Ασφάλεια δημόσιων Wi-Fi δικτύων

Κωνσταντίνος Ζαφειρόπουλος

20390293, ice20390293@uniwa.gr

Ασφάλεια Δικτύων και Επικοινωνιών, Ιανουάριος 2024

Διδάσκοντες: Ι. Καντζάβελου, Ρ. Γαροφαλάκη, Α. Γεωργούλας

1. Εισαγωγή

Τα δημόσια σημεία πρόσβασης Wi-Fi σήμερα όντας ευρέως γνωστά, αξιοποιούνται σε παγκόσμια κλίμακα. Πολλά άτομα επιλέγουν να συνδεθούν σε αυτά τα hotspot λόγω της φθηνής φύσης τους σε αντίθεση με τις συνδέσεις δεδομένων κινητής τηλεφωνίας. Σύμφωνα με έρευνα της Symantec στην οποία συμμετείχαν 15.532 καταναλωτές σε 15 διεθνείς αγορές, το 46% των ερωτηθέντων δεν διστάζουν να συνδεθούν σε δίκτυα Wi-Fi μέσα σε λίγα λεπτά από την άφιξή τους σε τοποθεσίες όπως αεροδρόμια, εστιατόρια, εμπορικά κέντρα, ξενοδοχεία και παρόμοιους χώρους. Αντίθετα, το 60% των συμμετεχόντων αγνοεί τους πιθανούς κινδύνους που συνδέονται με τη χρήση ενός μη αξιόπιστου δικτύου και πιστεύουν ότι τα προσωπικά τους στοιχεία είναι ασφαλή [1].

Το Wi-Fi, παράλληλα με τα δίκτυα κινητής τηλεφωνίας GSM, ξεχωρίζει ως η κυρίαρχη λύση στον τομέα των ασύρματων τεχνολογιών [2], [3]. Εντός των ασύρματων δικτύων, ανακύπτει όμως μια πρωταρχική ανησυχία για την ασφάλεια: οποιοσδήποτε εντός της περιοχής σήματος έχει τη δυνατότητα να επιχειρήσει μη εξουσιοδοτημένη πρόσβαση σε ένα τέτοιο δίκτυο αξιοποιώντας τυχόν αδυναμίες και ελαττώματα στα πρωτόκολλα Wi-Fi [4]. Σύμφωνα με την Έκθεση Norton, ανακαλύφθηκε ότι το 68% των ατόμων που χρησιμοποιούν δημόσιο Wi-Fi πέφτουν θύματα εγκλημάτων στον κυβερνοχώρο. Αυτά τα εγκλήματα έχουν τη δυνατότητα να εκμεταλλεύονται και να κλέβουν ευαίσθητα δεδομένα όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης, μηνύματα συνομιλίας, email, φωτογραφίες αλλά και να εξάγουν προσωπικές πληροφορίες, συμπεριλαμβανομένων λεπτομερειών σχετικά με τη θρησκεία, την εθνικότητα και τον σεξουαλικό τους προσανατολισμό [5-6]. Η έκθεση του Vanhoef τόνισε αυτό το ζήτημα το 2013. Σήμερα, η τεχνολογία έχει προχωρήσει ραγδαία, οδηγώντας στη συνεχή ανάπτυξη και ανακάλυψη νέων επιθέσεων στον κυβερνοχώρο, ιών και εκμεταλλεύσεων [5].

Είναι είδη σαφές πως πρέπει να μην χρησιμοποιούμε δημόσια δίκτυα Wi-Fi. Εναλλακτικά, εάν η αποφυγή τους δεν είναι εφικτή, είναι απαραίτητο να ασφαλίσουμε τη σύνδεση πριν συνεχίσουμε στη χρήση τους. Τα παραπάνω επιβεβαιώνονται στην συνέχεια με την παρουσίαση πιθανών επιθέσεων που μπορούν να εκτελέσουν οι χάκερ (hacker) για να υποκλέψουν και να παρακολουθήσουν την κυκλοφορία του δικτύου. Καθώς και με τρόπους αντιμετώπισης ή προστασίας από τέτοιου είδους επιθέσεις που καθιστούν τα δημόσια δίκτυα Wi-Fi και τους χρήστες αυτών ευάλωτους [7-8].

2. Επισκόπηση της βιβλιογραφίας

Σε αυτή την ενότητα αναφέρουμε προηγούμενες μελέτες, περιγράφοντας το state of the art σχετικά με υποκλοπή προσωπικών στοιχείων μέσω δημόσιων Wi-Fi, παρακολούθηση του ιστού (web tracking) και άλλες αδυναμίες των δημόσιων Wi-Fi. Η Cheng et al. [8] συγκέντρωσε δεδομένα δημόσιων Wi-Fi από 20 αεροδρόμια σε τέσσερα έθνη. Η μελέτη τους αποκάλυψε ότι περίπου το 66% των ταξιδιωτών αποκαλύπτουν ακούσια προσωπικές πληροφορίες όταν χρησιμοποιούν hotspot αεροδρομίων για δραστηριότητες όπως η περιήγηση στον Ιστό και η χρήση εφαρμογών για κινητά τηλέφωνα. Οι περισσότεροι κίνδυνοι για Wi-Fi/WLAN συνδέονται με τη δυνατότητα παρεμβολής της υπάρχουσας επικοινωνίας και τη λήψη ή και παρεμβολή πακέτων. Η λήψη πακέτων μπορεί να πραγματοποιηθεί χρησιμοποιώντας την κάρτα δικτύου σε εποπτευόμενη λειτουργία [9]. Η Sombatruang et al. [10] διεξήγε μια παρόμοια μελέτη στην Ιαπωνία με τη δημιουργία 11 πειραματικών ανοιχτών δημόσιων δικτύων Wi-Fi. Το πείραμα των 150 ωρών επιβεβαίωσε την έκθεση προσωπικών πληροφοριών, συμπεριλαμβανομένων των φωτογραφιών και των διαπιστευτηρίων των χρηστών να μεταδίδονται μέσω HTTP. Η Klasnja et al. [11] ερεύνησε τη συνείδηση του απορρήτου και της ασφάλειας 11 χρηστών Wi-Fi αναλύοντας τα δεδομένα της διαδικτυακής κίνησης. Η μελέτη δείχνει ότι οι καταναλωτές έχουν ελλιπή γνώση των κινδύνων που ενέχει η χρήση Wi-Fi και ψευδή αίσθηση προστασίας.

Σε αντίθεση με τους προσωπικούς υπολογιστές, τα smartphone και τα tablet, τα δημόσια σημεία πρόσβασης (AP) δεν έχουν αλληλεπίδραση με τον χρήστη και συνήθως δεν διαθέτουν αυτοματοποιημένες ενημερώσεις ασφαλείας. Μόλις αγοραστούν και αναπτυχθούν αυτά τα εμπορικά διαθέσιμα AP, συχνά παραμένουν μη ενημερωμένα, ακόμη και όταν τα τρωτά σημεία εντοπίζονται και τεκμηριώνονται με την πάροδο του χρόνου, όπως στη βάση δεδομένων CVE [12]. Αυτή η έλλειψη ενημέρωσης σχετικά με τα αναφερόμενα τρωτά σημεία καθιστά αυτά τα AP σταδιακά λιγότερο ασφαλή. Η εκμετάλλευση των τρωτών σημείων σε δημόσια σημεία πρόσβασης είναι σχετικά απλή σε σύγκριση με τις προσωπικές συσκευές, καθώς ενδέχεται να μην απαιτούν κωδικούς πρόσβασης ή να έχουν εύκολα προσβάσιμους κωδικούς πρόσβασης. Επιπλέον, εφαρμογές για κινητές συσκευές όπως το Wi-Fi Master Key [13], με πάνω από 800 εκατομμύρια χρήστες, διευκολύνουν την κοινή χρήση κωδικών πρόσβασης Wi-Fi. Αν και αυτή η ευκολία προσφέρει στους χρήστες δωρεάν πρόσβαση στο Διαδίκτυο, δημιουργεί επίσης μια ευκαιρία για τους εισβολείς να διερευνήσουν και να εκμεταλλευτούν δίκτυα. Μόλις εκμεταλλευτούν αυτά τα τρωτά σημεία, τα παραβιασμένα AP μπορούν να χρησιμοποιηθούν για σοβαρές επιθέσεις όπως η ανακατεύθυνση DNS, το ηλεκτρονικό ψάρεμα (phishing) και η ηλεκτρονική κλοπή ταυτότητας/κωδικού πρόσβασης [14].

Τα ασύρματα δίκτυα αποτελούν ένα βολικό μέσο για τα άτομα να συνδέονται στο Διαδίκτυο, ένα χαρακτηριστικό που συχνά θεωρείται πολύτιμο από τις επιχειρήσεις είναι να προσφέρουν δωρεάν υπηρεσίες Wi-Fi στους πελάτες τους[15]. Ο αριθμός των δωρεάν σημείων πρόσβασης Wi-Fi στο Ηνωμένο Βασίλειο έφτασε περίπου τις 269.000 το 2016, με πάνω από 200 σταθμούς του μετρό του Λονδίνου να συνεχίζουν να παρέχουν δωρεάν πρόσβαση Wi-Fi [15]. Αυτή η προσβασιμότητα επιτρέπει στα άτομα να δημιουργήσουν εναλλακτικές ταξιδιωτικές ρυθμίσεις κατά τις περιόδους αποσύνδεσης. Παρά αυτά τα πλεονεκτήματα, είναι σημαντικό να αναγνωρίσουμε τους κινδύνους ασφαλείας που σχετίζονται με τη χρήση του Wi-Fi στο κοινό.

Η Παρακολούθηση Ιστού (Web Tracking), αποτελεί ένα ευρέως διαδεδομένο φαινόμενο στο Διαδίκτυο και χρησιμοποιείται για μια ποικιλία σκοπών, συμπεριλαμβανομένων στοχευμένων διαφημίσεων, ελέγχων ταυτότητας, αναλύσεων ιστού και εξατομίκευση. Η Eckersley έδειξε ότι το 83.6% των χρηστών που επισκέφτηκαν την σελίδα panopticlick.eff.org μπορούσαν να ταυτοποιηθούν μοναδικά από ένα αποτύπωμα που απαρτιζόταν μόνο από 8 στοιχεία/παράγο-

ντες. Η Laperdrix et al. έδειξε ότι η ιστοσελίδα AmIUnique.org μπορεί να αναγνωρίσει μοναδικός το 89.4% των αποτυπωμάτων βασισμένη σε 17 στοιχεία περιλαμβάνοντας το HTML5 canvas και το WebGL API [1]. Σε μια πρόσφατη εκτεταμένη έρευνα, οι G´omezBoix et al. [1] διεξήγαγε μια μελέτη σε έναν κορυφαίο γαλλικό ιστότοπο, συγκεντρώνοντας πάνω από 2 εκατομμύρια δακτυλικά αποτυπώματα συσκευών πραγματικού κόσμου, το καθένα από τα οποία περιλαμβάνει 17 χαρακτηριστικά. Τα ευρήματά τους αποκάλυψαν ότι μόνο το 33,6% των δακτυλικών αποτυπωμάτων της συσκευής είναι μοναδικά, δημιουργώντας αμφιβολίες για την αποτελεσματικότητα των τεχνικών δακτυλικών αποτυπωμάτων σε πρακτικά σενάρια. Είναι αξιοσημείωτο ότι η συνεχιζόμενη έρευνα διερευνά ενεργά προηγμένες μεθόδους δακτυλικών αποτυπωμάτων που στοχεύουν στον εντοπισμό της «χρυσής εικόνας», αναφερόμενη σε συνεπείς διαμορφώσεις λογισμικού και υλικού που συχνά αναπτύσσονται σε μεγάλες επιχειρήσεις (όπως συζητείται στο [16]).

Μια ολοκληρωμένη μελέτη του 2019 εξετάζει τις επιθέσεις κοινωνικής μηχανικής, τις ταξινομήσεις τους και τις στρατηγικές για τον εντοπισμό και την πρόληψη μέσω μιας εκτενούς έρευνας [17]. Η ευαισθησία των δικτύων Wi-Fi σε παραβιάσεις ασφαλείας αποδίδεται συχνά σε εσφαλμένες διαμορφώσεις, έλλειψη συντήρησης δικτύου και ενημερώσεις.

Έρευνα [18] υπογραμμίζει την έλλειψη ενημέρωσης των χρηστών σχετικά με τις συνδέσεις που δημιουργούνται από εφαρμογές για κινητές συσκευές, αφήνοντας ευάλωτο σημαντικό αριθμό ασύρματων δικτύων λόγω της απουσίας μέτρων ασφαλείας. Τα ανασφαλή δίκτυα Wi-Fi εκθέτουν τα μεταδιδόμενα δεδομένα σε εύκολη παρακολούθηση όταν δεν εφαρμόζεται σωστή κρυπτογράφηση από άκρο σε άκρο σε εφαρμογές. Η ασφάλεια των μεθόδων κρυπτογράφησης ασύρματου δικτύου, όπως το Wi-Fi Protected Setup (WPS), εξετάζεται στο [18], όπου συζητούνται ευπάθειες όπως η επίθεση με χειραψία 4 κατευθύνσεων απόκτησης κλειδιού και η κακή δίδυμη επίθεση (Evil-twin attack). Μια διαδικτυακή έρευνα αποκαλύπτει ότι η πλειονότητα των ερωτηθέντων δεν είναι καλά ενημερωμένοι σχετικά με την ασφάλεια ασύρματης σύνδεσης [18]. Ενώ πολλές επιχειρήσεις εφαρμόζουν προστατευτικά μέτρα όπως τείχη προστασίας και λογισμικό προστασίας από ιούς για την ασφάλεια σύνδεσης από άκρο σε άκρο, οι εσφαλμένες διαμορφώσεις και τα ζητήματα συμβατότητας παραμένουν πηγές παραβιάσεων της ασφάλειας. Μια έρευνα του 2018 που διεξήχθη στο δίκτυο πανεπιστημιούπολης "Universiti Utara Malaysia" τονίζει την ανάγκη οι διαχειριστές του δικτύου να αντιμετωπίζουν αυτά τα ζητήματα ασφάλειας [19]. Τέλος, ένα ολοκληρωμένο πλαίσιο του Evil-twin, που εκμεταλλεύεται ευπάθειες από την πλευρά του πελάτη, χρησιμεύει ως εργαλείο απόδειξης της ιδέας για τον έλεγχο της ασφάλειας και την αύξηση της ευαισθητοποίησης σχετικά με τα τρωτά σημεία του Wi-Fi [18].

3. Ορισμός Προβλήματος

Οι απειλές για τα δίκτυα Wi-Fi σε κάποιο βαθμό είναι οι ίδιες με άλλα δίκτυα. Οι κύριες πηγές απειλών είναι τρεις: το Διαδίκτυο, το ηλεκτρονικό ταχυδρομείο (email) και η δυνατότητα υποκλοπής επικοινωνίας και άρα προσωπικών στοιχείων ή και παρακολούθησης του ιστού. Η διαφορά μεταξύ ασύρματων από ενσύρματων δικτύων είναι η δυνατότητα υποκλοπής και παρέμβαση τρίτων σε συνεδρίες μετάδοσης[9]. Η ανάλυση και η σύλληψη των πακέτων είναι δυνατή μέσω της χρήσης εργαλείων ανάλυσης πακέτων. Υπάρχουν διαθέσιμα πληθώρα εργαλείων για την ανάλυση πακέτων όπως τα airodump-ng, tcpdump, Tshark, Ethereal, Wireshark. Το πιο δημοφιλές πρόγραμμα ανάλυσης, υποκλοπής πακέτων είναι πλέον το Wireshark, το οποίο αντικατέστησε το πρόγραμμα Ethereal. Χρησιμοποιώντας το Wireshark, μπορούμε μέσω της κάρτας υπό εποπτευόμενη λειτουργία να έχουμε πρόσβαση σε χιλιάδες πακέτα στην περίπτωση

ανοιχτών δικτύων χωρίς κρυπτογράφηση. Όταν υπάρχει κρυπτογράφηση στα δημόσια δίκτυα Wi-Fi μπορεί κανείς να καταγράψει μόνο το πλαίσια διαχείρισης, ελέγχου και τα beacon frames επειδή αυτά τα πλαίσια είναι σε απλό κείμενο (plain text) και δεν είναι κρυπτογραφημένα[9].

Παρόλα αυτά τα συχνότερα πρωτόκολλα ασφαλείας που συναντάμε σε δημόσια Wi-fi είναι WEP , WPA και WPA2 και όχι WPA3 που είναι το πιο ασφαλές και ενημερωμένο μέχρι στιγμής. Αναλυτικότερα το WEP, γνωστό για την αδύναμη κρυπτογράφηση και το ανασφαλές πρωτόκολλο χειραψίας του, αποσύρθηκε λόγω εκμεταλλεύσιμων αδυναμιών, όπως η χρήση του ίδιου κλειδιού για έλεγχο ταυτότητας και κρυπτογράφηση[20]. Το WPA, που προοριζόταν ως προσωρινή λύση, αντιμετώπισε ορισμένα από τα ελαττώματα του WEP, αλλά εισήγαγε νέα τρωτά σημεία, συμπεριλαμβανομένων προβλημάτων με το Wi-Fi Protected Setup (WPS) και τη χρήση ενός μη ασφαλούς αλγορίθμου κρυπτογράφησης (RC4). Το WPA2 βελτιώθηκε σε σχέση με τους προκατόχους του εφαρμόζοντας έναν πιο ισχυρό αλγόριθμο κρυπτογραφίας και υιοθετώντας πλήρως το πρότυπο 802.11i, προσφέροντας αυξημένη προστασία από διάφορες επιθέσεις[20].

Παραθέτουμε τις βασικότερες αδυναμίες και επιθέσεις που μπορεί να δεχτεί ένα δημόσιο Wi-fi και μπορεί να έχει σοβαρές συνέπειες για τους συνδεδεμένους χρήστες:

Sniffing: Ένας εισβολέας αποσπά, υποκλέβει τα πακέτα που ταξιδεύουν μεταξύ δύο συστημάτων, παρακολουθεί την κίνηση του δικτύου και με αυτόν τον τρόπο μπορεί να αποκτήσει πρόσβαση στα στοιχεία σύνδεσης του χρήστη, διαπιστευτήρια και άλλες ευαίσθητες πληροφορίες που ρέουν στο δίκτυο. [21]

Spoofing: Ένας εισβολέας στέλνει μηνύματα σε έναν υπολογιστή με μια διεύθυνση IP που υποδεικνύει ότι το μήνυμα προέρχεται από έναν φαινομενικά αξιόπιστο οικοδεσπότη. Αυτές οι επιθέσεις μπορούν να εφαρμοστούν εύκολα και μπορούν να έχουν αντίκτυπο στην απόδοση του δικτύου.[22]

Side-jacking: Ένας εισβολέας αποσπά πακέτα από ένα δίκτυο και με αυτό μπορεί να κλέψει το cookies της συνεδρίας. Χρησιμοποιεί αυτά τα cookies για έλεγχο ταυτότητας σε διακομιστή ιστού. Οι ιστοσελίδες συνήθως χρησιμοποιούν το πρωτόκολλο HTTPS (Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκειμένου) μόνο τη στιγμή σύνδεσης για να προστατέψουν το όνομα χρήστη και τον κωδικό πρόσβασης, αλλά αργότερα αλλάζουν σε HTTP (Πρωτόκολλο μεταφοράς υπερκειμένου). Σε αυτή τη διαδικασία, τα cookies εξακολουθούν να αποστέλλονται στον διακομιστή πάνω από το μη ασφαλές πρωτόκολλο HTTP και τότε ένας χάκερ μπορεί να υποκλέψει πληροφορίες. [23]

Rogue access points: Πρόκειται για παραπλανητικά σημεία πρόσβασης που εμφανίζονται ως νόμιμα σημεία πρόσβασης αλλά μπορεί να είναι πλαστά που έχουν δημιουργηθεί από έναν εισβολέα. Αυτά τα APs παραπλανούν τους χρήστες κάνοντάς τους να συνδεθούν σε ψεύτικα σημεία πρόσβασης. Μόλις πραγματοποιηθεί σύνδεση στο πλαστό σημείο πρόσβασης, η κίνηση των χρηστών ανακατευθύνεται και αναλύεται από τον επιτιθέμενο. Αυτό εμπίπτει στην κατηγορία των επιθέσεων MITM (Man in the Middle). [24]

Η επίθεση Evil-twin αναφέρεται σε ένα πλαστό σημείο πρόσβασης που μιμείται την ταυτότητα ενός νόμιμου. Αφού συνδεθεί ένας χρήστης σε ένα δίκτυο Wi-Fi, αυτό το δίκτυο προστίθεται στη λίστα των προτιμώμενων δικτύων του, μια τυπική δυνατότητα στα πρόσφατα λειτουργικά συστήματα. Για να εκτελέσει μια επίθεση, ο επιτιθέμενος αποσυνδέει τον χρήστη από το αυθεντικό σημείο πρόσβασης, προτρέποντας τη συσκευή του χρήστη να συνδεθεί αυτόματα

στο παραπλανητικό σημείο πρόσβασης. Αυτό συμβαίνει επειδή το παραπλανητικό σημείο πρόσβασης μοιράζεται το ίδιο SSID και όνομα δικτύου με το νόμιμο, και η ισχύς του σήματος του ξεπερνά αυτή του πραγματικού σημείου πρόσβασης [25]. Μόλις αποσυνδεθεί επιτυχώς, το σύστημα ελέγχει τη λίστα προτιμώμενων δικτύων και, καθώς τα ονόματα ταιριάζουν, δημιουργεί μια σύνδεση με το ψεύτικο (Evil-twin) σημείο πρόσβασης. Κατά τη σύνδεση, τυχόν κωδικοί πρόσβασης που εισάγει ο χρήστης αποθηκεύονται αυτόματα στη βάση δεδομένων του εισβολέα λόγω των διαμορφώσεων του Evil-twin access point [25].

Τα αποτελέσματα μιας επίθεσης Evil-twin στον τελικό χρήστη είναι σημαντικά. Μόλις συνδεθεί, ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στον κωδικό πρόσβασης Wi-Fi του χρήστη, στους λογαριασμούς email, στις πληροφορίες πιστωτικής/χρεωστικής κάρτας και στους ιστότοπους κοινωνικής δικτύωσης. Επιπλέον, ο εισβολέας μπορεί να χειραγωγήσει ποιοι ιστότοποι εμφανίζονται στον χρήστη και ποιοι όχι [25].

4. Προτεινόμενη Λύση

Υπάρχουν ορισμένα μέτρα που πρέπει να ληφθούν πριν συνδεθεί ένας χρήστης σε ένα δημόσιο Wi-Fi ή hotspot, για να αποφύγει να πέσει θύμα των παραπάνω επιθέσεων.
Είναι τα εξής[25]:

1. Μετά την αποσύνδεση από ένα άγνωστο Wi-Fi, είναι επιθυμητό να σαρώσετε το σύστημα για να εάν έχει εισαχθεί ιός σε αυτό, ώστε να μπορεί να διορθωθεί αμέσως πριν από οποιαδήποτε βλάβη.

2. Οι ιστότοποι που διαθέτουν κρυπτογράφηση HTTPS είναι πιο ασφαλείς στη χρήση. Συνεπώς πρέπει να χρησιμοποιείται με προσοχή ιστότοπους με άλλη κρυπτογράφηση και μάλιστα πριν από την εισαγωγή ευαίσθητων πληροφοριών σε αυτούς.

3. Οι χρήστες πρέπει να προσέχουν τα παραπλανητικά σημεία πρόσβασης επειδή τα ονόματα αυτών είναι παρόμοια με τα νόμιμα σημεία πρόσβασης.

4. Ένας χρήστης πρέπει να βεβαιωθεί ότι το τείχος προστασίας είναι ενεργοποιημένο και ότι πρέπει να προστατευθεί ο ίδιος\από επιθέσεις ιών εγκαθιστώντας προγράμματα προστασίας από ιούς.

5. Κατά τη σύνδεση σε δημόσιο σημείο πρόσβασης, όπως σε καφετέριες ή εστιατόρια, ο χρήστης πρέπει να ελέγξει με τον προμηθευτή εάν το Hotspot είναι νόμιμο.

6. Είναι καλύτερα να αλλάξετε τις ρυθμίσεις της πρόσβασής σας στο Wi-Fi και να απενεργοποιήσετε την αυτόματη επανασύνδεση σε ένα δίκτυο Wi-Fi επειδή οι περισσότερες Evil-twin επιθέσεις χρησιμοποιούν αυτήν την ευπάθεια.

7. Οι εύκολοι κωδικοί πρόσβασης διευκολύνουν έναν εισβολέα να σπάσει έναν λογαριασμό. Έτσι πρέπει να ρυθμίσετε ένα δυνατό κωδικό πρόσβασης που έχει κεφαλαία, πεζά, σύμβολα και αλφαριθμητικούς χαρακτήρες για να βεβαιωθείτε ότι δεν σπάει εύκολα με επιθέσεις brute force ή dictionary.

8. Μην αποθηκεύετε ποτέ τους κωδικούς πρόσβασης ή οποιαδήποτε σημαντική πληροφορία σε κοινόχρηστους φακέλους.

9. Δεν είναι ασφαλής η πρόσβαση σε τραπεζικές εφαρμογές ενώ είστε συνδεδεμένοι σε δημόσιο Wi-Fi.

10. Η χρήση ενός εικονικού ιδιωτικού δικτύου μειώνει τις πιθανότητες απώλειας ευαίσθητων δεδομένων σε μεγάλη έκταση.

11. Το ασύρματο δίκτυο πρέπει να είναι απενεργοποιημένο όταν δεν χρησιμοποιείται.

Μέθοδοι προστασίας από επιθέσεις Evil-twin:

WPA-PSK: Αυτή η προσέγγιση περιλαμβάνει χρήστες που λαμβάνουν έναν εμπιστευτικό κωδικό πρόσβασης μέσω μιας προκαθορισμένης μεθόδου, όπως η διανομή μέσω κινητών συσκευών. Αποδεικνύεται αποτελεσματικό στον μετριασμό των Evil-twin επιθέσεων σε μεγάλες και μεσαίες επιχειρήσεις λόγω του διαχειρίσιμου κόστους υλοποίησης. Ωστόσο, για δημόσια ανοιχτά Wi-Fi ή μικρότερες επιχειρήσεις, μια εναλλακτική μέθοδος, όπως το μοντέλο Trust on First Use (TOFU), μπορεί να είναι πιο κατάλληλη [25]. Ωστόσο, έρχεται με μειονεκτήματα, συμπεριλαμβανομένης της ευαισθησίας σε επιθέσεις MITM.

Για να ενισχύσουμε περαιτέρω την ασφάλεια, ιδιαίτερα όσον αφορά την ταυτότητα AP, προτείνουμε τη δέσμευση ταυτοτήτων AP σε αυτο-υπογεγραμμένα δημόσια κλειδιά μέσω μιας νέας μονάδας ελέγχου ταυτότητας που έχει σχεδιαστεί για το επεκτάσιμο πρωτόκολλο ελέγχου ταυτότητας 802.1X (EAP). Η προτεινόμενη ασύρματη τεχνική ελέγχου ταυτότητας (EAP-SWAT) ακολουθεί την αρχή εμπιστοσύνης κατά την πρώτη χρήση (TOFU) για τον έλεγχο ταυτότητας του AP και τη δημιουργία κλειδιών συνεδρίας για ασφαλή παράδοση δεδομένων. Αν και οι πελάτες στο μοντέλο TOFU μπορεί να είναι επιρρεπείς σε αρχικές επιθέσεις πλαστοπροσωπίας κατά την πρώτη συσχέτιση AP, οι επακόλουθες συσχετίσεις διασφαλίζουν συνεπή ταυτότητα AP. Αυτή η προσέγγιση προσφέρει ισχυρή προστασία από Evil-twin επιθέσεις χωρίς να απαιτούνται εκ των προτέρων κοινά μυστικά (όπως στο WPA-PSK) ή προηγούμενες σχέσεις εμπιστοσύνης[26].

Μία επιπλέον μέθοδος προστασίας είναι η εφαρμογή του πρωτοκόλλου WPA3. Η εισαγωγή του WPA3 σηματοδότησε μια σημαντική πρόοδο στην ασφάλεια Wi-Fi, με στόχο να διορθώσει τα προβλήματα που εντοπίζονται σε παλαιότερα πρωτόκολλα. Το WPA3 παρουσίασε το πρωτόκολλο χειραψίας DragonFly για την αντιμετώπιση γνωστών τρωτών σημείων στο 802.11i, παρέχοντας βελτιωμένη ασφάλεια στον αμοιβαίο έλεγχο ταυτότητας και τη συμφωνία κλειδιού συνεδρίας. Παρά τις αρχικές ευπάθειες που ανακαλύφθηκαν στο πρωτόκολλο χειραψίας του WPA3, έχουν κυκλοφορήσει συνεχείς ενημερώσεις κώδικα προμηθευτών για τη βελτίωση της ασφάλειας[20]. Επιπλέον, η ευκαιριακή ασύρματη κρυπτογράφηση (OWE), που δεν αποτελεί μέρος της προδιαγραφής WPA3, επιτρέπει την κρυπτογράφηση ανοιχτών δικτύων, ενισχύοντας περαιτέρω τη συνολική ασφάλεια των δημόσιων Wi-Fi. Ενώ το WPA3 και τα νεότερα πρωτόκολλα αντιπροσωπεύουν βελτιώσεις στους σχεδιασμούς ασφαλείας του Wi-Fi, εξακολουθούν να υπάρχουν ανησυχίες σχετικά με το εάν τα υποκείμενα ζητήματα ασφάλειας από πρωτόκολλα παλαιού τύπου έχουν μετριαστεί πλήρως. Μια αξιολόγηση διαφόρων εφαρμογών ασφαλείας 802.11 αποκαλύπτει ότι μόνο οι πιο ακριβές και εξελιγμένες υλοποιήσεις, όπως το Geo-Fenced και το EAP-TLS, παρέχουν υψηλό βαθμό ασφάλειας από άκρο σε άκρο. Ανάλογα με την έκδοση του 802.11 και την επιλεγμένη εφαρμογή ασφάλειας, οι παράγοντες κινδύνου

και απειλής συνεχίζουν να εξελίσσονται[20]. Για αυτό το λόγο παραθέτουμε επιπλέον μεθόδους αντιμετώπισης και προστασίας από τις απειλές και τις αδυναμίες των δημόσιων Wi-Fi ώστε να προστατευθούν οι χρήστες.

VPN (Εικονικό ιδιωτικό δίκτυο): Για χρήστες που συνδέονται συχνά σε δημόσια Wi-Fi, η εγγραφή σε μια υπηρεσία VPN είναι μια βιώσιμη επιλογή. Ένα VPN διασφαλίζει την κρυπτογράφηση όλων των δεδομένων που μεταδίδονται από το δίκτυο, λειτουργώντας ως ισχυρό εμπόδιο μεταξύ του χρήστη και του ιστού [25]. Αυτή η λύση αποδεικνύεται αποτελεσματική και οικονομικά αποδοτική. Ακόμα κι αν ένας εισβολέας επιχειρήσει να κρυφακούσει μη κρυπτογραφημένη κίνηση μεταξύ του διακομιστή και του Διαδικτύου, δεν μπορεί να διακρίνει ποιες πληροφορίες αντιστοιχούν σε μεμονωμένους χρήστες, καθώς προέρχονται από έναν μόνο διακομιστή VPN.

Context-leashing (δέσμευση περιβάλλοντος): Καταγράφει όλα τα ορατά σημεία πρόσβασης (AP) όταν ένας πελάτης συνδέεται για πρώτη φορά σε ένα AP. Αυτά τα καταγεγραμμένα AP χρησιμεύουν ως ασύρματα ορόσημα, επιτρέποντας στον πελάτη να προσδιορίσει το σωστό περιβάλλον ή τοποθεσία για αυτό το δίκτυο. Οι επακόλουθες συσχετίσεις θα πρέπει να συμβαίνουν αυτόματα μόνο εάν το παρατηρούμενο περιβάλλον ευθυγραμμίζεται με το προηγουμένως καταγεγραμμένο περιβάλλον. Αυτή η μέθοδος είναι πρακτική, απαιτεί μόνο προσαρμογές από την πλευρά του πελάτη, χρήστη χωρίς πρόσθετο υλικό, καμία ρητή συμμετοχή του χρήστη και μοιράζεται εννοιολογικές ομοιότητες με επιτυχημένες μεθόδους εντοπισμού ασύρματης συσκευής [26]. Η εμπειρική αξιολόγηση με πραγματικά ίχνη από διάφορα ασύρματα Wi-Fi καταδεικνύει ότι η δέσμευση περιβάλλοντος επιτυγχάνει υψηλό ποσοστό ανίχνευσης για Evil-twin σενάρια, ενώ ελαχιστοποιεί τα ψευδώς θετικά σε διάφορα μοντέλα επιθέσεων.

5. Υλοποίηση Προτεινόμενης Λύσης.

Ακολουθεί πρακτική επίδειξη επιθέσεων σε δημόσια Wi-Fi καθώς και τρόποι, διαπίστωσης διαρροής απορρήτου σε αυτά αλλά και υλοποιήσεις των λύσεων που προαναφέρθηκαν.
Evil twin επίθεση, μια επίθεση που βασίζεται στο γεγονός ότι οι συσκευές μπορούν να δουν το SSID μόνο του ασύρματου δικτύου. Ουσιαστικά αποτελούν διπλότυπό ενός ασύρματου δικτύου πλαστογραφώντας το όνομα του δικτύου και τη MAC του διεύθυνση με την ελπίδα ότι οι πελάτες θα συνδεθούν στο σημείο πρόσβασής[26].

Βήματα:
1. Συνδεθείτε σε ασύρματο δίκτυο: για να αποκτήσετε πρόσβαση στο Internet.
Σε τύπο τερματικού…. Εκεί που είναι το wlan0, το όνομα της διεπαφής σας.
2. Ξεκινήστε το Airmon-Ng wlan0: για να μεταβείτε στη λειτουργία παρακολούθησης (monitor mode).
3. Ξεκινήστε το Airdump-Ng wlan0: για συλλογή πληροφοριών από την κυκλοφορία του δικτύου.
4. Προσδιορίστε τον στόχο, Δημιουργήστε ένα νέο AP με την ίδια Διεύθυνση SSID και MAC.
Χρησιμοποιώντας αυτό τον κώδικα:
airbase-ng -a <BSSID εδώ> --essid <ESSID εδώ> -c
<κανάλι εδώ> <όνομα διεπαφής>
5. Αναγκάστε τον στόχο να αποσυνδεθεί από το πραγματικό δίκτυο και έτσι να συνδεθεί ξανά στο ψεύτικο AP που δημιουργήσαμε.
Χρησιμοποιώντας αυτόν τον κώδικα:

aireplay-ng --deauth 0 -a <BSSID> mon0 --ignorenegative-one

6. Ο στόχος θα επανασυνδεθεί στο ψεύτικο δίκτυο, όπου πολλαπλές περαιτέρω επιθέσεις μπορούν να γίνουν όπως η DNS πλαστογράφηση[25].

Ο στόχος των διαφόρων μεθόδων διασφάλισης της ιδιωτικής ζωής κατά τη χρήση υπηρεσιών LBS έχει ως στόχο τη μείωση του κινδύνου απάτης. Επί του παρόντος δεν υπάρχει ολοκληρωμένη ασφάλεια, καθεμία από τις υπάρχουσες μεθόδους θεωρείται ανεξάρτητη, αν και στις πτυχές τους συχνά μοιράζονται παρόμοια χαρακτηριστικά. Υπάρχουν τρεις βασικές μέθοδοι όπως η παροχή ψευδών δεδομένων, η ανωνυμοποίηση και θόλωση ακρίβειας[9].

Η παροχή ψευδών πληροφοριών έχει ως στόχο την παροχή της υπηρεσίας διαδικτύου με λανθασμένα δεδομένα για τον χρήστη. Η εισαγωγή ψευδών πληροφοριών μπορεί να σχετίζεται με το όνομα χρήστη (ID) και δεδομένα τοποθεσίας για παράδειγμα. Μπορούμε να δώσουμε το όνομα του παράλληλου δρόμου ή μέρος που βρίσκεται κοντά στην πραγματική τοποθεσία. Επιπλέον, τα δεδομένα υποδεικνύονται όταν επισκεπτόμαστε πολλά φορές το ίδιο μέρος που μπορούμε να αλλάξουμε. Αυτή η μέθοδος μπορεί εύκολα να εφαρμοστεί από έναν χρήστη. Αντί για την πραγματική ταυτότητα δίνουμε οποιοδήποτε όνομα και επίσης αλλάζουμε τις συντεταγμένες της τοποθεσίας[9].

Παρακάτω περιγράφονται σύμφωνα με την μελέτη [1] τρόποι εντοπισμού παραβίασης σύνδεσης και υποκλοπής προσωπικών δεδομένων μέσω της CPInspector.

Προσδιορισμός τρίτων στην σύνδεση. Προσδιορίσαμε τους εταιρικούς ιστότοπους για κάθε hotspot. Στη συνέχεια, χρησιμοποιούμε τις εγγραφές WHOIS για να προσδιορίσουμε τομείς τρίτων συγκρίνοντας το όνομα κατόχου τομέα με τον ιδιοκτήτη εταιρικού ιστότοπου Wi-Fi. Σε περιπτώσεις όπου οι πληροφορίες προστατεύονται από την πολιτική απορρήτου WHOIS, επισκεπτόμαστε τον τομέα για να εντοπίσουμε οποιαδήποτε ανακατεύθυνση σε έναν γονικό ιστότοπο. Τότε αναζητούμε πληροφορίες εγγραφής του γονικού ιστότοπου. Εάν αυτό αποτύχει, εξετάζουμε με μη αυτόματο τρόπο το τομέα του Οργανισμού στο πιστοποιητικό TLS του, εάν είναι διαθέσιμο. Διαφορετικά, προσπαθούμε για την αναγνώριση του κατόχου του τομέα με βάση το email εγγραφής WHOIS. Εμείς επίσης χρησιμοποιήστε το Crunchbase.com και το Hoovers.com για να προσδιορίσετε εάν οι οργανισμοί είναι θυγατρικές ή εξαγορές μεγαλύτερων εταιρειών[1].

Προσδιορισμός ανιχνευτών τρίτων. Χρησιμοποιούμε EasyList, EasyPrivacy και Fanboy για να εντοπίσουμε γνωστούς ιχνηλάτες τρίτων. Αυτές οι λίστες βασίζονται σε σενάρια μαύρης λίστας ονόματα, διευθύνσεις URL ή τομείς, οι οποίοι ενδέχεται να αποτύχουν να εντοπίσουν νέους ιχνηλάτες ή παραλλαγές του γνωστοί ιχνηλάτες[1]. Για το λόγο αυτό, ταξινομούμε τους ιχνηλάτες τρίτων ως εξής: (α) Ένας γνωστός ιχνηλάτης είναι ένας τρίτος που έχει ήδη εντοπιστεί στα παραπάνω μαύρες λίστες. (β) Ένας πιθανός ανιχνευτής είναι οποιοσδήποτε τρίτος που μπορεί ενδεχομένως να παρακολουθήσει δραστηριότητες περιήγησης του χρήστη αλλά δεν περιλαμβάνονται σε μαύρη λίστα. Παρατηρήσαμε ότι παραλλαγές γνωστών ιχνηλατών όπως το Google Analytics, δεν υπήρχαν στις μαύρες λίστες[1].

Ο εντοπισμός της ένεσης διαφήμισης (add injection) αποτελεί μέρος του πλαισίου μας, συμπεριλαμβανομένης μιας ενότητας αφιερωμένης στον εντοπισμό αλλαγών στις επισκέψεις των χρηστών, όπως οι διαφημίσεις με ένεση. Επισκεπτόμαστε δύο ιστότοπους δόλωμα (honeysites) στον έλεγχό μας, που φιλοξενούνται στο AmazonAWS και στο BBC.com μέσω ενός οικιακού δικτύου και ενός δημόσιου σημείου πρόσβασης. Στη συνέχεια, συγκρίνουμε τις διαφορές στο ανακτηθέν περιεχόμενο, ειδικά τα δέντρα DOM [8]. Η χρήση των honeysites μας επιτρέπει να αποφεύγουμε πιθανά ψευδώς θετικά αποτελέσματα λόγω του δυναμικού περιεχομένου του ιστότοπου, όπως δυναμικές διαφημίσεις. Το πρώτο honeysite είναι μια στατική ιστοσελίδα, ενώ

το δεύτερο περιέχει δυναμικό περιεχόμενο με τέσσερις ψεύτικες διαφημίσεις. Αυτές οι ψεύτικες διαφημίσεις δημιουργήθηκαν χρησιμοποιώντας αποσπάσματα πηγαίου κώδικα από το Google Adsense, το Google TagManager, το Taboola.com και το BuySellAds.com.

Συλλογή δεδομένων: Συνολικά συλλέχθηκαν 679 σύνολα δεδομένων από την αποκλειστική πύλη και τη σελίδα προορισμού των 80 hotspot (12 hotspot μετρήθηκαν σε πολλές φυσικές τοποθεσίες) μεταξύ Σεπ. 2018 και Απρ. 2019. Εξαιρέσαμε 103 σύνολα δεδομένων λόγω διαφόρων σφαλμάτων (π.χ. αποτυχίες δικτύου)[1]. Αναλύσαμε πάνω από 18,5 GB συλλεγόμενης επισκεψιμότητας για μετρήσεις έκθεσης και παρακολούθησης απορρήτου, αναφέροντας αποτελέσματα από 67 μοναδικά hotspot (576 σύνολα δεδομένων). Συζητάμε τα αποτελέσματα στο Sec. 4. Για πειράματα έγχυσης διαφημίσεων, συλλέξαμε 368 σύνολα δεδομένων από τον εντοπισμό έγχυσης στους δύο ιστότοπους honey και στον ιστότοπο BBC.com σε 98 τοποθεσίες hotspot. Αναλύσαμε πάνω από 8,7 GB συλλεγμένων επισκέψεων για ένεση διαφήμισης και αναφέραμε αποτελέσματα από 87 μοναδικά hotspot (368 σύνολα δεδομένων). Δεν παρατηρήθηκαν τροποποιήσεις του περιεχομένου κατά τις προσπάθειες ένεσης[1].

6. Συζήτηση και Συμπεράσματα.

Πολλοί άνθρωποι ανά τον κόσμο χρησιμοποιούν δημόσια Wi-Fi που παρέχονται από ένα διαρκώς αυξανόμενο αριθμό επιχειρήσεων ή και δημόσιων, κυβερνητικών υπηρεσιών. Ωστόσο, αυτά τα δίκτυα Wi-Fi είναι επιρρεπή σε παρεμβάσεις τρίτων κατά τη διάρκεια συνεδριών επικοινωνίας, αποτελώντας σημαντική απειλή για τους χρήστες αλλά και τους παρόχους του συγκεκριμένου σημείου πρόσβασης. Αν και μπορεί να φαίνεται αδύνατο να αντιμετωπιστεί αυτή η ευπάθεια, η χρήση VPN και η ευρεία υιοθέτηση του HTTPS σε ιστότοπους και εφαρμογές για κινητά διαδραματίζουν κρίσιμο ρόλο στην ασφάλεια των προσωπικών και οικονομικών δεδομένων των χρηστών από πιθανούς κακόβουλους παράγοντες στο ίδιο hotspot.
Παρά τα μέτρα αυτά, η επίμονη απειλή, παρακολούθησης συσκευών των χρηστών, παραμένει λόγω της πρόσβασης των hotspot σε διευθύνσεις MAC και σε προσωπικά αναγνωρίσιμες πληροφορίες. Αυτός ο κίνδυνος απορρήτου, που συχνά παραβλέπεται, απαιτεί μια πιο ενδελεχή εξέταση των δημόσιων hotspot από τις κυβερνητικές ρυθμιστικές αρχές. Οι συστάσεις για τους χρήστες των hotspot περιλαμβάνουν την αποχή από την κοινή χρήση προσωπικών πληροφοριών, τη χρήση ιδιωτικής περιήγησης και πρόσθετα προγράμματος περιήγησης κατά της παρακολούθησης, τη χρήση λογισμικού για ψεύτικες διευθύνσεις MAC (ειδικά στα Windows) και τη διαγραφή του ιστορικού του προγράμματος περιήγησης μετά τη χρήση του hotspot.

Διάφορα εργαλεία όπως η απόκρυψη SSID, το φιλτράρισμα διευθύνσεων MAC, η κρυπτογράφηση και τα πρωτόκολλα ελέγχου ταυτότητας, όπως το WPA2-PSK και το WPA3, στοχεύουν στην ενίσχυση της ασφάλειας, αλλά δεν είναι αλάνθαστα. Η απαγόρευση της χρήσης συσκευών Wi-Fi στις γειτονιές δεν είναι εφικτή, καθιστώντας έτσι τις γνώσεις αλλά και την ευαισθητοποίηση των χρηστών κρίσιμα στοιχεία άμυνας. Οι χρήστες θα πρέπει να είναι προσεκτικοί όταν συνδέονται σε άγνωστα hotspot, αποφεύγοντας την πρόσβαση σε ευαίσθητους ιστότοπους, όπως διαδικτυακές πλατφόρμες τραπεζικών συναλλαγών και αποφεύγοντας την κοινή χρήση προσωπικών δεδομένων. Η αύξηση της ευαισθητοποίησης των χρηστών μπορεί να βελτιώσει σημαντικά τη συνολική ασφάλεια στο τρέχον τοπίο των δημόσιων Wi-Fi.

Προκειμένου να ενισχυθεί η πρόσβαση και το απόρρητο των χρηστών, με παράλληλη ελαχιστοποίηση του φόρτου για τους προγραμματιστές λογισμικού που συμμορφώνονται με τους κανονισμούς ασφάλειας δεδομένων, τα πρωτόκολλα δοκιμών λογισμικού πρέπει να γίνουν πιο αυστηρά. Οι ολοκληρωμένες περιπτώσεις δοκιμών θα πρέπει να διασφαλίζουν αποτελεσματική μετάδοση δεδομένων τόσο μέσω ενσύρματων δικτύων όσο και μέσω δημόσιων δεδομένων Wi-Fi και κινητής τηλεφωνίας. Συνεπώς, οι χρήστες θα πρέπει να χρησιμοποιούν τα δημόσια

Wi-Fi μόνο όταν είναι απαραίτητο, για να αποφύγουν τους κινδύνους κατασκοπείας, καθώς και να εγκαθιστούν και να ενημερώνουν τακτικά προγράμματα προστασίας στις συσκευές τους.

7. Αναφορές

[1] S. Ali, T. Osman, M. Mannan, and A. Youssef, "On Privacy Risks of Public WiFi Captive Portals."Accessed: Nov.13, 2023. [Online]. Available: https://users.encs.concordia.ca/~mmannan/publications/cpinspector-dpm2019.pdf

[2] I. Dolińska and A. Masiukiewicz, "Wireless technologies and application," AFiBV Publishing (in Polish), 2013.

[3] Aruba White Paper, "802.11ac technology, Chapter I: Introduction and technology overview," Aruba Networks Inc. 2012.

[4] Vattapparamban, E., C¸ iftler, S., G¨uven¸c, I., Akkaya, K., Kadri, A.: Indoor occupancy tracking in smart buildings using passive sniffing of probe requests. In: 2016 IEEE International Conference on Communications Workshops (ICC), pp. 38–44 (2016).

[5] Caneill, M. and Gilis, J. (2010). Attacks against the WiFi protocols WEP and WPA. [online] Pdfs.semanticscholar.org. Available: https://pdfs.semanticscholar.org/ebf5/defff09c27fd77421c32a176ecc05cd73983.pdf [Accessed 3 Dec. 2019].

[6] Atkinson, S., Mitchell, E., Rio, M., Matich, G.: Your WiFi is leaking: what do your mobile apps gossip about you? Future Gener. Comput. Syst. 80, 546–557 (2018).

[7] Sidiropoulos, N. and Mioduszewski, M. (2012). Open Wifi SSID Broadcast vulnerability. [online] Os3.nl. Available: https://www.os3.nl/_media/2012-2013/courses/ssn/open_wifi_ssid_broadcast_vulnerability.pdf [Accessed 3 Dec. 2019].

[8] Cheng, N., Wang, X., Cheng, W., Mohapatra, P. and Seneviratne, A. (2013). Characterizing privacy leakage of public WiFi networks for users on travel. [online] Available: https://www.researchgate.net/profile/Aruna_Seneviratne/publication/261__060472_Characterizing_privacy_leakage_of_public_WiFi_networks_for_users_on_travel/links/560e32d008ae2aa0be4a8265/Characterizingprivacy-leakage-of-public-WiFi-networks-for-users-on-travel.pdf [Accessed 3 Dec. 2019].

[9] V. Tarykin and V. Podvornyi, "Security threats in Wi-Fi networks," *International Research Journal of Advanced Engineering and Science*, vol. 1, no. 3, pp. 6–11, 2016, Accessed: Dec. 04, 2023. [Online]. Available: https://irjaes.com/wp-content/uploads/2020/10/IRJAES-V1N3P60Y16.pdf

[10] Sombatruang, N., Kadobayashi, Y., Sasse, M., Baddeley, M., Miyamoto, D.: The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1–11 (2018).

[11] Klasnja, P., Consolvo, S., Jung, J., Greenstein, M., LeGrand, L., Powledge, P., Wetherall, D.:When I am on Wi-Fi, I am fearless privacy concerns & practices in eeryday Wi-Fi use. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 1993–2002 (2009).

[12] "Common Vulnerabilities and Exposures List," https://cve.mitre.org/ , accessed: 2016-01-31.

[13] "WiFi Master Key hits 800M users," http://www.mobileworldlive.com/apps/news-apps/wifi-master-key-hits-800m-users/, accessed: 2016-05-10.

[14] R. Tang et al., “How Vulnerable Is the Public WiFi AP You Are Using?” Available: https://netman.aiops.org/wp-content/uploads/2017/05/PID1194354.pdf
[15] Sombatruang, N., Sasse, A., Baddeley, M.: Why do people use unsecure public Wi- Fi? An investigation of behaviour and factors driving decisions. In: Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, pp. 61–72 (2016)
[16] Klein, A., Pinkas, B.: DNS cache-based user tracking. In: Network and Distributed System Security Symposium (NDSS’19). San Diego, CA, USA (Feb 2019)
[17] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey", Future Internet, vol. 11, no. 4, pp. 89, 2019.
[18] I. Hossain, M. M. Hasan, S. Faisal Hasan and M. R. Karim, "A study of security awareness in Dhaka city using a portable WiFi pentesting device," 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), Dhaka, Bangladesh, 2019, pp. 1-6, doi: 10.1109/ICIET48527.2019.9290589.
[19] A. R. Lubis, F. Fachrizal, M. Lubis and H. M. Tahir, "Wireless service at Public University: A survey of users perception on security aspects", 2018 International Conference on Information and Communications Technology (ICOIACT), pp. 78-83, 2018.
[20] J. Adams, “WiFiCue: Public Wireless Access Security Assessment Tool,” SSRN Electronic Journal, 2023, doi: https://doi.org/10.2139/ssrn.4635997.
[21] By Ansari. S, Rajeev, S.G., Chandrasekhar, H.S. Packet sniffing: a brief introduction, IEEE Jan 2003
[22] Jie Yang ,Yingying Chen , W. Trappe , J. Cheng, Detection and Localization of Multiple Spoofing Attackers in Wireless Networks, IEEE Issue No.01 - Jan. (2013 vol.24)
[23] Kumar.V, Three Tier Verification Technique to foil session sidejacking attempts, IEEE Nov.2011
[24] Srilasak, S., Wongthavarawat, K.,and Phonphoem A, Integrated Wireless Rogue Access Point Detection and Counterattack System, IEEE April 2008
[25] Gonzales.H , Bauer.K, Lindqvist.J,McCoy.D, Practical Defenses for Evil Twin Attacks in 802.11, IEEE Dec. 2010
[26]“Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux | IEEE Conference Publication | IEEE Xplore,” ieeexplore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9099187&tag=1 (accessed Dec. 09, 2023).