) μεταφράζει ονόματα κεντρικών υπολογιστών σε διευθύνσεις IP εντός μικρών δικτύων που δεν περιλαμβάνουν τοπικό διακομιστή ονομάτων. Είναι μια υπηρεσία μηδενικής διαμόρφωσης δικτύων (Zero-configuration networking, Zeroconf) και χρησιμοποιεί τις ίδιες διεπαφές προγραμματισμού, μορφές πακέτων και τρόπο λειτουργίας με την υπηρεσία DNS (Domain Name Service). Σχεδιάστηκε για να λειτουργεί είτε ως αυτόνομο πρωτόκολλο είτε ως συμβατό με τυπικούς διακομιστές DNS. Παρομοίως με το MDNS, άλλα πρωτόκολλα που χρησιμοποιούνται σε Zeroconf δίκτυα είναι το DNS-SD (DNS Service Discovery), SLP (Service Location Protocol), LLMNR (Link-Local Multicast Name Resolution) και SSDP (Simple Service Discovery Protocol). Όλα τα παραπάνω πρωτόκολλα επιτρέπουν τη διαφήμιση και την ανακάλυψη υπηρεσιών δικτύου χωρίς την ανάγκη πρόσθετης διαμορφωμένης υποδομής δικτύου.

Το πρωτόκολλο MDNS περιορίζει επίσης την ανάγκη για DNS διακομιστή (server) στις περιπτώσεις όπου τα ονόματα της συσκευής χρειάζεται να μεταφραστούν σε ηλεκτρονικές διευθύνσεις (IP) εντός δικτύου. Η αναζήτηση δεδομένων σχετικά με το DNS απαιτεί ένα διαμορφωμένο server όπου οι έξυπνες συσκευές δημιουργούν ένα DNS ερώτημα (query). Το MDNS, όπως και το DNS, είναι ένα UDP (User Datagram Protocol) πρωτόκολλο που χρησιμοποιεί τη πόρτα (port) 5353 (DNS το port 53) και χρησιμοποιεί πολλαπλές εκπομπές πακέτων για να μεταφράσει τοπικά ονόματα υπολογιστών σε IP εντός του τοπικού δικτύου. Το MDNS χρησιμοποιεί τα ονόματα υπολογιστή με τοπικό σύνδεσμο όπου οποιοσδήποτε υπολογιστής εντός δικτύου να μπορεί να χρησιμοποιήσει και να διαφημίσει το τοπικό του όνομα με την επέκταση ".local. Για παράδειγμα όταν μια συσκευή χρειάζεται να μεταφράσει ένα όνομα σε IP, μπορεί να στείλει ένα query MDNS μέσα στο δίκτυο χρησιμοποιώντας μια διεύθυνση multicast. Η συσκευή που περιέχει το όνομα που ζητήθηκε μπορεί να απαντήσει χρησιμοποιώντας μια ανταπόκριση MDNS εγγραφής πόρων(Resource Record). Στις περιπτώσεις των Ethernet πλαισίων (frames) τα queries και τα Resource Records αποστέλλονται στην διεύθυνση MAC (Media Access Control) και για το IPv4 χρησιμοποιείται η διεύθυνση 224.0.0.251. Ένα απλό παράδειγμα φαίνεται πιο κάτω [Εικόνα 6] όπου με κόκκινες γραμμές είναι το ερώτημα (request) και με κίτρινες γραμμές οι απαντήσεις (response).



Εικόνα 6 (luca, 2017) - MDNS .local 1

4.5.3 Απειλές και κίνδυνοι MDNS πρωτοκόλλου

Υπάρχουν πολλές αναφορές και ανησυχίες σχετικά με την ασφάλεια του πρωτοκόλλου MDNS και τους πιθανούς κινδύνους σχετικά με την ιδιωτικότητα του χρήστη. Αρχικά ότι το Zeroconf προϋποθέτει ότι όλοι οι χρήστες που βρίσκονται στο τοπικό δίκτυο είναι αξιόπιστοι. Οι περισσότεροι υπολογιστές, εκτυπωτές και οι έξυπνες συσκευές υποστηρίζουν πρωτόκολλα Zeroconf από προεπιλογή και τα χρησιμοποιούν για να διαφημίσουν τη διεύθυνση τους και τις διαθέσιμες υπηρεσίες που παρέχουν. Ως εκ τούτου, σε περίπτωση που μια συσκευή που χρησιμοποιείται σε δημόσιο, μη ασφαλές ή παραβιασμένο δίκτυο τότε μπορούν να υποκλαπούν πολλές πληροφορίες.

Το πρωτόκολλο MDNS είναι ανοιχτό σε κατάχρηση από εξωτερικά συστήματα. Μπορεί να χρησιμοποιηθεί ως ενισχυτής κυκλοφορίας σε μια κατανεμημένη επίθεση άρνησης υπηρεσίας εναντίον διακομιστών NeCTAR ή τρίτων διακομιστών DNS. Οι εισβολείς στέλνουν ένα αίτημα σε μια υπηρεσία mDNS η οποία τους αναμεταδίδει στον στόχο επίθεσης. Μια τέτοια επίθεση μπορεί επίσης να καταναλώσει σημαντικό εύρος ζώνης δικτύου και είναι πιθανό να οδηγήσει σε μαύρη λίστα δικτύου (blacklisting). Η υπηρεσία mDNS μπορεί επίσης να χρησιμοποιηθεί για τη συλλογή πληροφοριών σχετικά με τα συστήματά σας που θα μπορούσαν να χρησιμοποιηθούν για να βοηθήσουν τους χάκερ να αποκτήσουν πρόσβαση σε αυτά (Crawley, 2017).

Επιπρόσθετα μια ευπάθεια στη δυνατότητα πύλης mDNS του λογισμικού σημείων πρόσβασης της σειράς Cisco Aironet θα μπορούσε να επιτρέψει σε έναν μη επαληθευμένο, παρακείμενο εισβολέα να προκαλέσει μια συνθήκη άρνησης υπηρεσίας (DoS) σε μια επηρεαζόμενη συσκευή. Αυτή η ευπάθεια οφείλεται στην ανεπαρκή επικύρωση εισόδου της εισερχόμενης κίνησης mDNS. Ένας εισβολέας θα μπορούσε να εκμεταλλευτεί αυτήν την ευπάθεια στέλνοντας ένα δημιουργημένο πακέτο mDNS σε μια επηρεαζόμενη συσκευή μέσω ενός ασύρματου δικτύου που έχει ρυθμιστεί σε λειτουργία τοπικής μεταγωγής FlexConnect ή μέσω ενός ενσύρματου δικτύου σε ένα διαμορφωμένο mDNS VLAN. Μια επιτυχημένη εκμετάλλευση θα μπορούσε να επιτρέψει στον εισβολέα να προκαλέσει επανεκκίνηση του σημείου πρόσβασης, με αποτέλεσμα να δημιουργηθεί μια συνθήκη DoS.

Μελετώντας και αναλύοντας τα πακέτα δικτύου που έχουν συλλεχθεί μέσω της πειραματικής διαδικασίας, παρόλο που το μεγαλύτερο μέρος των δεδομένων που μεταφέρονται μέσω του δικτύου είναι κρυπτογραφημένο, μπορούν αν αντληθούν χρήσιμες πληροφορίες που σχετίζονται με το πρωτόκολλο MDNS. Το Google Home Nest Mini χρησιμοποιεί MDNS πρωτόκολλο για να χρησιμοποιήσει τις υπηρεσίες που παρέχει μέσα στο δίκτυο. Πιο κάτω φαίνεται ένα στιγμιότυπο οθόνης ενός UDP Stream μέσω του Wireshark. Όπως φαίνεται πιο κάτω μπορούν να αντληθούν χρήσιμα πεδία όπως ονόματα και υπηρεσίες που παρέχει.

Εικόνα 7: Παράδειγμα UDP Stream 1

Παρατηρώντας τα πακέτα φαίνεται ότι το Google Home Nest Mini λειτουργεί μέσα στο δίκτυο και το όνομα που έχει δοθεί από το χρήστη στη συσκευή είναι GHNM καθώς και το όνομα full house (το full house έχει δημιουργηθεί σαν group με την προοπτική ότι θα ενωθούν περισσότερες από μία έξυπνες συσκευές. Επιπρόσθετα παρατηρήθηκε πως όταν γίνονται ερωτήματα σχετικά με νέα (τεχνολογικά, επιχειρηματικά, αθλητικά, κλπ) κάποια από τα πεδία που δεν κρυπτογραφούνται μέσα στα πακέτα δικτύου φαίνονται πιο κάτω.

- rs=Spotify
- rs=Google News
- rs=Casting: CNBC Teck Check
- rs=Casting: Bloomberg First Word
- rs=Casting: BBC Sports News
- rs=Casting: ESPN Radio

"Ένας κακόβουλος χρήστης μπορεί πολύ εύκολα να παρακολουθήσει τα πακέτα που στέλνονται μέσα στο δίκτυο και να αποσπάσει αυτές τις πληροφορίες, με τη προϋπόθεση ότι έχει πρόσβαση στο ίδιο δίκτυο με το θύμα. Ώς εκ τούτου ο επιτιθέμενος μπορεί να συμπεράνει ότι το θύμα χρησιμοποιεί έξυπνη συσκευή, πότε τη χρησιμοποιεί, ποια είναι τα ενδιαφέροντα του θύματος, το όνομα της συσκευής και σε ποια τοποθεσία βρίσκεται μέσα στο σπίτι. Αυτές οι πληροφορίες είναι πολύ χρήσιμες για ένα κακόβουλο χρήστη έτσι ώστε να μπορεί να αναλύσει τις κινήσεις του θύματος για να μπορέσει να προβεί σε περαιτέρω επιθέσεις όπως social-engineering και phishing attacks.

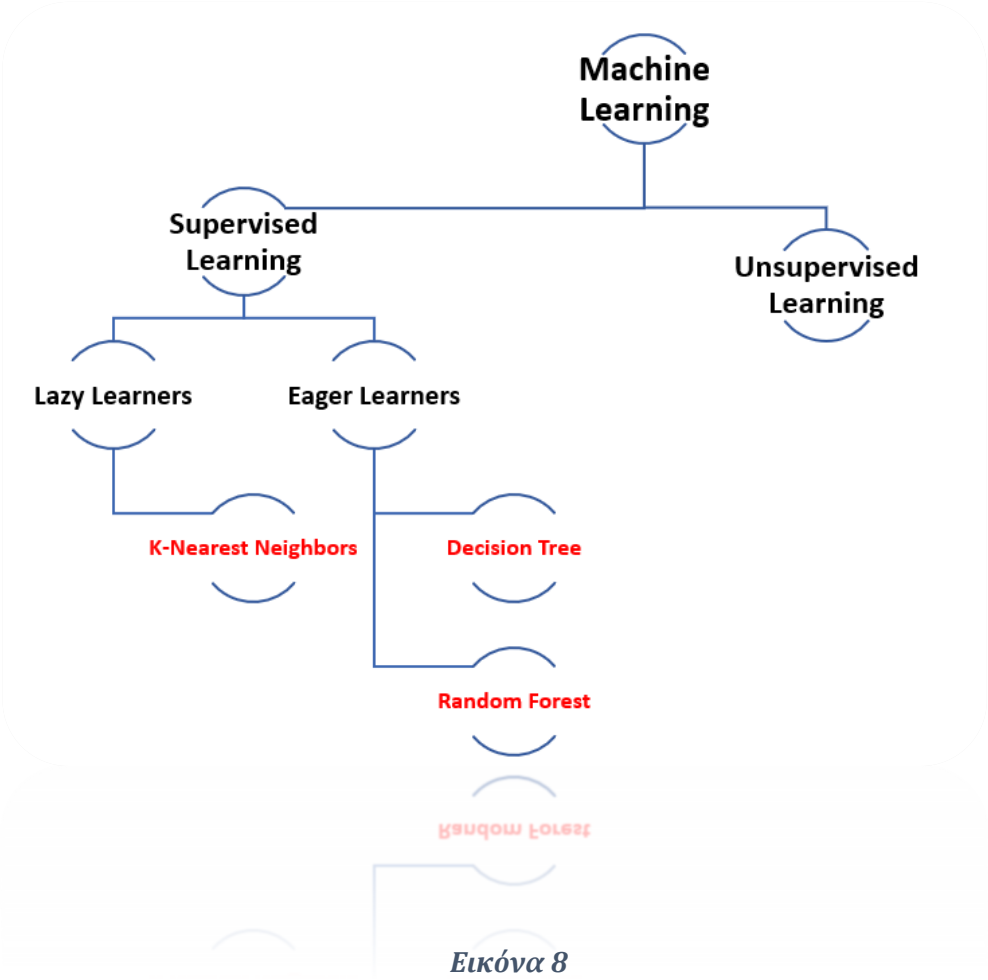
Σε συνέχεια των πιο πάνω, ενώ το πρωτόκολλο MDNS χρησιμοποιείται συνήθως σε ένα τοπικό δίκτυο, θεωρητικά δεν επιτρέπεται για ένα μηχάνημα εκτός δικτύου να κάνει ένα ερώτημα MDNS unicast. Παρόλα αυτά υπάρχουν συσκευές που ανταποκρίνονται από προεπιλογή σε ένα ερώτημα unicast το οποίο προέρχεται εκτός του τοπικού δικτύου. Αυτή η ευπάθεια δημοσιεύτηκε επίσημα και αποκαλύφθηκε από έναν ερευνητή ασφαλείας σε συνεργασία με το CERT (Wassermann, 2015). Ο ερευνητής χρησιμοποιώντας εργαλεία ανοιχτού κώδικα έδειξε πώς ευάλωτες συσκευές απαντούσαν σε ερωτήματα MDNS μέσω του διαδικτύου και ότι ευαίσθητες πληροφορίες (όπως MAC address, ονόματα υπολογιστών, σειριακό αριθμό συσκευών, μοντέλο συσκευών και πληροφορίες διαχείρισης) που διέρρεαν από τις συσκευές αυτές. Τέλος, αυτή η ευπάθεια θα μπορούσε να χρησιμοποιηθεί σε μια επίθεση ενίσχυσης DDoS.

4.5.4 Ταξινόμηση εποπτευομένης εκμάθησης (Supervised Learning Classifiers)

Τα δεδομένα που συλλέχθηκαν κατά τη φάση του πειράματος χρησιμοποιήθηκαν στη διαδικασία ταξινόμησης δεδομένων χρησιμοποιώντας τεχνικές και αλγόριθμους μηχανικής εκμάθησης (Machine Learning). Σε αυτή την ενότητα, δίνεται μια επισκόπηση των διαθέσιμων κατηγοριών και μεθόδων που παρέχει η μηχανική εκμάθηση και στη συνέχεια αναλύονται και επεξηγούνται περαιτέρω οι Αλγόριθμοι και οι Μέθοδοι που χρησιμοποιήθηκαν για αυτήν την έρευνα.

4.5.4.1 Ανασκόπηση ταξινόμησης

Η Μηχανική Εκμάθηση αποτελεί ένα υποσύνολο της Τεχνητής Νοημοσύνης και της Επιστήμης Δεδομένων (Data Science), η οποία αυξάνει τις τεχνικές και τις στατιστικές μεθόδους για καλύτερη πρόβλεψη ενός αποτελέσματος. Η μηχανική εκμάθηση χωρίζεται αρχικά σε δύο κατηγορίες, την ελεγχόμενη εκμάθηση (Supervised Learning) και τη μη-ελεγχόμενη εκμάθηση (Unsupervised Learning). Οι αλγόριθμοι που ανήκουν στην πρώτη κατηγορία χρησιμοποιούν μια προσέγγιση η οποία ορίζεται από τη χρήση επισημασμένων (labeled) συνόλων δεδομένων για την εκπαίδευση των δεδομένων. Σε αυτή τη περίπτωση ο αλγόριθμος θα εκπαιδευτεί από δεδομένα που θα του δώσει ο χρήστης τα οποία αντιστοιχούν με συγκεκριμένα δεδομένα εξόδου. Αντίθετα οι αλγόριθμοι που ανήκουν στο Unsupervised Learning δεν χρειάζονται επισημασμένα δεδομένα που να αντιστοιχούν σε συγκεκριμένες εξόδους, αλλά εξετάζουν λεπτομερώς τα δεδομένα για να ανακαλύψουν μοτίβα για να ομαδοποιήσουν τα δεδομένα. Σε αυτή τη περίπτωση δεν υπάρχει εκπαίδευση του αλγορίθμου αλλά ο αλγόριθμος είναι υπεύθυνος να αναλύσει τη δομή των δεδομένων.
Για τους σκοπούς της έρευνας αυτής, χρησιμοποιήθηκαν αλγόριθμοι ταξινόμησης Supervised Learning, για τον λόγω ότι συλλέχθηκαν και χρησιμοποιήθηκαν επισημασμένα δεδομένα για την εκπαίδευση των αλγορίθμων. Εκτός από τις μεθόδους ταξινόμησης, υπάρχουν διαφορετικές μεθόδοι που μπορούν να χρησιμοποιηθούν, τόσο για το Supervised όσο και για το Unsupervised Learning. Τέτοιες μέθοδοι περιλαμβάνουν, την ομαδοποίηση (Clustering), τις μεθόδους συνόλου (Ensemble Methods), τα νευρωνικά δίκτυα (Neural Networks) και τη βαθιά μάθηση (Deep Learning), τη μεταβιβαστική μάθηση (Transfer Learning), την ενισχυτική μάθηση (Reinforcement Learning) και άλλα. Δεδομένου ότι ο στόχος αυτή την έρευνα είναι η Ταξινόμηση, θα εξεταστούν μόνο οι μέθοδοι και οι αλγόριθμοι ταξινόμησης. Διάγραμμα των αλγορίθμων που έχουν χρησιμοποιηθεί φαίνεται παρακάτω [Εικόνα 8].



Εικόνα 8

4.5.4.2 Αλγόριθμοι και μέθοδοι που χρησιμοποιήθηκαν

Για την ταξινόμηση χρησιμοποιήθηκαν δύο μέθοδοι γνωστοί ως Lazy Learners και Eager Learners. Τα δεδομένα χωρίστηκαν σε δεδομένα εκπαίδευσης (training data) και δοκιμαστικά δεδομένα (test data) σε όλους του αλγόριθμους που έχουν χρησιμοποιηθεί. Η κύρια διαφορά των δύο αλγορίθμων είναι στον τρόπο που χρησιμοποιούν τα δεδομένα εκπαίδευσης τα οποία στη συνέχεια χρησιμοποιούνται για να ταξινομηθούν τα δεδομένα δοκιμής.

Οι εν λόγω αλγόριθμοι, κατά τη φάση της εκπαίδευσης δεδομένων αποθηκεύουν απλώς τα δεδομένα μαζί με τις ετικέτες τους χωρίς περαιτέρω επεξεργασία των δεδομένων. Όταν φτάνουν τα δεδομένα της δοκιμής, οι Lazy Learners ταξινομούν τα δεδομένα με αυτά που

είναι πιο σχετικά αφού πρώτα τα έχουν συγκρίνει με τα δεδομένα εκπαίδευσης. Αντίθετα, οι αλγόριθμοι Eager Learners όταν λαμβάνουν τα δεδομένα εκπαίδευσης ξεκινούν επίσης τη διαδικασία ταξινόμησης δημιουργώντας ένα μοντέλο που να βασίζεται στα δεδομένα. Όταν λαμβάνουν τα δεδομένα δοκιμής, οι Eager Learners κάνουν την ταξινόμηση στο μοντέλο που έχει ήδη κατασκευαστεί κατά τη φάση της εκπαίδευσης.

Σύμφωνα με τον τρόπο που λειτουργούν και αλληλοεπιδρούν με τα δεδομένα οι δύο αυτοί αλγόριθμοι μέθοδοι έχουν μερικά πλεονεκτήματα και μειονεκτήματα. Εφόσον οι Lazy Learners δεν διεξάγουν κάποια επεξεργασία στα δεδομένα εκπαίδευσης, συνήθως είναι πολύ γρηγορότεροι στη φάση της εκπαίδευσης αλλά χρειάζονται περισσότερα δεδομένα (επομένως περισσότερο αποθηκευτικό χώρο) και περισσότερο χρόνο στη φάση ταξινόμησης των δεδομένων. Οι Eager Learners χρειάζονται περισσότερο χρόνο και λιγότερο αποθηκευτικό χώρο στη φάση επεξεργασίας των δεδομένων εκπαίδευσης του αλγορίθμου, αλλά είναι επίσης γρηγορότεροι κατά τη φάση ταξινόμησης των δεδομένων. Επιπρόσθετα, εάν υπάρχουν μη-σχετικές πληροφορίες κατά τη φάση της εκπαίδευσης του αλγορίθμου, οι Lazy Learners θα εκπαιδεύσουν το σύστημα συμπεριλαμβανομένων των αχρείαστων πληροφοριών, αφού δεν γίνεται καμία επεξεργασία των δεδομένων. Σε μια τέτοια περίπτωση οι Eager Learners είναι πολύ πιο αποδοτικοί με πιο ακριβή αποτελέσματα.

Για την εξαγωγή των αποτελεσμάτων έχουν χρησιμοποιηθεί τρεις αλγόριθμοι. Ο K-Nearest Neighbors (KNN) που αποτελεί έναν από τους πιο γνωστούς Lazy Learners αλγόριθμους, και οι Decision Tree και Random Forest που είναι Eager Learners αλγόριθμοι. Ο αλγόριθμος KNN όταν λαμβάνει τα δεδομένα εκπαίδευση τα αποθηκεύει με βάση τα χαρακτηριστικά τους και τις ετικέτες τους σε ένα πολυδιάστατο χώρο. Κατά τη φάση της δοκιμής, ο αλγόριθμος συγκρίνει καθένα από τα δεδομένα δοκιμής με τα αποθηκευμένα δεδομένα και προσπαθεί να βρει το πλησιέστερο «γείτονα». Η σύγκριση γίνεται με βάση την απόσταση (π.χ. Ευκλείδεια απόσταση) των δεδομένων δοκιμής από τα ήδη ταξινομημένα δεδομένα που έχουν αποθηκευτεί. Η παράμετρος k μπορεί να οριστεί από τον χρήστη και ορίζει τον αριθμό των «γειτόνων» που θα συγκρίνει ο αλγόριθμος με κάθε ένα από τα νέα δεδομένα δοκιμής.

Ο αλγόριθμος Decision Tree δημιουργεί ένα μοντέλο δέντρου για την αναπαράσταση και την ταξινόμηση των δεδομένων. Κάθε κόμβος του δέντρου χρησιμεύει ως χαρακτηριστικό

των δεδομένων και οι συνδέσεις το δέντρου είναι κανόνες που καθορίζουν μια απόφαση. Στην απλούστερη μορφή του, ο αλγόριθμος δημιουργεί ένα δέντρο που βασίζεται σε μια σειρά από δηλώσεις "if-else" που χωρίζουν το σύνολο δεδομένων σε υποσύνολα και κάθε φύλλο επισημαίνεται με μια κλάση. Ο αλγόριθμος ταξινομεί τα δεδομένα δοκιμής με βάση το μοντέλο δέντρου που έχει δημιουργηθεί, εφαρμόζοντας τους κανόνες για κάθε κόμβο και άκρη του δέντρου. Όταν τα δεδομένα δοκιμής φτάνουν σε ένα φύλλο, υποδηλώνει ότι τα δεδομένα έχουν ταξινομηθεί και επισημαίνονται από μια συγκεκριμένη κλάση ή μια κατανομή πιθανότητας αυτής της κλάσης.

Ο αλγόριθμος Random Forest χρησιμοποιεί τις βασικές αρχές ενός αλγορίθμου Decision Tree αλλά συνδυάζει πολλά Decision Trees για να δημιουργήσει μια τελική ταξινόμηση-πρόβλεψη. Κάθε μεμονωμένο Δέντρο αποφάσεων εξάγει μια απόφαση σχετικά με την ταξινόμηση των δεδομένων και στη συνέχεια ο αλγόριθμος συνδυάζει όλες τις προβλέψεις και ταξινομεί τα δεδομένα με βάση την πλειοψηφία μιας προβλεπόμενης κλάσης. Αυτός ο συνδυασμός προβλέψεων δίνει ένα πιο συγκεκριμένο και ισχυρό μοντέλο που είναι σε θέση να απορρίψει μεμονωμένα λάθη ή εσφαλμένες προβλέψεις ενός μόνο Δέντρου Αποφάσεων.

5. Ταξινόμηση Αποτελεσμάτων

Σε αυτό το κεφάλαιο παρουσιάζονται τα αποτελέσματα της ταξινόμησης χρησιμοποιώντας τις μεθόδους και τους αλγόριθμους που έχουν προαναφερθεί. Αρχικά, δίνεται μια επισκόπηση του στόχου της ταξινόμησης και του στόχου επιθυμίας αυτής της ανάλυσης. Στη συνέχεια, επεξηγούνται τα διάφορα σενάρια, τα οποία πραγματοποιήθηκαν κατά τη φάση εκπαίδευσης και δοκιμής κάθε ταξινομητή. Επιπλέον, τα αποτελέσματα της ταξινόμησης αναλύονται και συγκρίνονται περαιτέρω. Τέλος, παρουσιάζονται ορισμένοι περιορισμοί και μειονεκτήματα των αποτελεσμάτων.

5.1 Ταξινόμηση

Κατά την περίοδο του πειράματος καταγράφηκαν και συλλέχθηκαν συνολικά 30 αρχεία δεδομένων χρησιμοποιώντας το Wireshark, όπως περιεγράφηκε στην Ενότητα 4. Όλα τα δεδομένα και τα πακέτα που συλλέχθηκαν περιλαμβάνουν χρήσιμες πληροφορίες που μπορούν να χρησιμοποιηθούν για την ταξινόμηση των δεδομένων. Ένα Dataframe δημιουργήθηκε με την επεξεργασία των μη-επεξεργασμένων δεδομένων προκειμένου να μπορεί να χρησιμοποιηθεί ως είσοδος για τους ταξινομητές. Συγκεκριμένα, το Dataframe έχει δημιουργηθεί με εξαγωγή των κατάλληλων πληροφοριών που θα χρησιμοποιηθούν για κάθε ένα από τα αρχεία Wireshark. Στη συνέχεια, τα αποτελέσματα της δοκιμής ταχύτητας του δικτύου (speed-test), που περιλαμβάνουν την ταχύτητα λήψης (download) και μεταφόρτωσης (upload) συλλέχθηκαν πριν από κάθε αρχείο, προστέθηκαν στο Dataframe. Πραγματοποιήθηκε κάποια πρόσθετη επεξεργασία των δεδομένων προκειμένου να

κατηγοριοποιηθούν τα δεδομένα με βάση τη μορφή που φαίνεται στο παρακάτω σχήμα [Εικόνα 9].

download_speed	file_date	file_name	length	question_no	time_end	time_start	upload_speed
87.17	07/11/2021 12:41	day1.csv	377	Q1	07/11/2021 12:41	07/11/2021 12:41	32.48
87.17	07/11/2021 12:41	day1.csv	313	Q2	07/11/2021 12:41	07/11/2021 12:41	32.48
87.17	07/11/2021 12:41	day1.csv	322	Q3	07/11/2021 12:41	07/11/2021 12:41	32.48
87.17	07/11/2021 12:41	day1.csv	385	Q4	07/11/2021 12:42	07/11/2021 12:41	32.48
87.17	07/11/2021 12:41	day1.csv	377	Q5	07/11/2021 12:42	07/11/2021 12:42	32.48

Εικόνα 9

Η διάρκεια κάθε ερώτησης θεωρείται ο χρόνος που ο χρήστης έχει αρχίσει να κάνει το ερώτημα, μέχρι την έναρξη του επόμενου ερωτήματος. Ως αποτέλεσμα, λαμβάνονται υπόψη τόσο το ερώτημα όσο και η απάντηση που έχει ληφθεί από το GHNM. Το μήκος είναι το άθροισμα του μήκους των πακέτων για κάθε πρωτόκολλο που καταγράφηκαν κατά τη διάρκεια κάθε ερώτησης.

Ο στόχος της ταξινόμησης είναι να εξετάσει και να αναλύσει την ικανότητα ενός ταξινομητή να προβλέπει σε ένα μεγάλο ποσοστό το ερώτημα που έχει γίνει όταν δίνεται ως είσοδος ορισμένη ποσότητα πληροφοριών. Είναι προφανές ότι εάν όλες οι παραπάνω πληροφορίες δίνονταν ως είσοδος, θα ήταν απλό για έναν ταξινομητή να συνδυάσει τις πληροφορίες και να προβλέψει τον αριθμό της ερώτησης και να επισημάνει σωστά τα δεδομένα. Επίσης, η ακρίβεια της πρόβλεψης θα ήταν επιφανειακή, καθώς ένας εισβολέας κανονικά δεν θα είχε τόσες πολλές λεπτομέρειες και πληροφορίες σχετικά με τα δεδομένα.

5.2 Εκπαίδευση ταξινομητών και δοκιμή σεναρίων

Όπως αναφέρθηκε πιο πάνω, η παροχή όλων των λεπτομερειών και πληροφοριών των δεδομένων σε έναν ταξινομητή θα ήταν ένα μη ρεαλιστικό σενάριο και αποτέλεσμα. Ως εκ τούτου, έχουν εξεταστεί διαφορετικά σενάρια όπου έχει δοθεί μια ορισμένη ποσότητα

πληροφοριών σχετικά με τα δεδομένα στους ταξινομητές κατά τη διάρκεια της εκπαίδευσης και της φάσης δοκιμής.

Για όλα τα σενάρια, πριν από την ταξινόμηση, τα δεδομένα έχουν χωριστεί έτσι ώστε το 70% των συνολικών δεδομένων να έχει χρησιμοποιηθεί για εκπαίδευση και το υπόλοιπο 30% των δεδομένων να έχει χρησιμοποιηθεί για τον έλεγχο και την πρόβλεψη. Ο διαχωρισμός των δεδομένων γίνεται τυχαία, επομένως χρησιμοποιούνται διαφορετικά δεδομένα κάθε φορά που πραγματοποιείται η ταξινόμηση. Επιπλέον, κάθε αλγόριθμος προσθέτει τυχαιότητα (π.χ. γεννήτρια τυχαίων αριθμών) στην επιλογή των δεδομένων που θα χρησιμοποιήσει για την εκπαίδευση και τη δοκιμή. Αυτό συνήθως παράγει ελαφρώς διαφορετικά αποτελέσματα στην ακρίβεια της πρόβλεψης κάθε φορά που πραγματοποιείται η δοκιμή και η πρόβλεψη. Για κάθε σενάριο ο έλεγχος έγινε πολλές φορές και τα αποτελέσματα και τα ποσοστά ακρίβειας που παρουσιάζονται είναι ο μέσος όρος των προβλέψεων που παράγονται κάθε φορά.

Αρχικά, ως είσοδος δόθηκε μόνο το άθροισμα του μήκους κάθε πρωτοκόλλου για κάθε ερώτηση και ο αλγόριθμος προσπάθησε να προβλέψει και να επισημάνει τον αριθμό ερώτησης κάθε αρχείου. Όλοι οι αλγόριθμοι έχουν δημιουργήσει παρόμοιες προβλέψεις με μέση ακρίβεια περίπου 12% για όλους τους αλγόριθμους. Δεδομένου ότι υπάρχουν 30 ερωτήσεις προς επισήμανση, η πρόβλεψη του αριθμού της ερώτησης τυχαία θα ήταν 1/30, περίπου 3,33%. Προσθέτοντας μόνο το μήκος ως παράμετρο, ένας εισβολέας θα μπορούσε να προβλέψει την ετικέτα κάθε ερώτησης περίπου τέσσερις φορές με μεγαλύτερη ακρίβεια [Πίνακας 3].

Δεδομένα εισαγωγής	Αλγόριθμος	Ακρίβεια
Length	Decision Tree	~13%
	K-Nearest Neighbors	~12%
	Random Forest	~12%

Πίνακας 3

Στη συνέχεια, ως δεδομένα εισόδου εκτός από το μήκος, δόθηκαν οι ταχύτητες λήψης και αποστολής. Προσθέτοντας πληροφορίες ως είσοδο στους αλγόριθμους θα μπορούσε κάποιος να περιμένει ότι οι αλγόριθμοι έχουν βελτιωμένη ακρίβεια στις προβλέψεις τους. Ωστόσο, χρησιμοποιώντας τις ταχύτητες λήψης και μεταφόρτωσης χωρίς περαιτέρω υπολογισμούς, η ακρίβεια των αλγορίθμων μειώνεται. Αυτό οφείλεται στο γεγονός ότι δεν υπάρχει άμεση συσχέτιση μεταξύ των ερωτήσεων και των ταχυτήτων λήψης και αποστολής. Ως αποτέλεσμα, όταν οι αλγόριθμοι χρησιμοποιούν τις ταχύτητες λήψης και μεταφόρτωσης ως δυνατότητα και προσπαθούν να κάνουν προβλέψεις χρησιμοποιώντας αυτήν την πρόσθετη δυνατότητα, η ακρίβειά τους μειώνεται. Η μείωση της ακρίβειας της πρόβλεψης είναι ακόμη πιο εμφανής στον αλγόριθμο Random Forest, καθώς ο αλγόριθμος κάνει μια βαθύτερη διεργασία όταν προσπαθεί να βρει μια συσχέτιση μεταξύ των χαρακτηριστικών και των ετικετών[Πίνακας 4].

Δεδομένα εισαγωγής	Αλγόριθμος	Ακρίβεια
Length Download Upload	Decision Tree	~12%
	K-Nearest Neighbors	~10%
	Random Forest	~5%

Πίνακας 4

Για το επόμενο σενάριο, η διάρκεια, η ώρα έναρξης και η ώρα λήξης κάθε ερώτησης δόθηκε ως είσοδος σε κάθε αλγόριθμο. Για κάθε ερώτηση, η ώρα έναρξης είναι η ώρα που ο χρήστης άρχισε να κάνει το ερώτημα και η ώρα λήξης είναι η ώρα έναρξης του επόμενου ερωτήματος. Σε αυτό το σενάριο, ο αλγόριθμος KNN ξεπέρασε τους αλγόριθμους Decision Tree και Random Forest και είχε περίπου 4,5 φορές καλύτερη απόδοση [Πίνακας 5].

Δεδομένα εισαγωγής	Αλγόριθμος	Ακρίβεια
Length Start time End Time	Decision Tree	~15%
	K-Nearest Neighbors	~63%
	Random Forest	~12%

Πίνακας 5

Θα μπορούσε να υποστηριχθεί ότι τα παραπάνω αποτελέσματα και η πολύ υψηλή ακρίβεια του αλγόριθμου KNN είναι πολύ ενθαρρυντικά ως και μη ρεαλιστικά, εφόσον θα ήταν πολύ δύσκολο για έναν εισβολέα να έχει τους χρόνους που ο χρήστης κάνει τα ερωτήματα. Ωστόσο, μια πρόβλεψη θα μπορούσε να γίνει από έναν εισβολέα εξετάζοντας προσεκτικά τα πακέτα και κοιτάζοντας μέσα από τα πεδία, για παράδειγμα στα πακέτα MDNS, τα οποία θα μπορούσαν να παρέχουν κάποιες πληροφορίες και να χρησιμοποιηθούν για την πρόβλεψη. Επίσης, υπάρχουν στατιστικά στοιχεία των πακέτων τα οποία θα μπορούσαν να χρησιμοποιηθούν από έναν επιτιθέμενο για την εύρεση της ώρας έναρξης και λήξης που έχει γίνει ένα ερώτημα.

5.3 Σύγκριση Αποτελεσμάτων

Πιο κάτω [Πίνακας 6], φαίνονται όλα τα σενάρια με τα διαφορετικά δεδομένα εισόδου μαζί με τα αποτελέσματα ακρίβειας κάθε αλγορίθμου για κάθε περίπτωση. Άλλα σενάρια έχουν επίσης δοκιμαστεί αλλά δεν περιλαμβάνονται, καθώς θεωρήθηκαν μη ρεαλιστικά ή μη χρήσιμα για την αξιολόγηση. Για παράδειγμα, όταν η συνολική διάρκεια κάθε ερώτησης χρησιμοποιήθηκε ως είσοδος, όλοι οι αλγόριθμοι είχαν ακρίβεια κοντά στο 100% αφού η διάρκεια κάθε ερώτησης είναι μοναδική και μπορεί να καθορίσει την ετικέτα του αριθμού της ερώτησης.

Δεδομένα εισαγωγής	Decision Tree	K-Nearest Neighbors	Random Forest
Length	~13%	~12%	~12%
Length,Download,Upload	~12%	~10%	~5%
Length,Start/End time	~15%	~63%	~12%

Πίνακας 6

Η υψηλότερη ακρίβεια πρόβλεψης έχει παρατηρηθεί όταν το μήκος του πακέτου, η ώρα έναρξης και η ώρα λήξης κάθε ερώτησης δόθηκε ως είσοδος στον αλγόριθμο KNN, με πρόβλεψη κοντά στο 63%. Ωστόσο, η ώρα έναρξης και λήξης κάθε ερώτησης θεωρείται ακραίο σενάριο και κανονικά θα ήταν δύσκολο για έναν εισβολέα να μπορέσει να το βρει. Μια εκτίμηση της ώρας έναρξης και λήξης θα μπορούσε να είναι εφικτή για έναν εισβολέα χρησιμοποιώντας τις πληροφορίες και τα στατιστικά στοιχεία που μπορούν να ληφθούν με την υποκλοπή όλων των πακέτων. Ωστόσο, θα ήταν ακόμα δύσκολο για έναν επιθετικό να επιτύχει μια τόσο υψηλή ακρίβεια πρόβλεψης.

5.4 Περιορισμοί

Για όλα τα αποτελέσματα και τις προβλέψεις, υποτίθεται ότι ένας κακόβουλος χρήστης θα μπορούσε να έχει πρόσβαση στο δίκτυο που λειτουργεί το GHNM. Επιπρόσθετα τα οικιακά δίκτυα δεν θεωρούνται ασφαλή και συνήθως υπάρχουν ελάχιστοι έως καθόλου αμυντικοί μηχανισμοί, για να αποκτήσει ένας εισβολέας τέτοια ποσότητα δεδομένων θα χρειαζόταν πρόσβαση στο δίκτυο για αρκετό καιρό χωρίς ο χρήστης να γνωρίζει την ύπαρξη του εισβολέα στο τοπικό δίτκυο.

Επιπλέον, κατά τη διάρκεια του πειράματος τα ερωτήματα έγιναν με διαδοχική σειρά και με την ίδια σειρά για να χρησιμοποιηθούν για όλη τη διάρκεια του πειράματος. Αυτό διευκόλυνε τη μέτρηση της ώρας έναρξης και λήξης κάθε ερώτησης και το συνδυασμό όλων των πληροφοριών που συλλέχθηκαν από τη λήψη πακέτων και τους ελέγχους ταχύτητας δικτύου, τα οποία στη συνέχεια χρησιμοποιήθηκαν για την εκπαίδευση και τη δοκιμή των αλγορίθμων.

Επιπλέον, κάθε ένας από τους αλγόριθμους περιέχει διαφορετικές μεταβλητές και παράγοντες που μπορούν να αναλυθούν και να μελετηθούν στατιστικά προκειμένου να επιτευχθούν οι πιο ακριβείς προβλέψεις για τους αλγόριθμους. Για τις ιδανικές προβλέψεις και την ακρίβεια των αλγορίθμων, αυτές οι μεταβλητές και παράγοντες πρέπει να αναλυθούν περαιτέρω στατιστικά και να μελετηθούν σε βάθος για κάθε αλγόριθμο.

6. Επίλογος

Αυτή η έρευνα διερεύνησε τις πιθανές απειλές που θα μπορούσε να επιφέρει η χρήση IoT και πιο συγκεκριμένα ένας ΕΨΒ, στους χρήστες οικιακών συσκευών. Η επιβολή κανονισμών και νόμων που στοχεύουν στην προστασία του απορρήτου των χρηστών είναι αναμφισβήτητα προς τη σωστή κατεύθυνση. Η αρχή Private by Design θα πρέπει να είναι υποχρεωτική απαίτηση για όλα τα συστήματα που στέλνουν, λαμβάνουν, συλλέγουν ή αποθηκεύουν ιδιωτικές πληροφορίες. Ειδικά για τις έξυπνες οικιακές συσκευές που σχετίζονται άμεσα με προσωπικές πληροφορίες, η ασφάλεια και το απόρρητό τους θα πρέπει να είναι πολύ δυνατά. Ωστόσο, οι αναφορές και τα περιστατικά σχετικά με τη χρήση των ΕΨΒ δείχνουν ότι η ασφάλειά τους δεν καλύπτει όλες τις προσδοκίες. Τα αποτελέσματα και τα συμπεράσματα αυτής της μελέτης επιβεβαιώνουν ότι το απόρρητο των καθημερινών συνδεδεμένων συσκευών εξακολουθεί να μην έχει διασφαλιστεί στο μέγιστο βαθμό.

6.1 Επεκτασιμότητα

Αν και το δείγμα των ερωτημάτων που έχουν επιλεγεί για το πείραμα καλύπτει μερικές από τις πιο συνηθισμένες ερωτήσεις που χρησιμοποιούν συνήθως οι χρήστες, μπορούν να χρησιμοποιηθούν περισσότερα ερωτήματα για την περαιτέρω μελέτη του απορρήτου ενός ΕΨΒ. Επιπλέον, μπορούν να δοκιμαστούν περισσότεροι αλγόριθμοι για να βρεθεί ποιος από τους αλγόριθμους είναι καταλληλότερος για την ταξινόμηση των δεδομένων.

Επίσης, θα μπορούσε να κατασκευαστεί ένα ολοκληρωμένο σύστημα σε πραγματικό χρόνο που θα είναι σε θέση να συλλέγει τα δεδομένα που μεταδίδονται από ένα ΕΨΒ και να εκτελεί

ταξινόμηση σε πραγματικό χρόνο. Ένα τέτοιο σύστημα θα απαιτούσε τη βελτιστοποίηση των αλγορίθμων, προκειμένου να είναι σε θέση να πραγματοποιήσει ταξινόμηση για δεδομένα που μεταδίδονται κατά τη χρήση ενός ΕΨΒ από έναν χρήστη σε πραγματικό χρόνο.

Βιβλιογραφία

Abd, N., M. Ramokapane, K. & M. Such, J., 2019. *More than Smart Speakers: Security and Privacy Perceptions of Smart Home,* s.l.: usenix.org.

Aveek, K. D., Parth, H. P., Chen-Nee, C. & Prasant, M., 2016. *Uncovering privacy leakage in ble network traffic of wearable fitness trackers,* s.l.: s.n.

Crawley, S., 2017. *Multicast DNS (mDNS) vulnerability,* s.l.: s.n.

CUELLAR, S. E. V., 2020. *Privacy issues and digital forensic analysis for,* s.l.: s.n.

Gamblin, J., 2018. [Ηλεκτρονικό]
Available at: https://jerrygamblin.com/2018/10/29/google-home-insecurity/

Google, S., 2021. *Google Support.* [Ηλεκτρονικό]
Available at: https://support.google.com/googlenest/answer/7130274?hl=en
[Πρόσβαση June 2021].

Gray, S., 2016. *Always ON: Privacy implications of microphone-enabled devices, Future of Privacy Forum,* s.l.: s.n.

Gu, C., Zhang, S. & Sun, Y., 2011. *Real-Time Encrypted Traffic Identification Using Machine Learning,* s.l.: J. Software.

Hoy, M. B., 2018. *Alexa, Siri, Cortana, and More: An Introduction to Voice Assistants,* s.l.: researchgate.

Hyunji, C., Iorga, M., Jeffrey, V. & Sangjin , L., 2017. *Alexa, Can I Trust You?,* s.l.: s.n.

Jide, S. E., Jose, M. S. & Guillermo, S. T., 2020. *Smart Home Personal Assistants: A Security and Privacy,* s.l.: s.n.

Junwoo, S. και συν., 2017. *An Analysis of Economic Impact on IoT under GDPR,* s.l.: IEEE.

luca, 2017. [Ηλεκτρονικό]
Available at: https://jerrygamblin.com/2018/10/29/google-home-insecurity/

micakisa, 2017. *Exploring the Amazon Echo Dot, Part 1: Intercepting Firmware Updates.* [Ηλεκτρονικό]
Available at: https://medium.com/@micaksica/exploring-the-amazon-echo-dot-part-1-intercepting-firmware-updates-c7e0f9408b59

micakisa, 2017. *medium.com.* [Ηλεκτρονικό]
Available at: https://medium.com/@micaksica/exploring-the-amazon-echo-dot-part-1-intercepting-firmware-updates-c7e0f9408b59

Morgenstern, M., 2017. OK, Google Home. What about privacy?.

Nguyen & Armitage, G., 2008. *A Survey of Techniques for Internet Traffic Classification Using Machine Learning,* s.l.: IEEE Comm. Surveys & Tutorials.

Noah, A., Dillon, R. & Nick, F., 2017. *A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,* s.l.: s.n.

Rachelle, B. και συν., 2017. *Privacy in a world of the Internet of Things A Legal and Regulatory Perspective,* s.l.: Networked Society Institute.

Wachter, S., 2018. *Normative challenges of identification in the Internet of Things: Pivacy, profiling, discrimination, and the GDPR, computer law & security review,* s.l.: Elsevier Ltd.

Wassermann, G., 2015. [Ηλεκτρονικό]
Available at: https://www.kb.cert.org/vuls/id/550620/