Τεχνολογικό Πανεπιστήμιο Κύπρου

Τμήμα Επικοινωνίας και Σπουδών Διαδικτύου

Αλμπέρτο Μπούλλο

Πτυχιακή εργασία

"Ασύρματα οικιακά δίκτυα στην Κύπρο και η ασφάλεια τους"

Πτυχιακή εργασία: Αλμπέρτο Μπούλλο

Πνευματικά δικαιώματα

Copyright © Αλμπέρτο Μπούλλο, 2012
Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Επικοινωνίας και Σπουδών Διαδικτύου του Τεχνολογικού Πανεπιστημίου Κύπρου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος

Περιεχόμενα

Κατάλογος Εικόνων / Διαγραμμάτων

Εισαγωγή

Το πλήθος των οικιακών ασυρμάτων δικτύων αυξάνεται ραγδαία ως αποτέλεσμα της εξέλιξης των φορητών ηλεκτρονικών συσκευών όπως τα smart phones, οι κάμερες ασφαλείας, τα ασύρματα τηλέφωνα, ηχεία, και παιχνιδομηχανές (consoles όπως xbox, playstation), οι φορητοί υπολογιστές κάθε μορφής (laptops, netbooks, tablets) και άλλα πολλά. Οι συσκευές αυτές μπορούν να χρησιμοποιούν υπηρεσίες που προέρχονται από τον Παγκόσμιο Ιστό ή από ένα τοπικό δίκτυο υπολογιστών και για ευκολία χρήσης τους προτυποποιήθηκε η ασύρματη δικτύωση τους και, κατά συνέπεια, η δυνατότητα σύνδεσης τους στο Διαδίκτυο.

Η ασύρματη δικτύωση, από την άλλη πλευρά, με την εξέλιξη της έφερε στην αγορά διάφορα προϊόντα που καθιστούν εύκολη την επικοινωνία μεταξύ τέτοιων συσκευών. Η βάση της επικοινωνίας αυτής είναι ο δρομολογητής (router) ή για την ακρίβεια διαμορφωτής / αποδιαμορφωτής (modem) με δυνατότητες δρομολόγησης πακέτων δεδομένων ώστε να καθίσταται εφικτή η δημιουργία ασύρματου οικιακού δικτύου υπολογιστών (για την ακρίβεια ασύρματου οικιακού δικτύου ηλεκτρονικών συσκευών).

Σήμερα οι περισσότερες εταιρίες Παροχής Υπηρεσιών Διαδικτύου (ISP – Internet Service Provider) αναγνωρίζοντας τη σημασία της ασύρματης οικιακής δικτύωσης παρέχουν δωρεάν δρομολογητές. Με τη σύναψη συμβολαίου με μια τέτοια εταιρία, η εταιρία αναλαμβάνει την εγκατάσταση του τοπικού ή/και ασυρμάτου δικτύου μέσω της συσκευής δρομολόγησης (modem ή router) στην οικία του συνδρομητή. Ως αποτέλεσμα κάθε συνδρομητής μπορεί να συνδέσει κάθε συσκευή στο δίκτυο, είτε ενσύρματα μέσω κάποιου καλωδίου, είτε ασύρματα μέσω του Σημείου Πρόσβασης (AP – access point) που δημιουργεί ο ασύρματος δρομολογητής (wireless router).

Περιγραφή προβλήματος

Όταν οι συνδρομητές δημιουργούν ασύρματη δικτύωση στο σπίτι τους μπορεί να μην αντιλαμβάνονται ένα από τα πιο μεγάλα προβλήματα που αυτή δημιουργεί: την ασφάλεια τους. Τα σήματα των οικιακών ασυρμάτων δικτύων δεν σταματούν στους τοίχους του σπιτιού μας. Οποιοσδήποτε μπορεί να "δει" το ασύρματο δίκτυο μας και γι' αυτό πρέπει να έχουμε κάποιο είδος ελέγχου σε αυτό κυρίως όσον αφορά την σύνδεση σε αυτό ανεπιθύμητων χρηστών μέσω δικών τους ασύρματων συσκευών.

Υπάρχουν πολλοί τρόποι να αυξηθεί η ασφάλεια ενός τοπικού ασύρματου δικτύου και οι εταιρίες τηλεπικοινωνιών, αλλά και η διεθνής επιστημονική κοινότητα, έχουν αφιερώσει χρόνο για να κάνουν τα ασύρματα τοπικά δίκτυα ασφαλή. Με την ραγδαία εξάπλωση των οικιακών ασύρματων δικτύων προκύπτει αφενός η ανάγκη να υπάρχει ασφάλεια πρόσβασης σε αυτά και αφετέρου να είναι οι χρήστες ενήμεροι όσον αναφορά τα ζητήματα ασφάλειας του τοπικού τους δικτύου. Οι εταιρίες που παρέχουν υπηρεσίες σύνδεσης στο Διαδίκτυο πολλές φορές δεν δίνουν τις απαραίτητες πληροφορίες στους συνδρομητές τους για τα θέματα ασφάλειας και έτσι σε πολλές περιπτώσεις τα οικιακά ασύρματα τοπικά δίκτυα μένουν ευάλωτα σε επιθέσεις χωρίς οι συνδρομητές να το γνωρίζουν.

Τα δεδομένα στα ασύρματα δίκτυα μεταφέρονται μέσω ραδιοκυμάτων στον αέρα (beacon frames). Στην περίπτωση που το ασύρματο δίκτυο επεκτείνεται (κάνει broadcast το AP) εκτός του σπιτιού μας, οποιοσδήποτε μπορεί να συνδεθεί σε αυτό έστω και αν βρίσκεται εκτός της οικίας μας. Αυτό είναι ισοδύναμο με το να συνδέσει ένα καλώδιο δικτύου (Ethernet) στον δρομολογητή μας. Έτσι μπορεί μέσω να έχει πρόσβαση στο δίκτυο μας και το διαδίκτυο μέσω του δικού μας δρομολογητή. Το πρόβλημα αυτό μπορεί να μην μας ανησυχεί αλλά υπάρχει και συνέπειες τις οποίες δεν έχουμε σκεφτεί: το άτομο που συνδέεται στο δίκτυο μας είναι σαν να βρίσκεται μέσα στην οικία και να «ακούει» (sniff/monitoring) το τι συμβαίνει μέσα στο δίκτυο. Αυτό μπορεί να οδηγήσει σε κλοπή προσωπικών δεδομένων, αλλά, ακόμη χειρότερα, μπορεί το άτομο αυτό να λειτουργεί στο διαδίκτυο σαν να είμαστε εμείς (ο συνδρομητής) αφού η IP (Internet protocol address) δημόσια διεύθυνση του δικτύου μας είναι η ίδια για όλες τις συσκευές που είναι συνδεδεμένες στο δίκτυο μας. Άρα αν ένας χρήστης κάνει κάτι παράνομο στο διαδίκτυο (πχ κατέβασμα παράνομου υλικού) μέσω του δικτύου μας είναι σαν να το κάναμε εμείς αφού δεν υπάρχει τρόπος να διαχωρίζονται οι επιμέρους IP διευθύνσεις εντός του τοπικού μας δικτύου (LAN) αν δεν υπάρχει πρόσβαση στο δρομολογητή (router). Βλέποντας την δημόσια IP διεύθυνση "βλέπουν" την οικία ή αλλιώς τον συνδρομητή που κατέχει το δίκτυο. Το πιο πάνω είναι μόνο ένα παράδειγμα το τι μπορεί να συμβεί αν δεν είναι ασφαλές το δίκτυο μας.

Υπάρχουν πολλοί τρόποι αντιμετώπισης των προβλημάτων αυτών αλλά ο οι γνώσεις των χρηστών για τα θέματα ασφάλειας ποικίλουν. Έτσι σε πολλές περιπτώσεις δεν λαμβάνονται σωστά μέτρα για να ασφαλιστεί το οικιακό ασύρματο δίκτυο.

Αναγκαιότητα μελέτης

Έχουν γίνει μελέτες όσον αφορά την ασφάλεια των οικιακών ασυρμάτων δικτύου σε διάφορες χώρες. Αυτό που ελέγχεται είναι κατά πόσο σε μια περιοχή ή σε όλη την επικράτεια είναι ασφαλή τα ασύρματα δίκτυα. Στην παρούσα μελέτη διερεύνησα το βαθμό ασφάλειας των οικιακών ασυρμάτων δικτύων στη Λεμεσό ώστε να έχουμε μια εικόνα της κατάστασης στην Κύπρο, καθώς δεν συντρέχει κάποιος λόγος η κατάσταση να είναι διαφορετική σε άλλες πόλεις της Κύπρου ή στην ύπαιθρο.

Ο έλεγχος έγινε μέσω λογισμικού που παρατηρεί τα H/M (ηλεκτρομαγνητικά) κύματα (στις συχνότητες του ασύρματου δικτύου) στον αέρα και βρίσκει οποιοδήποτε AP (access point) υπάρχει στην περιοχή. Καταγράφτηκαν κάποιες επιπρόσθετες πληροφορίες για αντιπαραβολή με αντίστοιχες μελέτες στο εξωτερικό. Τα δεδομένα που πήραμε αποθηκεύτηκαν σε βάση δεδομένων για να μελετηθούν μέσω στατιστικών προγραμμάτων όπως το SPSS.

Στην Κύπρο δεν υπάρχουν επαρκείς πληροφορίες για την ασφάλεια των οικιακών ασυρμάτων δικτύων καθώς δεν έχουν γίνει συγκεκριμένες μελέτες στο συγκεκριμένο αντικείμενο. Η μόνη προσπάθεια που έχει γίνει είναι από ένα ξένο ερευνητή ασφάλειας από την εταιρία Kaspersky, τον Dmitry Bestuzhev ο οποίος έχει κάνει ένα “wifi study” όταν ήρθε στην Λεμεσό το 2010 [4]. Κάτι παρόμοιο με αυτό έχω κάνει στην παρούσα πτυχιακή όσον αφορά το τεχνικό κομμάτι ελέγχου της ασφάλειας των οικιακών ασυρμάτων δικτύων. Ο Bestuzhev έχει πάρει τις πληροφορίες μέσω αναζήτησης γυρνώντας την πόλη και παρατηρώντας τα σήματα wifi. Στην συνέχεια δημιούργησε κυκλικά διαγράμματα όπου παρουσίασε τα αποτελέσματα της ερευνάς του. Ένα ενδιαφέρον κομμάτι της πτυχιακής μου αφορούσε τη σύγκριση με τα αποτελέσματα που πήρε ο Bestuzhev. Έτσι έχουμε στοιχεία από το 2010 και το 2012 και μπορέσαμε να κάνουμε συγκρίσεις αλλά και γενικεύσεις καθώς και παρακολούθηση της διαχρονικής εξέλιξης του συγκεκριμένου θέματος. Δυστυχώς μετά από επικοινωνία μαζί του δεν μπόρεσε να μας δώσει τα files με τα δεδομένα (για να υπάρχει περισσότερη πληροφορία για το 2010), έτσι περιορίστηκα στα αποτελέσματα που έχει αναρτήσει στο blog της σελίδας του Kaspersky lab [4].

Είναι σημαντικό να γίνει μια αρχική προσπάθεια να πάρουμε τις πληροφορίες που χρειαζόμαστε και να τις συγκρίνουμε με αντίστοιχες προηγούμενες ή μελλοντικές τέτοιες μελέτες. Σε άλλες χώρες συγκεντρώνονται αρχεία κάθε χρόνο και με αποτέλεσμα να έχουμε διαχρονικές συγκρίσεις.

Εκτός από το τεχνικό θέμα με την αυτόματη συλλογή πληροφοριών κατασκευάστηκε και ένα μικρό ερωτηματολόγιο που δόθηκε σε τυχαίους συνδρομητές μέσω της μεθόδου χιονοστιβάδας. Το ερωτηματολόγιο περιλαμβάνει βασικά ερωτήματα για να μπορούμε να έχουμε μία γενικότερη εικόνα για τις γνώσεις που έχουν τα άτομα (συνδρομητές) όσον αφορά την ασφάλεια των ασυρμάτων δικτύων. Ο στόχος ήταν αφενός να ελεγχθούν κάποιες ερευνητικές υποθέσεις αλλά και να γίνει διασταύρωση των αποτελεσμάτων με τα

αποτελέσματα της τεχνικής μελέτης. Αυτό είναι σημαντικό για να μπορούμε να επιβεβαιώσουμε μερικές υποθέσεις που έχουμε ήδη κάνει.

Τέλος έχει γίνει προσπάθεια να μελετηθεί η στρατηγική κάθε εταιρίας (ISP) ως προς το θέμα οικιακής ασφάλειας των συνδρομητών, δηλαδή κατά πόσο οι εταιρίες αυτές προσφέρουν συσκευές οι οποίες είναι ασφαλείς χωρίς να χρειαστεί ένας χρήστης να κάνει αλλαγές. Δυστυχώς ή ευτυχώς η ασφάλεια του οικιακού ασυρμάτου δικτύου εξαρτάται σε μεγάλο βαθμό από αυτούς (ISPs).

Φιλοδοξούμε η παρούσα μελέτη να αποτελέσει την απαρχή προβληματισμού για τις εταιρείες ISP όσον αφορά την ασφάλεια των οικιακών ασυρμάτων δικτύων, διότι, όπως θα δούμε στη συνέχεια το θέμα της ασφάλειας είναι υπαρκτό και δυστυχώς οι εν λόγω εταιρείες δεν είναι άμοιρες ευθυνών.

Ερευνητικά ερωτήματα/υποθέσεις εργασίας

Η παρούσα μελέτη περιλαμβάνει τρεις υποθέσεις εργασίας:

- Οι Κύπριοι δεν λαμβάνουν μέτρα προστασίας για την ασφάλεια των ασύρματων οικιακών τους δικτύων.
- Οι εταιρίες (ISP) υπηρεσιών διαδικτύου δεν λαμβάνουν τα ενδεικνυόμενα μέτρα προστασίας των ασύρματων δικτύων των συνδρομητών τους αλλά ούτε και τους ενημερώνουν επαρκώς για τα θέματα ασφαλείας των δικτύων αυτών.
- Τα οικιακά ασύρματα δίκτυα στην Κύπρο δεν είναι αρκετά ασφαλή και μένουν ευάλωτα σε επιθέσεις.

Θα μπορούσαμε να διατυπώσουμε την υπόθεση με μία πρόταση.

- Οι Κύπριοι δεν λαμβάνουν μέτρα προστασίας των ασύρματων δικτύων και οι εταιρίες ακόμη δεν έχουν λάβει δραστικά μέτρα.

Θεωρητικό υπόβαθρο

Ένα βασικό μέρος της εργασίας μου είναι η αναζήτηση και η συλλογή δεδομένων και πληροφοριών που διακινούνται στην ατμόσφαιρα στις συχνότητες των ασυρμάτων δικτύων. Η μέθοδος αυτή έχει ήδη χρησιμοποιηθεί στο εξωτερικό από διάφορες ερευνητές. Τα δεδομένα που συλλέγονται καταχωρούνται σε βάσεις δεδομένων και συμπληρώνονται με επιπρόσθετες πληροφορίες όπως η τοποθεσία του ασυρμάτου δικτύου (GPS συντεταγμένες) για να μπορούν να παρουσιαστούν σε ένα χάρτη. Με τον τρόπο αυτό υπάρχει συνεχής εικόνα όσον αφορά την κατάσταση των ασυρμάτων δικτύων σε μια περιοχή. Η μεθοδολογία αυτή ξεκίνησε ως hobby και ονομάζεται Wardriving [6]. Σε διάφορες χώρες όλες αυτές οι πληροφορίες καταχωρούνται σε ιστοσελίδες και δημιουργούνται ετήσια στατιστικά για να υπάρχει διαχρονική παρακολούθηση (WiGLE – Wireless Geographic Logging Engine)[1].

Στην παρούσα μελέτη προσπάθησα να συλλέξω στοιχεία για την Κύπρο και ταυτόχρονα να τα συγκρίνω με αντίστοιχες μελέτες που έγιναν για αυτό το θέμα στο παρελθόν στην Κύπρο. Η μόνη έρευνα που βρήκα ήταν του ερευνητή ασφάλειας από την εταιρία Kaspersky, Dmitry Bestuzhev [4] ο οποίος έχει αναρτήσει στο blog του κυκλικά διαγράμματα με τις πληροφορίες που βρήκε στην Λεμεσό το 2010. Τα δεδομένα αυτά και τα τελικά του συμπεράσματα αν και όχι τόσο λεπτομερή βοήθησαν την έρευνα μου στο να γίνει σύγκριση με την περίοδο εκείνη και να δούμε την εξέλιξη του θέματος "ασφάλεια οικιακών ασυρμάτων δικτύων".

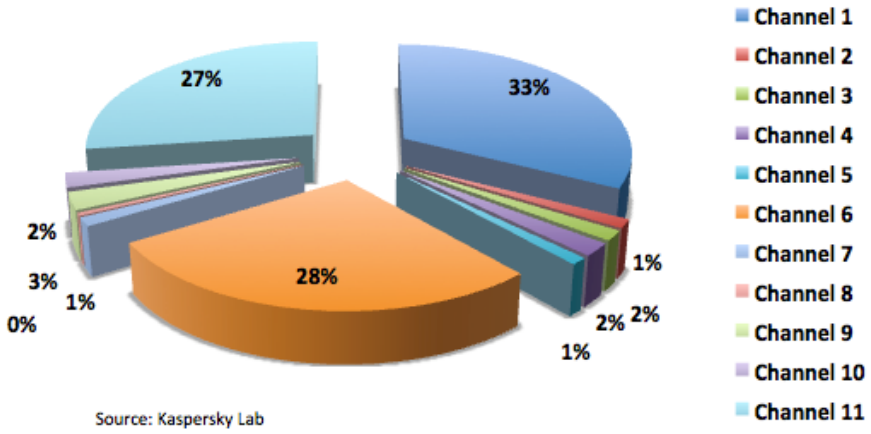


Image from: http://www.securelist.com/en/blog/2186/SAS2010_Wardriving_in_Limassol_Cyprus

Εικόνα 1: Ποσοστό χρήσης των τηλεπικοινωνιακών καναλιών στα οικιακά ασύρματα δίκτυα σύμφωνα με την έρευνα του Bestuzhev [4]

---

[1] *http://wigle.net/gps/gps/main/faq/*

Στην Εικόνα 1 βλέπουμε ένα από τα διαγράμματα που παρουσίασε ο Bestuzhev το οποίο αφορά τη χρήση των επιμέρους τηλεπικοινωνιακών καναλιών στα ασύρματα δίκτυα στη Λεμεσό. Όπως θα δούμε στη συνέχεια η χρήση των επιμέρους τηλεπικοινωνιακών καναλιών στα ασύρματα δίκτυα απεικονίζει την ικανότητα των ιδιοκτητών τους να αλλάζουν τις εκ των προτέρων (default) ρυθμίσεις του δρομολογητή τους και κατά συνέπεια την ικανότητα τους να ασφαλίζουν το δίκτυο τους.

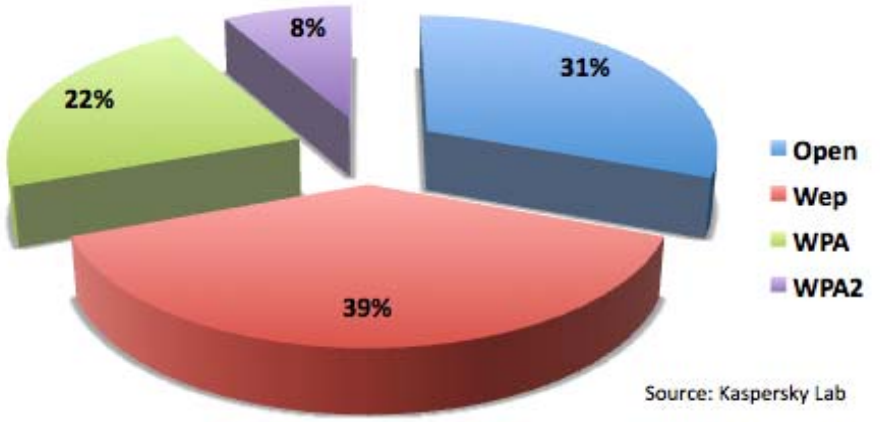


Image from: http://www.securelist.com/en/blog/2186/SAS2010_Wardriving_in_Limassol_Cyprus

Εικόνα 2: Μέθοδοι / πρωτόκολλα προστασίας που χρησιμοποιούνται στα ασύρματα οικιακά δίκτυα σύμφωνα με την έρευνα του Bestuzhev [4]

Στην Εικόνα 2 βλέπουμε ένα ακόμη από τα διαγράμματα που παρουσίασε ο Bestuzhev. Αφορά τη χρήση μεθόδων / πρωτοκόλλων ασφαλείας στα ασύρματα δίκτυα. Τα πρωτόκολλα ασφαλείας είναι η βασική μέθοδος προστασίας από μη εξουσιοδοτημένη πρόσβαση στα ασύρματα δίκτυα. Το ποιο πρωτόκολλο χρησιμοποιείται και με ποιες ρυθμίσεις αντανακλά το επίπεδο ασφάλειας του ασυρμάτου δικτύου. Περισσότερα για τα πρωτόκολλα προστασίας των ασυρμάτων δικτύων θα δούμε στην επόμενη ενότητα.

Θεωρητικό πλαίσιο

Στην ενότητα αυτή κάνουμε μια σύντομη παρουσίαση / ανασκόπηση των τεχνολογιών και των ορολογιών που σχετίζονται με το αντικείμενο της παρούσας μελέτης.

Wardriving

Wardriving ονομάζεται η συλλογή δεδομένων που βρίσκονται στον αέρα για να μπορέσουμε να ελέγξουμε συγκεκριμένες πληροφορίες που μας ενδιαφέρουν. Η χρήση του Wardriving στις συχνότητες λειτουργίας των ασυρμάτων δικτύων μας επιτρέπει να έχουμε άμεση γνώση για την ασφάλεια και τα προβλήματα των ασυρμάτων δικτύων στην περιοχή που ελέγχουμε. Μπορούμε επίσης να καταχωρήσουμε τις πληροφορίες αυτές σε ένα χάρτη (πχ Google maps) με πληροφορίες για κάθε ασύρματο δίκτυο που βρίσκουμε στην περιοχή. Ενδεικτικές πληροφορίες τέτοιου είδους είναι το SSID (δηλαδή το όνομα του Σημείου Πρόσβασης – Access Point), το τηλεπικοινωνιακό κανάλι το οποίο χρησιμοποιείται για την ανταλλαγή δεδομένων ανάμεσα στο Access Point και τις ασύρματες συσκευές που συνδέονται σε αυτό, αν χρησιμοποιεί κάποιο πρωτόκολλο ασφάλειας κτλ [6].

Access Point (AP)

Ένα Access Point (AP) δίνει και λαμβάνει δεδομένα μέσω ασύρματης επικοινωνίας σε οποιαδήποτε συσκευή είναι συνδεδεμένη σε αυτό. Στην πράξη το access point είναι ένας ασύρματος δρομολογητής με περιορισμένες δυνατότητες. Σε αντίθεση με τους ασύρματους δρομολογητές δεν προσφέρει προσφέρει λειτουργίες φραγής (firewall), δημιουργίας ιδιωτικού εικονικού δικτύου (VPN) κτλ. Ο πραγματικός σκοπός ενός AP είναι να διαμεσολαβεί την επικοινωνία μεταξύ ανάμεσα στις συσκευές του ασύρματου δικτύου. Λειτουργεί επομένως με την ίδια λογική όπως το hub στα ενσύρματα δίκτυα. Επομένως το AP δεν είναι απαραίτητο για τη δημιουργία τοπικού δικτύου ούτε και για τη σύνδεση μας στο Διαδίκτυο καθώς και τα δύο μπορούν να επιτευχθούν με ενσύρματο τρόπο[2].

Service Set Identifier (SSID)

SSID είναι το συμβολικό όνομα που δίνουμε στο ασύρματο δίκτυο μας. Για την ακρίβεια είναι το όνομα που δίνουμε στο Access Point. Μας βοηθά να ξεχωρίζουμε τα ασύρματα δίκτυα μεταξύ τους όταν τα αναζητούμε. Το SSID όμως δεν είναι μοναδικό για κάθε δίκτυο. Μπορεί να βρούμε, για παράδειγμα, 20 Wi-Fi δίκτυα με το όνομα “Linksys”. Μία από τις δυνατότητες που μας δίνουν οι κατασκευαστές είναι να μην κάνουμε broadcast (ανοικτή αναμετάδοση) το SSID ως μέτρο προστασίας πρόσβασης [5, p.52].

---

[2] http://support.netgear.com/app/answers/detail/a_id/235/~/what-is-an-access-point%3F

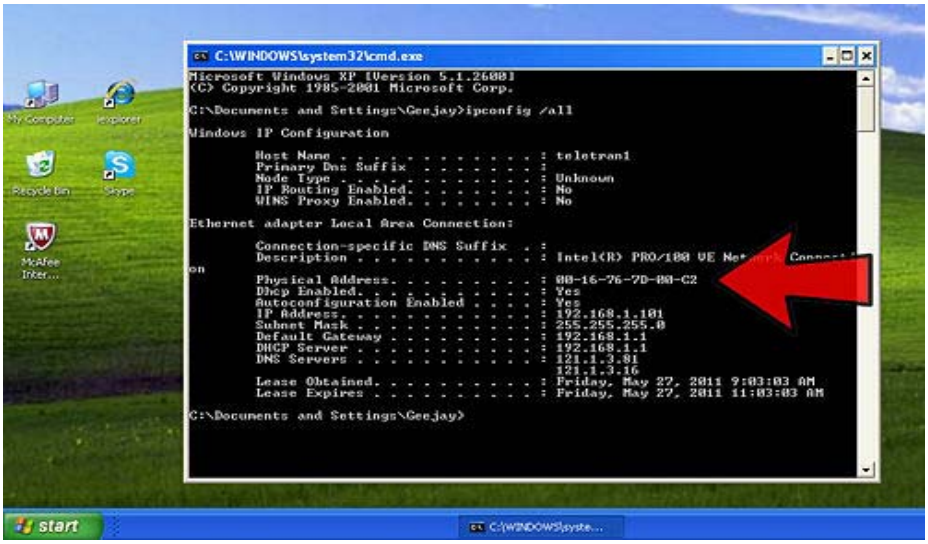
Ad-hoc σύνδεση

Ad-hoc ονομάζουμε τις συνδέσεις μεταξύ συσκευών χωρίς την παρουσία διαμεσολαβητή (για παράδειγμα σύνδεση PC και printer). Είναι συνήθως συνδέσεις 1:1 και στα ασύρματα δίκτυα πραγματοποιούνται χωρίς τη διαμεσολάβηση του AP ενώ στα ενσύρματα χωρίς τη διαμεσολάβηση του hub. Οι ad-hoc συνδέσεις δεν απαιτούν περίπλοκες εγκαταστάσεις, ρυθμίσεις ή εξοπλισμό. Τυπικά παραδείγματα ασύρματων ad-hoc συνδέσεων είναι οι συνδέσεις με χρήση του πρωτοκόλλου Bluetooth[3].

Machine Address Code (MAC address)

Το Machine Address Code η απλά MAC address είναι μία δωδεκαψήφια μοναδική τιμή καταχωρημένη σε κάθε συσκευή ή υλικό που μπορεί να συνδεθεί σε ένα τοπικό δίκτυο (ενσύρματο ή ασύρματο) και βοηθά στο να ξεχωρίζουμε τις συσκευές μεταξύ τους. Τα κινητά τηλέφωνα, για παράδειγμα, που υποστηρίζουν Wi-Fi σύνδεση έχουν μια ξεχωριστή MAC address όπως κάθε άλλη συσκευή με δυνατότητες ασύρματης δικτύωσης μέσω Wi-Fi. Τα πρώτα έξι ψηφία του MAC προσδιορίζουν τον κατασκευαστή της συσκευής και τα άλλα έξι αντιστοιχούν στο σειριακό αριθμό (serial number) που καταχωρεί κάθε κατασκευαστής στις συσκευές του [3].

Στην Εικόνα 3 βλέπουμε πως μπορούμε να εντοπίσουμε την MAC address της κάρτας δικτύου του υπολογιστή μας σε περιβάλλον Windows. Όπως μπορείτε να δείτε η MAC address αναφέρεται και ως Physical Address διότι σχετίζεται με το υλικό και δεν είναι κάτι που μπορούμε εμείς να τροποποιήσουμε (όπως για παράδειγμα μπορεί να συμβεί με την IP address).



Εικόνα 3: Εντοπισμός της MAC address σε υπολογιστή με λειτουργικό σύστημα Windows (run =>cmd => ipconfig /all)

[3] *http://support.netgear.com/app/answers/detail/a_id/954/~/selecting-between-infrastructure-and-ad-hoc-wireless-modes*

Ασύρματο δίκτυο – WLAN:

Ένα ασύρματο τοπικό δίκτυο (WLAN – Wireless Local Area Network) λειτουργικά δεν διαφέρει και από ένα ενσύρματο. Αμφότερα έχουν σκοπό να καταστήσουν εφικτή την επικοινωνία πολλών συσκευών που είναι εφοδιασμένες με κάρτα δικτύου. Ενσύρματο δίκτυο χρησιμοποιείται όταν χρειάζεται μεγαλύτερη ταχύτητα και αξιοπιστία στην ανταλλαγή δεδομένων μεταξύ των συσκευών, αφού οι ταχύτητες στα ασύρματα δίκτυα συνήθως δεν επαρκούν για υψηλούς ρυθμούς μετάδοσης όπως απαιτείται π.χ. για μεταφορά βίντεο υψηλής ποιότητας δε πραγματικό χρόνο ή για rendering τρισδιάστατων σκηνών (όπως συμβαίνει για δικτυακά παιχνίδια υψηλής προσομοίωσης). Η θεωρητική ταχύτητα ενός ασύρματου δικτύου μπορεί να είναι σχετικά μεγάλη (όπως για παράδειγμα το πρότυπο 802.11g το οποίο λειτουργεί στα 54 Mbit/s) αλλά στην πράξη η ταχύτητα μετάδοσης είναι μικρότερη καθώς επηρεάζεται από τις συνθήκες της ατμόσφαιρας και τα φυσικά εμπόδια. Άλλη μια σημαντική διαφορά ανάμεσα στα ενσύρματα και ασύρματα δίκτυα είναι το πως μεταδίδεται η πληροφορία. Στα ενσύρματα δίκτυα οι συσκευές είναι συνδεδεμένες μέσω καλωδίων (cat 6 κτλ) Ethernet και hubs (switches) και η μετάδοση γίνεται στη βασική συχνότητα των δεδομένων (χωρίς διαμόρφωση) ενώ στα ασύρματα δίκτυα η πληροφορία μεταδίδεται με διαμόρφωση στις συχνότητες ραδιοκυμάτων (radio spectrum) όπως συμβαίνει με τη μετάδοση ραδιοφωνικών και τηλεοπτικών σημάτων. Κάθε χώρα έχει δώσει συγκεκριμένες συχνότητες (radio wave spectrum) οι οποίες χρησιμοποιούνται για τα ασύρματα δίκτυα (συνήθως χρησιμοποιούνται οι συχνότητες 2.4Ghz και 5GHZ). Η απαίτηση για καλώδια καθιστά τα ενσύρματα τοπικά δίκτυα λιγότερο ελκυστικά εκτός και αν υπάρχει πρόβλεψη για εντοιχισμένη καλωδίωση εξαρχής. Ακόμη όμως και σε αυτή την περίπτωση η ανάγκη για σύνδεση στο τοπικό δίκτυο (αλλά και το διαδίκτυο) μέσω φορητών συσκευών όπως smart phones καθιστά την χρήση του ασύρματου δικτύου ελκυστική.

Εξαιτίας της ασύρματης επικοινωνίας μέσω ραδιοσυχνοτήτων η ασύρματη δικτύωση αποκαλείται και Wi-Fi (η αλλιώς wireless fidelity) δικτύωση. Τα πρότυπα τα οποία χρησιμοποιούμε σήμερα για ασύρματη δικτύωση ελέγχονται από τον οργανισμό WiFi Alliance που παρέχει την πιστοποίηση για τα προϊόντα που πληρούν τις προδιαγραφές του 802.11 (δες κατωτέρω).

Πρότυπα 802.11

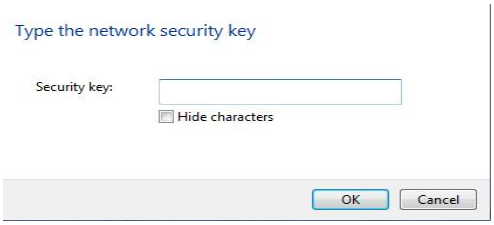
Η σειρά προτύπων 802.11 έχει δημιουργηθεί από την IEEE (Institute of Electrical and Electronic Engineering) και χρησιμοποιείται μέχρι σήμερα για τη προτυποποίηση της ασύρματης δικτύωσης συσκευών μέσω των Wi-Fi συχνοτήτων όπως η σειρά προτύπων IEEE 802.3 περιγράφει την ενσύρματη επικοινωνία συσκευών σε τοπικά δίκτυα. Όσες συσκευές υποστηρίζουν το πρότυπο 802.11, ανεξάρτητα από τον κατασκευαστή τους, έχουν τη δυνατότητα να συνδεθούν μεταξύ τους ασύρματα. Το πρότυπο 802.11 αποτελείται από μια σειρά πρωτοκόλλων. Η πρώτη έκδοση του προτύπου που χρησιμοποιήθηκε εμπορικά είναι το 802.11b το οποίο εξακολουθεί, αν και σπάνια, να χρησιμοποιείται μέχρι σήμερα.

Το 802.11b δημιουργήθηκε το 1999 και έχει την ιδιότητα να μοιράζει μέσω της DSSS (Direct-Sequence Spread Spectrum) λειτουργίας διάφορα «κανάλια» (channel), δηλαδή συχνότητες, περί την κεντρική διαθέσιμη συχνότητα ραδιοκυμάτων (2.4GHz ή 5 Ghz). Κάθε χώρα έχει προσδιορισμένα κανάλια, π.χ. στην Αμερική μπορούμε να χρησιμοποιήσουμε τα κανάλια 1 μέχρι 11, σε χώρες της Ευρωπαϊκής Ένωσης μπορούμε να χρησιμοποιήσουμε μέχρι το κανάλι 13 και στην Ιαπωνία μπορούν μέχρι το 14. Όλα τα κανάλια αυτά μπορούν να χρησιμοποιηθούν χωρίς άδεια νοουμένου ότι χρησιμοποιούνται για προσωπικό σκοπό. Η ονομαστική ταχύτητα του 802.11b είναι 11Mbps αλλά σε πραγματικές συνθήκες λειτουργίας η ταχύτητα είναι περίπου 5Mbps. Τέτοια ταχύτητα είναι ανεπαρκής για διανομή HD (High definition) video, για παράδειγμα μέσω του YouTube. Την ίδια χρονιά δημιουργήθηκε το 802.11a το οποίο χρησιμοποιούσε ψηλότερη συχνότητα (5GHz) αντί της συνηθισμένης 2.4GHz. Το πρότυπο αυτό είχε το πλεονέκτημα ότι χρησιμοποιούσε φάσμα λιγότερο δημοφιλές (μπορεί να υπάρξει αλλοίωση της ποιότητας του σήματος όταν υπάρχουν πολλά σήματα που εκπέμπονται στο ίδιο φάσμα) αλλά έχει το μειονέκτημα ότι όσο μεγαλύτερη συχνότητα χρησιμοποιείται τόσο περισσότερες απώλειες (λόγω απορ-ρόφησης από φυσικά εμπόδια) υπάρχουν άρα η εμβέλεια σε δεδομένη ισχύ είναι μικρότερη. Αντί να καλύπτει για παράδειγμα όλο το σπίτι και την αυλή του η εμβέλεια του μπορεί να περιορίζεται μόνο εντός του σπιτιού εξαιτίας των πολλαπλών εμποδίων που συναντά (τοίχοι, έπιπλα, κλπ). Το 802.11a έχει ονομαστική ταχύτητα μετάδοσης 54Mbps (σε πραγματικές συνθήκες περίπου 23Mbps) η οποία είναι υπέρ-αρκετή για χρήση σε ένα οικιακό ασύρματο δίκτυο. Ο λόγος που δεν έγινε τόσο εμπορικό είναι η έλλειψη συμβατότητας με τις περισσότερες συσκευές με δυνατότητα δικτύωσης που υπάρχουν στην αγορά και οι οποίες λειτουργούν στα 2.4GHz και χρησιμοποιούν το πρότυπο 802.11b και 802.11g. Θα πρέπει να αναφέρουμε ότι συσκευές που χρησιμοποιούν το πρότυπο 802.11g μπορεί να λειτουργήσουν με συσκευές που διαθέτουν 802.11b. Για παράδειγμα ένα AP (access point) το οποίο κάνει broadcasting χρησιμοποιώντας το πρότυπο 802.11g έχει την δυνατότητα να συνδέεται με συσκευές που χρησιμοποιούν το πρότυπο 802.11b. Ο περιορισμός θα είναι η ταχύτητα η οποία θα είναι 11Mbps στην περίπτωση αυτή.

Σήμερα το πιο διαδεδομένο πρότυπο είναι το 802.11g το οποίο δημιουργήθηκε το 2003 και υποστηρίζει ονομαστική ταχύτητα 54Mbps (σε πραγματικές συνθήκες λειτουργίας η ταχύτητα είναι περίπου 19Mbps), ταχύτητα επαρκή για μετάδοση ήχου και βίντεο σε ροή (streaming - δηλαδή χωρίς να χρειάζεται η τοπική αποθήκευση του αρχείου πρώτα). Το τελευταίο και πιο νέο πρότυπο είναι το 802.11n το οποίο δημιουργήθηκε το 2009. Είναι ακόμη σε δοκιμαστική φάση, δηλαδή δεν έχει τελειοποιηθεί εντελώς αν και υπάρχουν συσκευές στην αγορά. Το πρότυπο αυτό έχει θεωρητική ταχύτητα 600Mbps και υποστηρίζει πολλαπλές μονάδες εισόδου -εξόδου (MIMO), δηλαδή ασύρματες συσκευές με περισσότερες από μια κάρτες δικτύου.

Τα πρότυπα 802.11 δημιουργήθηκαν για προτυποποίηση της ασύρματης επικοινωνίας μεταξύ των συσκευών με σκοπό τη δημιουργία τοπικών δικτύων. Σχεδόν κάθε χρόνο νέες τεχνολογίες και νέα πρωτόκολλα εμφανίζονται για να διορθώσουν μερικά προβλήματα που μπορεί να υπάρχουν σε προηγούμενες εκδόσεις αλλά και να παρέχουν νέες υπηρεσίες

όσον αφορά την ανταλλαγή δεδομένων. Ένα παράδειγμα είναι το QoS (Quality of Service) το οποίο είναι υπεύθυνο να δίνει προτεραιότητα σε συγκεκριμένες μορφές δεδομένων έτσι ώστε να μην υπάρχει καθυστέρηση στην μετάδοση τους [5].



Εικόνα 4: Παράθυρο το οποίο μας ζητά να εισάγουμε το encryption key (ή Security Key όπως αναφέρεται στην εικόνα) για σύνδεση σε ένα ασύρματο δίκτυο.

Encryption Key:

Το encryption key είναι ένα συνθηματικό το οποίο μπορούμε να καθορίσουμε εμείς ώστε μόνα άτομα τα οποία το γνωρίζουν να μπορούν να συνδεθούν στο ασύρματο δίκτυο μας. Το encryption key καθορίζεται μέσα από τις ρυθμίσεις του AP. Όπως κάθε συνθηματικό η δύναμη του εξαρτάται από την πολυπλοκότητα του (δυσκολία να το μαντέψει κάποιος) και την μέθοδο κρυπτογράφησης του, η οποία καθορίζει την ανθεκτικότητα σε απόπειρες εύρεσης του μέσω προγραμμάτων που τρέχουν σε υπολογιστές. Υπάρχουν διάφοροι τύποι κλειδιών που σχετίζονται με διαφορετικά πρωτόκολλα ασφαλείας. Στην ουσία η διαφορά τους είναι ο τρόπος κρυπτογράφησης του συνθηματικού. Τα τρία πιο βασικά και εμπορικά πρωτοκολλά ασφαλείας που χρησιμοποιούνται στα APs και τους ασύρματους δρομολογητές είναι το WEP, το WPA και WPA2.

Wired Equivalent Privacy (WEP) protocol

Το WEP (Wired Equivalent Privacy) ήταν το πρώτο πρωτόκολλο ασφάλειας που δημιουργήθηκε στο πρότυπο 802.11 για τα ασύρματα τοπικά δίκτυα. Εξακολουθεί να χρησιμοποιείται μέχρι σήμερα παρόλο που θεωρείται λιγότερο ασφαλές από τα πρωτόκολλα WAP και WAP2. Το WEP είναι βασισμένο στον αλγόριθμο ασφάλειας RC4 με μυστικό κλειδί 40 bits ή 104 bits μαζί με ένα 24bit Initialisation Vector (IV) για την κρυπτογράφηση του μηνύματος και το checksum – ICV (Integrity Check Value). Ο αλγόριθμος RC4 όμως δεν αποδείχθηκε άτρωτος καθώς επιθέσεις εναντίον του έδειξαν πως μπορεί να αποκρυπτογραφηθεί το κλειδί μέσω συγκέντρωσης μεγάλου αριθμού IV's (Initialisation Vector) [5, p.128]. Η γενική αρχή λειτουργίας του αλγορίθμου RC4 φαίνεται στην Εικόνα 5.

Εικόνα 5: Γενική αρχή κρυπτογράφησης – αποκρυπτογράφησης δεδομένων

WPA

Το WPA (Wi-Fi Protected Access) είναι ένας πρωτόκολλο ασφαλείας με υψηλότερη αξιοπιστία από το WEP. Ο χρήστης μέσω του πρωτοκόλλου TKIP – temporary key integrity protocol έχει την δυνατότητα να εισάγει μία δική του φράση ως κωδικό πρόσβασης και με τη χρήση ενός καλού κωδικού το δίκτυο είναι σχεδόν ασφαλές. Το WPA εκτός από το TKIP χρησιμοποιεί και το AES (Advanced Encryption Standard) πρωτόκολλο το οποίο υπάρχει και στο WPA2 που είναι λιγότερο ευάλωτο από το WPA [5, p. 129].

Wi-Fi channels:

Τα Wi-Fi channels χρησιμοποιούνται από τα ασύρματα δίκτυα για καλύτερη λειτουργία. Μέσω της αλλαγής τηλεπικοινωνιακών καναλιών μπορούμε να χρησιμοποιήσουμε μια εναλλακτική συχνότητα μετάδοσης, περί την κεντρική συχνότητα των 2.4GHz, η οποία ενδέχεται να έχει μικρότερη χρήση, άρα λιγότερες παρεμβολές και μεγαλύτερη ταχύτητα και αξιοπιστία. Κάθε χώρα έχει δώσει συγκεκριμένες συχνότητες (radio wave spectrum) οι οποίες χρησιμοποιούνται για τα ασύρματα δίκτυα. Τα επιμέρους κανάλια (συνήθως 14 – δες εικόνα 6) έχουν συχνότητα φέροντος σήματος (carrier) διαφορετική κατά 5MHz από τα γειτονικά τους και συνολικό εύρος περίπου 22MHz έκαστο. Είναι φανερό ότι όλα τα κανάλια χρησιμοποιούν μέρος του φάσματος συχνοτήτων των γειτονικών τους καναλιών Στο πρότυπο 802.11a το οποίο έχει ευρύτερα κανάλια το κανάλι 8 δεν χρησιμοποιείται από άλλα. Hurley, C. (2004)

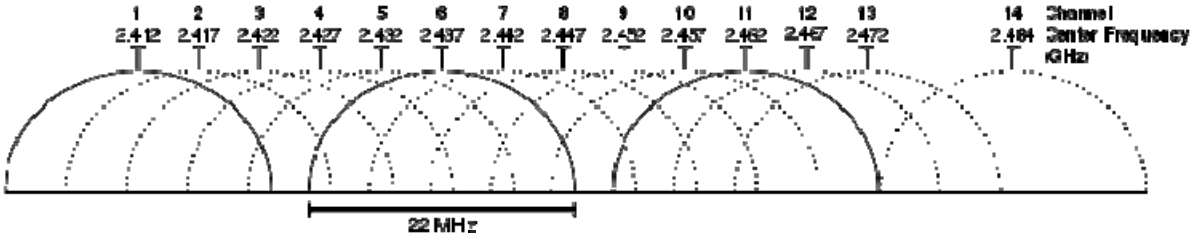


Image from:

http://www.art0.org/techjuice/wp-content/uploads/2011/04/2.4_GHz_Wi-Fi_channels_802.11bg_WLAN1.png

Εικόνα 6: Φάσμα συχνοτήτων του Wi-Fi

RADIUS:

Το Remote Authentication Dial In User Service (radius) [9], είναι ένα πρωτόκολλο που χρησιμοποιείται σε περιπτώσεις που υπάρχουν πολλοί χρήστες με διαφορετικά usernames και passwords ο καθένας που κάνουν χρήση ενός AP (όπως για παράδειγμα στα Hotspots). Σε αντίθεση με τα κλασσικά AP στα οποία δεν γίνεται διαχωρισμός χρηστών και οποιοσδήποτε γνωρίζει το Security Key μπορεί να συνδεθεί σε αυτά, τα hotspots δεν έχουν Security Key αλλά η πρόσβαση σε αυτά γίνεται με βάση κωδικούς πρόσβασης που κατέχουν διαφορετικοί χρήστες. Τον τελευταίο καιρό (και στην Κύπρο) οι εταιρίες (ISP) έχουν εγκαταστήσει σε πολλές περιοχές hotspots ή AP τα οποία χρησιμοποιούν την τεχνολογία

RADIUS. Έτσι η πρόσβαση στα hotspots παρέχεται σε επίπεδο χρήστη για να εξυπηρετεί τους συνδρομητές της εκάστοτε εταιρείας αλλά και να παρέχει πρόσβαση σε άλλους χρήστες με χρονοχρέωση. Για παράδειγμα μια εταιρία προσφέρει υπηρεσίες διαδικτύου μέσω των hotspots στους συνδρομητές της ακόμη και όταν αυτοί βρίσκονται εκτός του σπιτιού ή στον χώρο εργασίας (π.χ. όταν βρίσκονται στο αεροδρόμιο). Ο χρήστης ή συνδρομητής (συνήθως πληρώνεις κάποιο ποσό για να έχεις πρόσβαση) μέσω ενός συνδυασμού username και password συνδέεται σε ένα hotspot της εταιρίας. Το AP μέσω του RADIUS ζητά από τον χρήστη να δώσει τα στοιχεία του και τον κωδικό του. Ο χρήστης δίνει τις πληροφορίες και μέσω του RADIUS οι πληροφορίες αποστέλλονται σε ένα απομακρυσμένο server στον οποίο υπάρχουν καταχωρημένοι οι χρήστες. Ο server στέλνει πίσω αν τα στοιχεία είναι έγκυρα ή όχι. Η τεχνολογία RADIOUS δεν χρησιμοποιείται μόνο στα hotspots αλλά και από άλλες εταιρίες ή ιδρύματα που παρέχουν πρόσβαση σε συγκεκριμένες υπηρεσίες. Για παράδειγμα το Τεχνολογικό Πανεπιστήμιο Κύπρου χρησιμοποιεί την τεχνολογία RADIUS για να έχει ο κάθε φοιτητής, τεχνικός, ή καθηγητής πρόσβαση σε διαφορετικές υπηρεσίες του πανεπιστημίου.

Στην έρευνα που έκανα βρήκα μεγάλο αριθμό hotspots τα οποία είναι συνήθως είναι ανοιχτά (χωρίς κωδικό πρόσβασης) και τα κατηγοριοποίησα ανάλογα.

Wi-Fi Protected Setup (WPS):

Το WPS έχει σκοπό να διευκολύνει την εγκατάσταση ενός οικιακού ασύρματου δικτύου αλλά και την εύκολη δημιουργία ad-hoc συνδέσεων. Δημιουργήθηκε από την Wi-Fi Alliance το 2007 και ενσωματώθηκε σε πολλές συσκευές όπως ασύρματους δρομολογητές, εκτυπωτές, κλπ. Η τεχνολογία WPS διευκολύνει τους χρήστες που δεν γνωρίζουν καλά τα θέματα ασφάλειας και τις, αρκετά συχνά πολύπλοκες ρυθμίσεις που απαιτούνται, να μπορούν και αυτοί με έμμεσο τρόπο από μόνοι τους να δημιουργήσουν το δίκτυο τους. Το WPS το βρίσκουμε εγκατεστημένο σε καινούργιες συσκευές και μπορούμε να το βρούμε είτε σε μορφή Push-Button-Configuration είτε σε μορφή PIN. Η Push-Button είναι η πιο εύκολη μέθοδος για να εισάγει ένας χρήστης μια συσκευή με ασφάλεια στο δίκτυο του. Ο χρήστης απλά πιέζει το κουμπί στις συσκευές που θέλει να επικοινωνήσουν ή να συνδεθούν (πχ ένα δρομολογητή ή Access Point με έναν εκτυπωτή). Όταν πατήσει το WPS κουμπί στο δρομολογητή έχει στη διάθεση του δύο λεπτά να συνδέσει οποιαδήποτε άλλη συσκευή υποστηρίζει WPS τεχνολογία με το πάτημα του αντίστοιχου WPS κουμπιού της συσκευής αυτής. Άρα με το απλό πάτημα δύο κουμπιών συνδέει τον εκτυπωτή στο δίκτυο του χωρίς να χρειάζεται να ανοίξει ούτε ένα πρόγραμμα στον υπολογιστή και χωρίς συνδέσει κανένα καλώδιο. Το μόνο αρνητικό της μεθόδου Push-Button είναι ότι οποιοσδήποτε εξωτερικός χρήστης στην περίοδο των δύο λεπτών μπορεί να ενώσει τη δική του συσκευή στο δίκτυο χωρίς έγκριση [1]. Βεβαίως αυτό, είναι στατιστικά σχεδόν αδύνατο να συμβεί στην πράξη.

Image from: https://upload.wikimedia.org/wikipedia/commons/3/3d/Cisco_router_WPS_button.jpg

Εικόνα 7: Κουμπί WPS Push-Button-Configuration

Η άλλη μέθοδος που χρησιμοποιείται από το WPS είναι η μέθοδος PIN. Στη μέθοδο αυτή χρησιμοποιείται ένας κωδικός στο ενδιάμεσο της επικοινωνίας μεταξύ των συσκευών. Ο κωδικός αυτός είτε βρίσκεται γραμμένος στις συσκευές είτε δημιουργείται δυναμικά από κάποιο πρόγραμμα που υποστηρίζει την τεχνολογία WPS [2]. Για παράδειγμα, ένας χρήστης που θέλει να εισάγει μία νέα συσκευή στο δίκτυο του αντί να εισάγει τον WPA/WPA2/WEP κωδικό του (Security Key) που συνήθως είναι μεγάλος σε μέγεθος για μεγαλύτερη αξιοπιστία (με αποτέλεσμα να μην τον θυμάται ο χρήστης ή να είναι δύσκολη η εισαγωγή του), απλά εισάγει το οκταψήφιο PIN που βρίσκεται γραμμένο στη συσκευή (βλέπε Εικόνα 8). Ως αποτέλεσμα οι ρυθμίσεις η διαδικασία εγκατάστασης αυτοματοποιούνται χωρίς να χρειάζεται περαιτέρω παρέμβαση του χρήστη [2].

Image from: http://50.56.41.45/Cisco2/Images/kb17336-005_en.png

Εικόνα 8: WPS οκταψήφιος κωδικός πίσω από ένα δρομολογητή Linksys.

Τον Δεκέμβριο του 2011 ο Stefan Viehböck, ένας ανεξάρτητος ερευνητής ασφάλειας ανακοίνωσε ότι η μέθοδος PIN είναι ευάλωτη σε επιθέσεις τύπου brute-force (δοκιμή άπειρων κλειδιών μέχρι να βρεθεί ο κωδικός)[4]. Έχοντας βρει το WPS PIN του δρομολογητή μπορεί κάποιος να παρακάμψει την ασφάλεια του ασυρμάτου δικτύου (τον WPA2/WPA/WEP κωδικό) με αποτέλεσμα να έχει πρόσβαση στο ασύρματο δίκτυο [10].

[4] *https://en.wikipedia.org/wiki/Brute-force_attack*

Virtual Private Network (VPN)

Το VPN (εικονικό ιδιωτικό δίκτυο) χρησιμοποιείται όταν επιθυμούμε τη δημιουργία ενός δικτύου με περιορισμένο αριθμό συσκευών, χωρίς οι συσκευές αυτές να είναι τοπικά περιορισμένες σε μικρό χώρο (τοπικό δίκτυο), εντός ενός ευρύτερου δικτύου, συνήθως WAN (Wide Area Network). Για παράδειγμα η δημιουργία ενός δικτύου από πέντε υπολογιστές οι οποίοι μπορεί να βρίσκονται πολύ μακριά ο ένας από το άλλο αλλά είναι όλοι συνδεδεμένοι στο Διαδίκτυο και χρησιμοποιούν τα πρωτόκολλα του. Για να επιτευχθεί επομένως η δημιουργία του ιδιωτικού δικτύου θα πρέπει η επικοινωνία των συγκεκριμένων υπολογιστών να γίνεται με ασφαλή τρόπο και οι πληροφορίες που ανταλλάσσονται να είναι κρυπτογραφημένες. Η διαδικασία κρυπτογράφησης – αποκρυπτογράφησης είναι που κάνει την επικοινωνία μέσω του VPN πιο αργή από την κλασσική επικοινωνία με οποιαδήποτε άλλο υπολογιστή στο Διαδίκτυο.

Το VPN το χρησιμοποιούμε συνήθως για να ενωθούμε σε ένα απόμακρο δίκτυο π.χ. από το σπίτι μας στο δίκτυο του πανεπιστημίου για να έχουμε πρόσβαση στα δεδομένα μας και στις διάφορες λειτουργίες που μας παρέχει το απόμακρο δίκτυο (βλέπε Εικόνα 9). Όπως αναφέραμε ήδη οι πληροφορίες που μεταδίδονται μέσω της VPN σύνδεσης είναι κρυπτογραφημένες, ως εκ τούτου η περιήγηση στο Διαδίκτυο μέσω μιας σύνδεσης VPN είναι ασφαλέστερη (αλλά και πιο αργή). Τα τρία θεμελιώδη συστατικά της ασφάλειας του VPN είναι η κρυπτογράφηση, η πιστοποίηση και η διαχείριση κλειδιών[5]. Το VPN επιτρέπει στους χρήστες που βρίσκονται σε εξωτερικά δίκτυα των οποίων δεν γνωρίζουν την πιστότητα να παραμείνουν ασφαλές. Αν για παράδειγμα πρέπει να πραγματοποιήσεις κάποια συναλλαγή μέσω του διαδικτύου όντας συνδεδεμένος στο ασύρματο δίκτυο ενός αεροδρομίου τότε η ασφαλέστερη επιλογή είναι συνδεθείς με VPN σε κάποιο δίκτυο στο οποίο έχεις πρόσβαση. Σε αυτή την περίπτωση τα δεδομένα που αποστέλλονται από τη συσκευή σου είναι κρυπτογραφημένα και είναι σχεδόν αδύνατον για κάποιο άλλο υπολογιστή η συσκευή που βρίσκεται στο ίδιο (εξωτερικό) δίκτυο να τα υποκλέψει. Αυτό οφείλεται στο ότι οι πληροφορίες που μεταφέρουν τα packet headers ή στο Wi-Fi τα beacon frames, όπως πχ τις ιστοσελίδες που επισκεπτόμαστε, ποιες πληροφορίες αναζητούμε (keywords), πληροφορίες για λογαριασμούς και κωδικούς κτλ, δεν είναι εμφανίσιμες μέσω λογισμικών που δυνατόν παρακολουθούν τα δεδομένα που περνούν από το δίκτυο. Ένα από τα αρνητικά του VPN είναι ότι ο χρήστης για να εγκαταστήσει μια τέτοια τεχνολογία θα πρέπει να έχει εξειδικευμένες γνώσεις δικτύων γενικότερα, καθώς πρέπει να συνδέσει από τη μια πλευρά ένα server όπου θα είναι το μέρος του δικτύου που θέλουμε να έχουμε πρόσβαση και από την πλευρά τον εκάστοτε χρήστη που θα εισέρχεται στο δίκτυο. Η διαδικασία μπορεί να είναι χρονοβόρα και πολύπλοκη [12].

[5] *http://www.ip.gr/el/dictionary/136-VPN_Virtual_Private_Network*

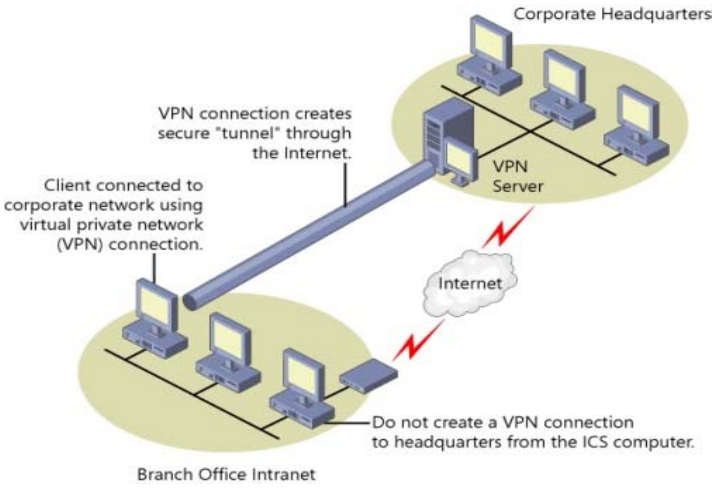


Image from: https://technet.microsoft.com/en-us/library/Bb457119.f25zs09_big%28en-us,TechNet.10%29.jpg

Εικόνα 9: VPN tunneling από υπολογιστή σε άλλο δίκτυο.

HTTP, HTTPS και SSL:

Το HTTP (Hypertext Transfer Protocol), είναι το πρωτόκολλο επικοινωνίας ανάμεσα σε έναν Web server, στον οποίο είναι αναρτημένες ιστοσελίδες, και σε ένα Web client δηλαδή έναν φυλλομετρητή (browser). Μέσω πρωτοκόλλου HTTP φυλλομετρητές και διακομιστές (Web servers) ανταλλάσσουν δεδομένα με μονοσήμαντο τρόπο. Στην περίπτωση του απλού HTTP τα δεδομένα μεταφέρονται χωρίς κρυπτογράφηση με αποτέλεσμα να μπορούν να υποκλαπούν με ευκολία [11].

Για την λύση του προβλήματος αυτού αναπτύχθηκε το πρωτόκολλο SSL (Secure Sockets Layer) το οποίο βοηθάει στην ασφαλή επικοινωνία μεταξύ φυλλομετρητών και διακομιστών. Το SSL αυτό δημιουργεί ένα ασφαλές κανάλι ανταλλαγής δεδομένων και κρυπτογραφεί τα δεδομένα που ανταλλάσσονται. Πριν γίνει η ανταλλαγή δεδομένων, ο διακομιστής και ο φυλλομετρητής επικοινωνούν μεταξύ τους για να εγκριθεί η ανταλλαγή δεδομένων. Στην συνέχεια ενεργοποιείται το SSL certificate μέσω του οποίου κάποιες εταιρείες (πχ verisign, globalsign, comodo) βεβαιώνουν ότι τα ο διακομιστής είναι πράγματι αυτός που ισχυρίζεται ότι είναι και όχι κάποιος "Δούρειος Ίππος" (όταν συνδεόμαστε για παράδειγμα στην τράπεζα μας το SSL certificate βεβαιώνει ότι πράγματι η συγκεκριμένη ιστοσελίδα είναι της τράπεζας και όχι κάποιου hacker που προσπαθεί να υποκλέψει στοιχεία). Στην πράξη πολλοί Web servers που υποστηρίζουν το πρωτόκολλο SSL δεν χρησιμοποιούν SSL cerificates από κάποια εταιρεία αναγνωρισμένη αλλά εκδίδουν δικά τους. Ο λόγος είναι ότι οι εξουσιοδοτημένες εταιρείες παροχής SSL certificates απαιτούν μηνιαία συνδρομή. Επομένως η χρήση SSL χωρίς την ύπαρξη έγκυρου SSL certificate εγγυάται μεν την κρυπτογραφημένη ανταλλαγή δεδομένων αλλά δεν εγγυάται ότι ο παραλήπτης είναι ο σωστός. Έτσι ενώ η υποκλοπή δεδομένων κατά τη μεταφορά τους δεν είναι εφικτή ο παραλήπτης μπορεί να τα αποκρυπτογραφήσει.

Η χρήση του SSL σε συνδυασμό με το HTTP προτυποποιήθηκε ως HTTPS (Hypertext Transfer Protocol with Secure socket layer). Η χρήση του SSL είναι σήμερα όλο και περισσότερο διαδεδομένη καθώς αποτελεί μια λύση στο θέμα της ασφάλειας μεταφοράς δεδομένων μέσω του Διαδικτύου [7].

Image from: http://www.globalsign.co.uk/images/ssl-info-standard-ssl-example.jpg

Εικόνα 10: SSL encryption από φυλλομετρητή όταν επισκέπτεται ο χρήστης μια ασφαλή σελίδα.

Μεθοδολογία

Η έρευνα μου χωρίζεται σε δύο μέρη:

Wardriving

Το πρώτο μέρος αποτελεί την αναζήτηση και την συλλογή δεδομένων στον αέρα (Wardriving). Αυτό έγινε με τη βοήθεια λογισμικού που η λειτουργία του ήταν να αναζητά και να αποθηκεύει τις πληροφορίες σε ένα text ή ένα csv file. Το τελευταίο μπορεί να επεξεργαστεί με τη βοήθεια του Microsoft Excel. Εκτός από το λογισμικό χρησιμοποίησα και υλικό (hardware): δύο φορητούς υπολογιστές με λειτουργικό σύστημα Linux. Ο ένας υπολογιστής πραγματοποιούσε την αναζήτηση και αποθήκευε για κάθε ασύρματο δίκτυο που εντόπιζε:

- (α) το όνομα του access point (SSID),
- (β) σε ποιο πρότυπο λειτουργεί (802.11b/g/n),
- (γ) σε ποιο κανάλι βρίσκεται (channel 1-13),
- (δ) το πρωτόκολλο ασφάλειας που λειτουργεί και χρησιμοποιεί (WEP, WPA, WPA2, open) και,
- (ε) σε μερικά σημεία που υπήρχε η δυνατότητα την τοποθεσία του ασυρμάτου δικτύου μέσω GPS συντεταγμένων.

Όταν δεν υπήρχε η δυνατότητα εύρεσης των GPS συντεταγμένων απευθείας από τον αρχικό υπολογιστή αυτές εντοπίζονταν μέσω μιας GPS συσκευής και αποθηκεύονταν χειρωνακτικά στο δεύτερο υπολογιστή. Όταν δεν υπήρχε δυνατότητα να γίνει Wardriving μέσω αυτοκινήτου υπήρχε και η δυνατότητα να χρησιμοποιηθεί λογισμικό από κινητό τηλέφωνο με λειτουργικό IOS όπως το iphone για πιο εύκολη αναζήτηση (warwalking). Ωστόσο τα προγράμματα λειτούργησαν κανονικά και δεν διαπιστώθηκε κάποιο πρόβλημα.

Στην Εικόνα 11 φαίνεται ένα στιγμιότυπο από το πρόγραμμα αναζήτησης και καταγραφής που χρησιμοποιήθηκε στο Wardriving.

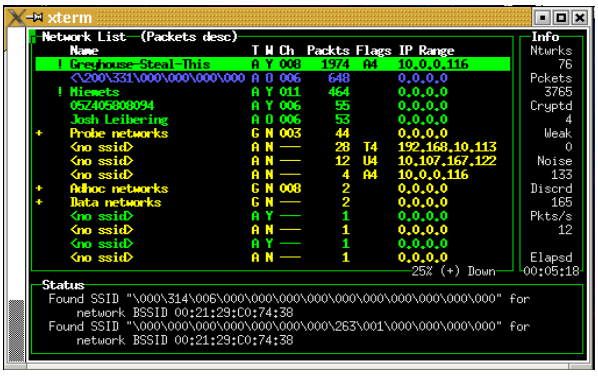


Image from: http://www.cromwell-intl.com/security/pictures/kismet.png

Εικόνα 11: Λογισμικό σε περιβάλλον Linux για αναζήτηση ασυρμάτων δικτύων μέσω Wardriving

Στο πρακτικό μέρος της έρευνας ο αριθμός των ασυρμάτων δικτύων που κατάφερα να καταγράψω ήταν 7070. Επειδή δεν ήθελα να υπάρχουν δίκτυα καταχωρημένα περισσότερες από μία φορές (πέρασα από την ίδια περιοχή δύο φορές για καλύτερο έλεγχο) έπρεπε να βρω ένα τρόπο να αναγνωρίζω διπλές καταχωρήσεις. Επειδή το SSID δεν είναι μοναδικό χαρακτηριστικό των AP (υπάρχουν πάρα πολλά APs με όνομα Linksys και NETGEAR) χρησιμοποίησα την MAC address των APs για φιλτράρισμα των διπλών καταχωρήσεων. Μετά την αφαίρεση των διπλών καταχωρήσεων είχαμε καταγραφή 4932 διαφορετικών ασύρματων δικτύων, αριθμός αρκετά υψηλός για να έχουμε αντιπροσωπευτικά συμπεράσματα, δεδομένου ότι η περιοχή που εξετάστηκε (κατά βάση ο δήμος Λεμεσού χωρίς τους περιφερειακούς δήμους – βλέπε Εικόνα 13) δεν πρέπει να περιλαμβάνει περισσότερα από 20000 νοικοκυριά, από τα οποία δεν έχουν όλα σύνδεση στο διαδίκτυο αλλά ακόμη και αν έχουν δεν έχουν υποχρεωτικά ασύρματο δίκτυο.

Στην Εικόνα 12 φαίνεται το τελευταίο τμήμα του αρχείου καταγραφής πριν και μετά την αφαίρεση των διπλών εγγραφών.

7061	2.01E+13	2.01E+13	00:21:96:4	PrimeTel	11	-89	0	Access Po	None	NoEncrypt	0	1	34.69048	33.02642	1414	-89	2.01E+13	34.69048	33.02642	1414
7062	2.01E+13	2.01E+13	00:24:17:2	CYTADE71	6	-91	0	Access Po	WPA Pers	TKIP	12	1	34.68724	33.02542	100	-85	2.01E+13	34.69048	33.02642	1414
7063	2.01E+13	2.01E+13	00:27:19:C	BL_CYTA	6	-93	0	Access Po	WEP	NoEncrypt	5	1	34.69048	33.02642	1414	-93	2.01E+13	34.68816	33.03107	1414
7064	2.01E+13	2.01E+13	00:1D:68:E	CYTAD795	11	-91	0	Access Po	WPA Pers	TKIP	5	1	34.69048	33.02642	1414	-91	2.01E+13	34.68816	33.03107	1414
7065	2.01E+13	2.01E+13	00:24:17:4	CYTA41BC	11	-93	0	Access Po	WPA Pers	TKIP	5	1	34.69048	33.02642	1414	-93	2.01E+13	34.68816	33.03107	1414
7066	2.01E+13	2.01E+13	00:24:17:3	CYTA769E	1	-89	0	Access Po	WEP	NoEncrypt	10	1	34.68724	33.02542	100	-85	2.01E+13	34.69048	33.02642	1414
7067	2.01E+13	2.01E+13	00:1F:9F:D	CYTA3651	6	-91	0	Access Po	WEP	NoEncrypt	6	1	34.69048	33.02642	1414	-91	2.01E+13	34.68816	33.03107	1414
7068	2.01E+13	2.01E+13	00:22:B0:E	1stFloor	1	-92	0	Access Po	WPA2 Per	TKIP+AES	6	1	34.69048	33.02642	1414	-89	2.01E+13	34.68816	33.03107	1414
7069	2.01E+13	2.01E+13	00:1D:68:E	CYTA0DC2	1	-91	0	Access Po	WEP	NoEncrypt	6	1	34.69048	33.02642	1414	-86	2.01E+13	0	0	0
7070	2.01E+13	2.01E+13	02:2A:7A::	HP-nomo	6	-93	0	Ad Hoc	None	NoEncrypt	7	1	34.68724	33.02542	100	-93	2.01E+13	0	0	0

(α)

4912	00:24:17:33:F3:E5	XRISA	9	-95	0	Access Po	WPA Persona	TKIP
4913	00:26:37:1D:6A:18	XSBoxGO_A18	6	-83	0	Access Po	WEP	NoEncryption
4914	00:24:17:41:6F:6E	XTREME	1	-90	0	Access Po	WPA Persona	TKIP
4915	00:24:17:33:1A:C3	xxxxxxxxxx	1	-88	0	Access Po	WPA Persona	TKIP
4916	08:76:FF:50:4B:93	yangos	1	-81	0	Access Po	WPA Persona	TKIP
4917	68:7F:74:F6:E0:2B	yiafotand	6	-95	0	Access Po	WPA2 Person	TKIP+AES
4918	00:21:91:0D:4C:2F	YIAKOUMIS	6	-91	0	Access Po	WPA2 Person	TKIP+AES
4919	00:21:29:EB:3F:BE	yiatros-wap	11	-85	0	Access Po	WEP	NoEncryption
4920	50:67:F0:27:81:EC	ZAION	1	-90	0	Access Po	WPA2 Person	AES
4921	00:21:91:0D:4D:03	ZAMO	3	-86	0	Access Po	None	NoEncryption
4922	00:18:39:1D:AE:53	zarisaccesspoint	11	-85	0	Access Po	WEP	NoEncryption
4923	00:1D:68:EA:43:7B	Zarko	11	-79	0	Access Po	WEP	NoEncryption
4924	00:90:D0:E0:01:25	ZavosPegasus	11	-90	0	Access Po	WEP	NoEncryption
4925	00:21:27:E4:CB:B6	Zazerka	1	-89	0	Access Po	WPA2 Person	TKIP+AES
4926	00:B0:0C:00:C6:DA	ZDemotiko	6	-95	0	Access Po	WPA2 Person	TKIP+AES
4927	00:1A:70:DE:D8:06	zeloslink	5	-86	0	Access Po	WPA Persona	TKIP
4928	00:24:17:32:75:51	ZONZO SHOES	6	-87	0	Access Po	WPA Persona	TKIP
4929	00:24:17:32:4E:35	ZOOM	10	-92	0	Access Po	WEP	NoEncryption
4930	00:24:17:1A:3A:65	Zpassion	11	-93	0	Access Po	WEP	NoEncryption
4931	00:22:6B:DD:49:B2	ZunixAir	6	-92	0	Access Po	WPA2 Person	TKIP+AES
4932	C0:C1:C0:4E:B9:F5	ZunixAir	6	-94	0	Access Po	WPA2 Person	TKIP+AES

(β)

Εικόνα 12: Απόσπασμα από τα αρχεία καταγραφής πριν (α) και μετά (β) την αφαίρεση των διπλών καταχωρήσεων.

Οι πληροφορίες που κρατήθηκαν στην μελέτη ήταν το MAC address (1η στήλη στην Εικόνα 12(β)), το SSID (2η στήλη), κανάλι (3η στήλη), ο τύπος δικτύου (AP, Ad-hoc), το πρωτόκολλο ασφαλείας και ο τύπος του κλειδιού κρυπτογράφησης και αν είναι ορατό ή όχι. Αποθηκεύτηκαν επίσης οι χωρικές συντεταγμένες του δικτύου (Εικόνα 12(α) στήλες 13-14) ώστε να μπορέσουμε να απεικονίσουμε τις τοποθεσίες των ασυρμάτων δικτύων στο Google Earth (βλέπε Εικόνα 13).

Καταγραφή αόρατων δικτύων

Στο σημείο πιθανόν να υπάρχει η απορία πως μπορέσαμε να καταγράψουμε τα μη ορατά ασύρματα δίκτυα (δηλαδή αυτά που δεν κάνουν broadcast το SSID τους). Για να τα επιτύχουμε αυτό θέσαμε την κάρτα δικτύου του υπολογιστή μας σε κατάσταση καταγραφής (monitor mode). Στην κατάσταση αυτή η κάρτα δικτύου μπορεί να καταγράψει όλα τα MAC address με τα οποία επικοινωνεί άμεσα και αυτά φυσικά δεν είναι άλλες συσκευές Wi-Fi άλλα Access Points με κρυμμένο SSID. Αφού λοιπόν SSID του συγκεκριμένου δικτύου δεν είναι ορατό τότε καταχωρείται στο αρχείο μας το αντίστοιχο δίκτυο ως αόρατο (όπως είπαμε όμως υπάρχουν καταγεγραμμένα το MAC address και οι GPS συντεταγμένες του).

Εικόνα 13: Απεικόνιση της θέσης των ασυρμάτων δικτύων που καταγράφηκαν στο Google Earth

Καταγραφή APs με τεχνολογία RADIUS

Πολλά δίκτυα στο δείγμα μας χρησιμοποιούσαν τεχνολογία RADIUS (hotspots). Τα δίκτυα αυτά εμφανίζονται ως ανοικτά (δηλαδή χωρίς πρωτόκολλο ασφαλείας και Security Key). Προσπάθησα να διαχωρίσω τα δίκτυα RADIUS, κοινής πρόσβασης, από τα οικιακά ασύρματα δίκτυα τα οποία δεν ήταν ασφαλισμένα με πρωτόκολλο ασφαλείας, διότι τα δίκτυα RADIUS παρότι εμφανίζονται ως ανοικτά δεν είναι. Ο διαχωρισμός των δικτύων RADIUS έγινε και πάλι με τη βοήθεια της MAC address. Όπως είδαμε νωρίτερα κάθε εταιρία έχει συγκεκριμένα διευθύνσεις MAC που της παρέχονται από την IEEE. Τα πρώτα έξι ψηφία της MAC καθορίζουν την εταιρία η οποία κατασκευάζει τη συσκευή και τα υπόλοιπα έξι είναι ο σειριακός αριθμός του προϊόντος με βάση την κωδικοποίηση που κάνει η κάθε εταιρεία στα προϊόντα της που διαθέτουν κάρτα δικτύου. Η IEEE έχει online βάση με τους κωδικούς των εταιρειών όσον αφορά τα πρώτα έξι ψηφία της διεύθυνσης MAC. Στην Κύπρο οι παροχείς υπηρεσιών διαδικτύου χρησιμοποιούν προϊόντα από συγκεκριμένες

εταιρείες (π.χ. η CYTA χρησιμοποιεί Access Points της εταιρείας Thomson). Έτσι μπόρεσα να εντοπίσω τα hotspots των διαφόρων εταιρειών κάνοντας αντιπαραβολή της MAC address με τη βάση δεδομένων της IEEE όσων αφορά τις διευθύνσεις MAC.

Κατηγοριοποίηση ασυρμάτων δικτύων με βάση τον πάροχο υπηρεσιών διαδικτύου

Στην έρευνα μου χώρισα τα ασύρματα δίκτυα με βάση τον πάροχο υπηρεσιών διαδικτύου. Ο λόγος είναι ότι κάθε εταιρεία έχει διαφορετική πολιτική ασφάλειας όσον αφορά τα ασύρματα δίκτυα. Για παράδειγμα κάποιες εταιρείες δεν επιτρέπουν στους συνδρομητές τους να αλλάξουν το SSID του δικτύου τους ενώ άλλες, όπως η CYTA, το επιτρέπουν. Τα ασύρματα δίκτυα της CYTA στα οποία οι συνδρομητές άλλαξαν το SSID έπρεπε να εντοπιστούν και να καταταχθούν σε αυτήν και όχι σε άλλες εταιρείες.

Η κατάταξη των ασυρμάτων δικτύων σε εταιρείες παροχής υπηρεσιών διαδικτύου έγινε και πάλι με τη βοήθεια της διεύθυνσης MAC. Γνώριζα όλες τις συσκευές που χρησιμοποιούσαν οι εταιρίες ISP αλλά και τις ονομασίες SSID που δίνουν ως προκαθορισμένη επιλογή (default) στα Access Points που δίνουν στους συνδρομητές τους. Μπορούσα επίσης να εντοπίσω αν ένα AP που δόθηκε από τη CYTA έχει δεχθεί αλλαγές η όχι μέσω του MAC address. Αν για παράδειγμα το όνομα ενός ασυρμάτου δικτύου είναι “wifi home” και η διεύθυνση MAC αντιστοιχεί στην εταιρία Thomson (η οποία είναι η εταιρία που προμηθεύει δρομολογητές και Access Points την CYTA) τότε είναι φανερό ότι το συγκεκριμένος AP έχει υποστεί αλλαγές ως προς τις ρυθμίσεις του από τον ιδιοκτήτητη του.

Ερωτηματολόγιο

Το δεύτερο μέρος της εργασίας περιλαμβάνει ερωτηματολόγιο σε διάφορους συνδρομητές που έχουν ασύρματο οικιακό δίκτυο. Η επιλογή του δείγματος ήταν τυχαία, μέσω της μεθόδου χιονοστιβάδας. Εναλλακτικά θα μπορούσα να είχα μιλήσει με ένα λειτουργό μιας εταιρίας που θα μπορεί να στείλει σε τυχαία άτομα email με το ερωτηματολόγιο αλλά δεν υπήρχε αρκετός χρόνος. Το ερωτηματολόγιο περιλάμβανε απλές ερωτήσεις και ο σκοπός του ήταν να κατανοήσουμε αν τα μέτρα προστασίας που παίρνουν οι συνδρομητές είναι επαρκή αλλά και να κρίνουμε αν είναι ενήμεροι για τα θέματα ασφαλείας του δικτύου τους. Για παράδειγμα μια ερώτηση ήταν: “γνωρίζεις το όνομα του προσωπικού σου ασύρματου δικτύου;” Αν η απάντηση είναι αρνητική τότε αυτό αποτελεί μια ισχυρή ένδειξη ότι το άτομο δεν ασχολήθηκε με το θέμα ασφάλειας του δικτύου του. Μια άλλη ερώτηση ήταν αν άλλαξε το όνομα ή τον κωδικό του ασυρμάτου του δικτύου. Έτσι μπορέσαμε να δημιουργήσουμε εύκολες μεταβλητές που μπόρεσαν να περιγράψουν κατά πόσο γνωρίζει ή αν έλαβε μέτρα προστασίας ο χρήστης. Το δείγμα της εργασίας δεν ήταν πολύ μεγάλο διότι δεν υπάρχει και ο κατάλληλος χρόνος διαθέσιμος στην πτυχιακή. Ο τελικός αριθμός του δείγματος είναι 152 άτομα όπου είναι αρκετά για μια εκτίμηση η οποία μπόρεσε να ενισχύσει τα αποτελέσματα που έχουμε λάβει από το Wardriving. Τα αποτελέσματα αναλύθηκαν μέσω του λογισμικού Microsoft Excel και συγκεκριμένων φόρμουλων ώστε να παρουσιαστούν μέσω διαγραμμάτων που δείχνουν τα ποσοστά για τις απαντήσεις.

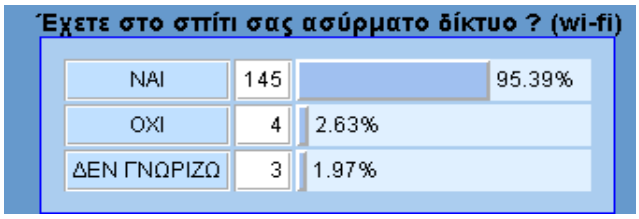
Αποτελέσματα

Έρευνα κοινής γνώμης

Μετά από την συλλογή ερωτηματολογίων και την πρακτική μελέτη μέσω λογισμικών εύρεσης ασυρμάτων δικτύων προκύπτουν μερικά ενδιαφέροντα συμπεράσματα.

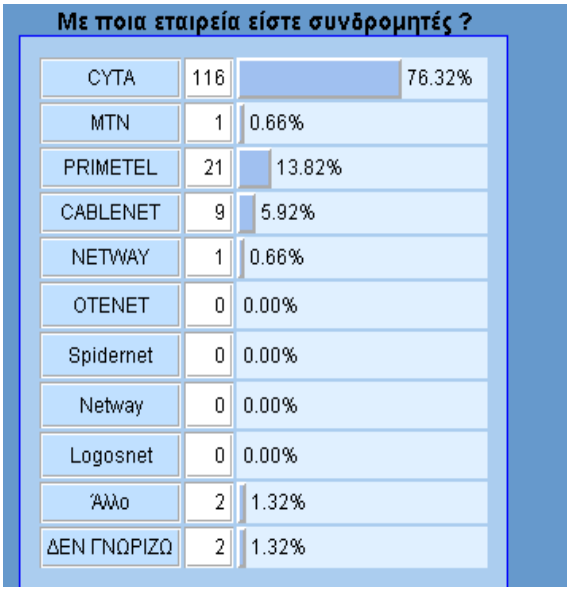
Το μέγεθος του δείγματος των ερωτηματολογίων έφθασε τα 152 άτομα, οι ερωτήσεις που υπήρχαν στο ερωτηματολόγιο προσπαθούσαν να δώσουν μια εικόνα με το κατά πόσο οι Κύπριοι γνώριζαν τους βασικούς τρόπους να ασφαλίζουν το ασύρματο δίκτυο τους και να απαντήσει τα ερευνητικά ερωτήματα που θέσαμε στην παρούσα μελέτη. Οι ερωτήσεις ήταν όσο πιο κατανοητές γίνεται με λίγες απαντήσεις συνήθως ναι ή όχι. Επιπρόσθετες ερωτήσεις έγιναν και για το αν οι χρήστες ασυρμάτου δικτύου χρησιμοποιούν επιπρόσθετες λειτουργίες ασφάλειας ή αν τις γνωρίζουν. Θα μελετήσουμε πιο κάτω την κάθε ερώτηση για να μπορέσουμε να δώσουμε πληροφορίες και συμπεράσματα.

Η Ερώτηση 1 ήταν μια απλή ερώτηση αν οι χρήστες έχουν ασύρματο δίκτυο στο σπίτι τους. Το 95% απάντησε ναι στην ερώτηση άρα στο δείγμα μας σχεδόν όλοι είχαν ασύρματο δίκτυο στο σπίτι τους και γνώριζαν την ύπαρξη του. Ένα ποσοστό 2% απάντησε ότι δεν γνώριζε αν υπάρχει ασύρματο δίκτυο στο σπίτι του. Προφανώς πρόκειται για μέλη οικογενειών τα οποία δεν είναι οι ίδιοι συνδρομητές σε μια εταιρεία παροχής υπηρεσιών διαδικτύου.

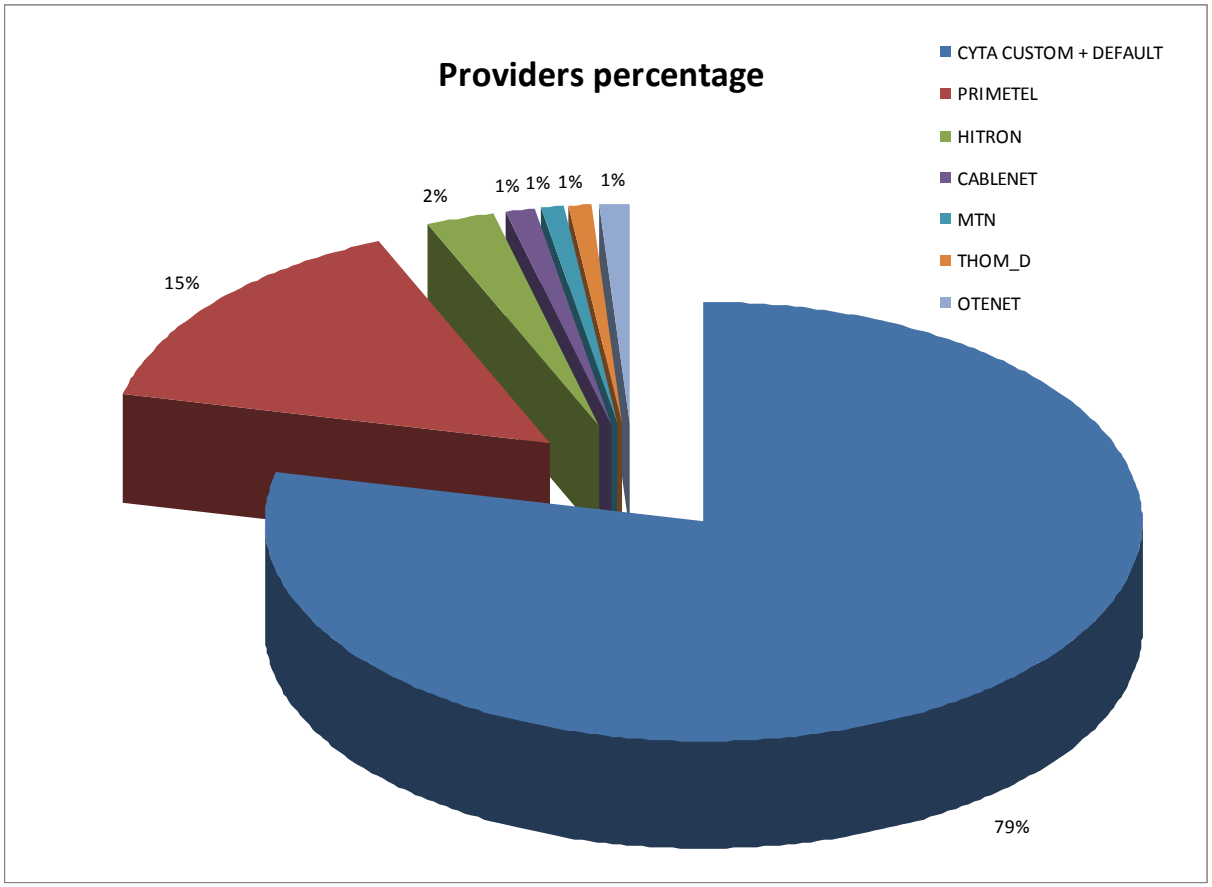


Εικόνα 14: Ερώτηση 1 από το ερωτηματολόγιο.

Η Ερώτηση 2 αφορούσε τις εταιρίες ISP, δηλαδή τις εταιρίες που παρέχουν πρόσβαση στο διαδίκτυο. Από την ερώτηση αυτή είχαμε επίσης μια εκτίμηση (όχι ακριβή λόγω του μεγέθους του δείγματος), σε επίπεδο τάξης μεγέθους, του μεριδίου αγοράς για κάθε εταιρεία όσον αφορά την παροχή υπηρεσιών διαδικτύου. Η εκτίμηση αυτή μπορούσε να διασταυρωθεί με ακριβέστερα στοιχεία μέσω της πρακτικής μελέτης. Στην Εικόνα 16 παρουσιάζονται τα αντίστοιχα στοιχεία που λήφθηκαν μέσω της πρακτικής μελέτης. Τόσο με βάση το ερωτηματολόγιο όσο και βάσει της πρακτικής μελέτης προκύπτει ότι οι περισσότεροι συνδρομητές έχουν σε πάροχο υπηρεσιών διαδικτύου τη CYTA, κάτι αναμενόμενο δεδομένου ότι η CYTA ήταν η πρώτη εταιρεία παροχής υπηρεσιών διαδικτύου στη Κύπρο.

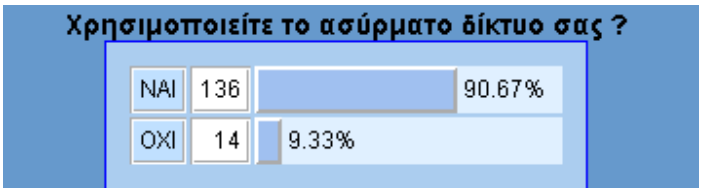


Εικόνα 15: Ερώτηση 2 από το ερωτηματολόγιο.

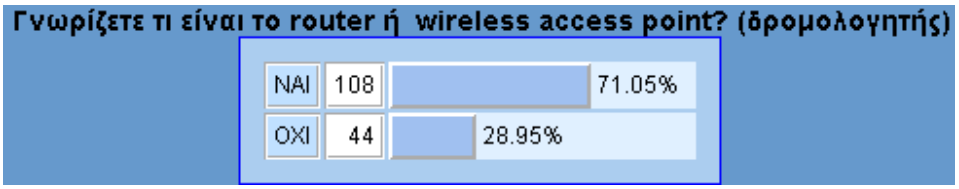


Εικόνα 16: Εκτίμηση μεριδίου αγοράς εταιρειών ISP μέσω της πρακτικής μελέτης (wardriving)

Η Ερώτηση 3 αφορούσε τη χρήση του οικιακού ασυρμάτου δικτύου. Οι περισσότερες απαντήσεις ήταν θετικές (90%), οι υπόλοιποι μπορεί να μην έχουν συσκευές που να χρησιμοποιούν ασύρματο δίκτυο ή απλά χρησιμοποιούν ενσύρματο δίκτυο για μεγαλύτερη ταχύτητα ή για σκοπούς ασφάλειας κλείνουν το ασύρματο τους δίκτυο. Τέλος σε αυτούς που έδωσαν αρνητική απάντηση περιλαμβάνονται και αυτοί που απλά δεν έχουν οικιακό ασύρματο δίκτυο.



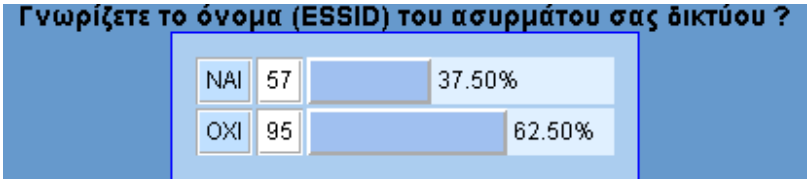
Εικόνα 17: Ερώτηση 3 από το ερωτηματολόγιο



Εικόνα 18: Ερώτηση 4 από το ερωτηματολόγιο

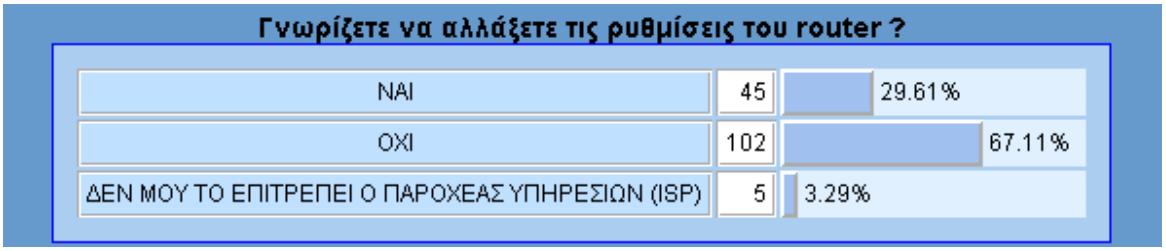
Από την τέταρτη ερώτηση και μετά οι ερωτήσεις εστιάζουν στην εκτίμηση των γνώσεων που έχουν οι χρήστες για τα ασύρματα δίκτυα και τα μέτρα προστασίας τους. Στην Ερώτηση 4 προσπαθούμε να δούμε αν οι χρήστες γνωρίζουν κάποια βασικά πράγματα για την τεχνολογία Wi-Fi, συγκεκριμένα για τον δρομολογητή ή access point, δηλαδή για τη συσκευή δημιουργίας ασυρμάτου δικτύου και διαμεσολάβησης σύνδεσης του δικτύου αυτού (ακριβέστερα των συσκευών που το απαρτίζουν) στο διαδίκτυο. Το 71% του δείγματος απάντησε ότι γνωρίζει τι είναι ένας δρομολογητής, άρα μπορούμε να εικάσουμε ότι το μεγαλύτερο μέρος του δείγματος γνωρίζει από πού προέρχεται το σήμα που λαμβάνουν οι ασύρματες συσκευές για να μπορέσουν να συνδεθούν στο διαδίκτυο. Το 29% που απάντησε ότι δεν γνωρίζει τι είναι ο δρομολογητής μπορεί απλά να μην γνωρίζει την τεχνική ονομασία της συσκευής ή απλά δεν έχει τις γνώσεις για το θέμα.

Στην Ερώτηση 5 έχουμε ένα ενδιαφέρον αποτέλεσμα: Οι χρήστες του ασυρμάτου δικτύου (πολλοί εκ των οποίων μπορεί να είναι οι ίδιοι συνδρομητές σε μια εταιρεία ISP) δεν γνωρίζουν το όνομα του ασυρμάτου τους δικτύου. Το 62% του δείγματος απάντησε ότι δεν γνωρίζει το όνομα του ασυρμάτου του δικτύου έναντι του 37% που απάντησε ότι το γνωρίζει. Με λίγα λόγια οι περισσότεροι χρήστες δεν γνωρίζουν σε ποιο access point είναι συνδεδεμένη η ασύρματη συσκευή που χρησιμοποιούν. Είναι συνδεδεμένοι στο δικό τους προσωπικό δίκτυο ή σε άλλο ξένο δίκτυο ή μήπως πληρώνουν χρονοχρέωση με σύνδεση σε κάποιο hotspot;



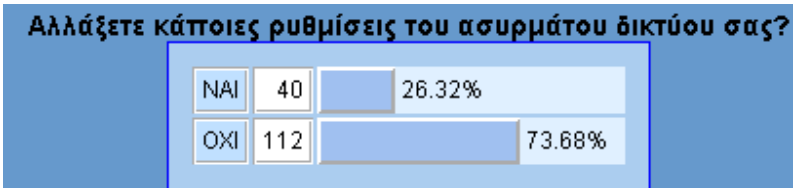
Εικόνα 19: Ερώτηση 5 από το ερωτηματολόγιο

Η επικινδυνότητα στο να μην γνωρίζει κάποιος σε ποιο δίκτυο βρίσκεται είναι καθώς έτσι μπορούν να εύκολα κλαπούν ευαίσθητα προσωπικά δεδομένα από τρίτους. Αν θεωρήσουμε αληθείς τις απαντήσεις που δόθηκαν στην ερώτηση αυτή τότε εφόσον οι χρήστες δεν γνωρίζουν σε ποιο δίκτυο είναι συνδεδεμένοι τότε είναι σχεδόν σίγουρο ότι δεν έχουν τις γνώσεις για να αλλάξουν τις βασικές ρυθμίσεις του ασύρματου τους δικτύου για να μένουν ασφαλείς. Είναι προφανές ότι οι ρυθμίσεις ασφαλείας για τους συνδρομητές που απάντησαν ότι δεν γνωρίζουν το όνομα του ασυρμάτου τους δικτύου είναι αυτές που ορίστηκαν από την εταιρεία παροχής υπηρεσιών κατά την πρώτη εγκατάσταση. Άλλες ερωτήσεις στην συνέχεια θα μας βοηθήσουν να έχουμε καλύτερη εικόνα για το θέμα αυτό.



Εικόνα 20: Ερώτηση 6 από το ερωτηματολόγιο

Η έκτη ερώτηση είναι πολύ σημαντική για την έρευνα μας: Διερευνά κατά πόσο οι χρήστες γνωρίζουν να αλλάξουν τις ρυθμίσεις του δρομολογητή τους. Ένας πολύ σημαντικός παράγοντας για να κρατήσεις το ασύρματο σου δίκτυο ασφαλές και μακριά από ανεπιθύμητα άτομα είναι η δυνατότητα (όταν παρέχεται από την εταιρεία) και ικανότητα (αν έχεις τις γνώσεις) να έχεις πρόσβαση στο δρομολογητή και να αλλάξεις κάποιες βασικές ρυθμίσεις όπως κωδικός πρόσβασης (Security Key) κτλ και να ελέγχεις αν υπάρχουν άλλα άτομα συνδεδεμένα στο δίκτυο. Στην Ερώτηση 6 το 67% απάντησε ότι δεν γνωρίζει να αλλάξει τις ρυθμίσεις του δρομολογητή, το 29% ότι γνωρίζει και ένα 3% ότι δεν του το επιτρέπει ο παροχέας ISP. Είναι αλήθεια ότι στους συνδρομητές της Primetel δεν επιτρέπεται να αλλάξουν ρυθμίσεις του δρομολογητή. Όμως σύμφωνα με την απάντηση στην Ερώτηση 2 και τις Εικόνες 15 και 16 το μερίδιο αγοράς της Primetel είναι 14-15%. Επομένως ένα σημαντικό ποσοστό από αυτούς που απάντησαν ότι δεν γνωρίζουν να αλλάξουν τις ρυθμίσεις του δρομολογητή τους και να γνώριζαν να το κάνουν δεν τους επιτρέπει ο πάροχος υπηρεσιών διαδικτύου (στη συγκεκριμένη περίπτωση η Primetel).



Εικόνα 21: Ερώτηση 7 από το ερωτηματολόγιο

Η Ερώτηση 7 αποτελεί συνέχεια στην Ερώτηση 6 και διερευνά αν οι συνδρομητές έχουν αλλάξει τις ρυθμίσεις του δρομολογητή. Όπως είδαμε στην προηγούμενη ερώτηση ένα ποσοστό 30% δήλωσαν ότι γνωρίζουν πως να αλλάξουν τις ρυθμίσεις του δρομολογητή. Από αυτούς μόνο το 26% δήλωσε πως έχει κάνει κάποιες αλλαγές στις ρυθμίσεις του ασύρματο τους δικτύου. Επομένως ένα συνολικό ποσοστό 74% δεν έχει κάνει τέτοιες αλλαγές, είτε γιατί δεν γνωρίζει (το μεγαλύτερο μέρος) είτε γιατί αμέλησε ή δεν το έκρινε σκόπιμο. Επομένως ένα μεγάλο μέρος των οικιακών ασυρμάτων δικτύων παραμένουν ευάλωτα εξαιτίας είτε άγνοιας βασικών θεμάτων ασφάλειας είτε λόγω αμέλειας.

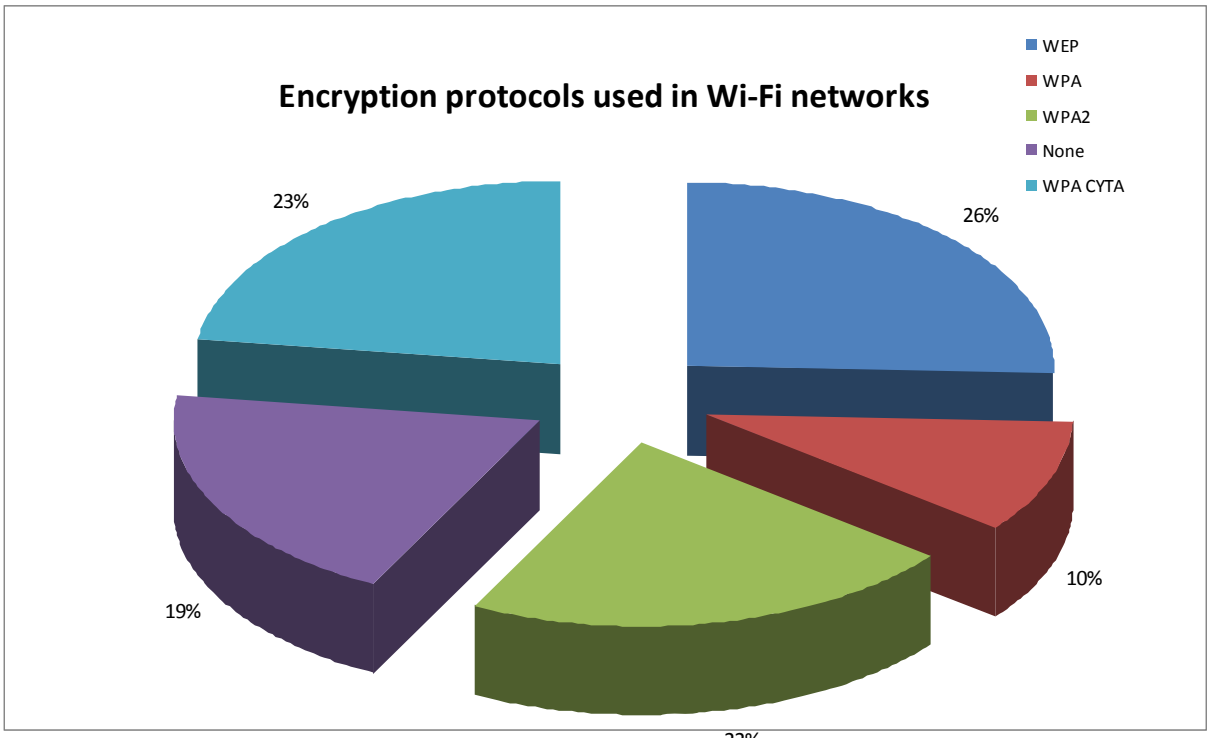
Εικόνα 22: Ερώτηση 8 από το ερωτηματολόγιο

Η Ερώτηση 8 αφορά αυτούς που δήλωσαν ότι έχουν κάνει αλλαγές στις ρυθμίσεις του ασυρμάτου τους δικτύου (το 26% του συνολικού δείγματος). Από αυτούς το 34%–35% έχει αλλάξει το όνομα (SSID) του ασυρμάτου δικτύου και τον κωδικό πρόσβασης που είναι οι δύο πιο σημαντικές ρυθμίσεις που θα έπρεπε να αλλάζουν όλοι οι κάτοχοι ασυρμάτων δικτύων. Βεβαίως ακόμη και με τις αλλαγές αυτές το ασύρματο δίκτυο δεν είναι απολύτως ασφαλές. Πολύ λίγοι έχουν χρησιμοποιήσει MAC filtering ή έχουν αποκρύψει το SSID του δικτύου τους, μέτρα που προσθέτουν αυξάνουν την ανεπιθύμητη πρόσβαση σε ένα ασύρματο δίκτυο (χωρίς όμως να το ασφαλίζουν πλήρως). Το 13% του δείγματος απάντησε ότι κλείνει ή έχει απενεργοποιήσει το ασύρματο του δίκτυο. Αυτό αποτελεί μια λύση για να κάνεις ασφαλές το δίκτυο σου αλλά χάνεις την δυνατότητα να χρησιμοποιείς την τεχνολογία του ασυρμάτου δικτύου και περιορίζεσαι στα καλώδια. Από την άλλη όταν κάποιος να κλείνει το ασύρματο δίκτυο όταν δεν το χρησιμοποιεί είναι σίγουρος μεν ότι κανείς δεν μπορεί να συνδεθεί σε αυτό κατά την διάρκεια που μένει κλειστό αλλά τί γίνεται όταν αυτό είναι ανοικτό και χρησιμοποιείται; Η απενεργοποίηση του ασυρμάτου δικτύου

μας παραπέμπει και στην Ερώτηση 3 (δες Εικόνα 17) όπου το 9% του δείγματος δήλωσε ότι δεν χρησιμοποιεί το ασύρματο του δίκτυο. Πιθανότατα κάποιοι από αυτούς το κάνουν για λόγους ασφάλειας.

Εικόνα 23: Ερώτηση 9 από το ερωτηματολόγιο

Η Ερώτηση 9 εξειδικεύει περισσότερο την Ερώτηση 8 εστιάζοντας σε πιο πρωτόκολλο κρυπτογράφησης χρησιμοποίησαν οι χρήστες για την ασφάλιση του ασύρματου τους δικτύου. Ο σκοπός της ερώτησης αυτής είναι να ελέγξουμε αν χρησιμοποιούν ισχυρό πρωτόκολλο ασφαλείας ή ευάλωτο. Οι απαντήσεις δείχνουν ότι 45% των χρηστών χρησιμοποιούν το WEP (το οποίο είναι το πιο ευάλωτο). 32% του δείγματος χρησιμοποιεί το WPA2 και 22% το WPA. Τα αποτελέσματα αυτά επιβεβαιώνονται και από την μελέτη καταγραφής μέσω του Wardriving (δες Εικόνα 24). Συνοπτικά οι χρήστες που χρησιμοποιούν το WEP πρωτόκολλο (45%) δεν είναι σχεδόν καθόλου προστατευμένοι ενώ οι υπόλοιποι είναι σχετικά ασφαλείς.



Εικόνα 24: Χρήση των πρωτοκόλλων ασφαλείας με βάση το wardriving

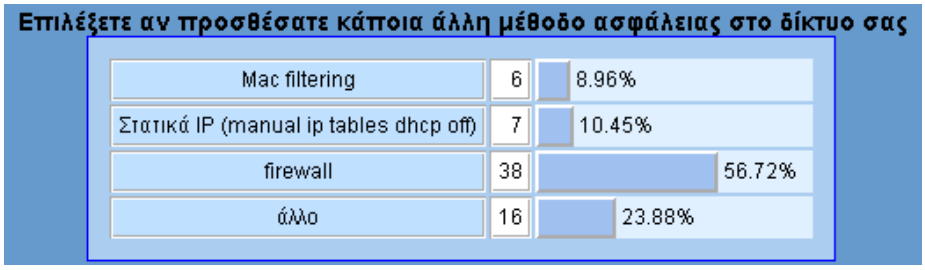
Η Ερώτηση 10 μας δίνει πιο λεπτομερή εικόνα για το θέμα του κωδικού ασφάλειας (security key). Στην ερώτηση κατά πόσο αλλάζουν τον κωδικό πρόσβασης, το 50% απάντησαν ποτέ

όλοι σχεδόν οι υπόλοιποι κάποτε. Το να αλλάζεις κωδικό είναι καλός τρόπος να προστατεύεσαι αλλά αν το πρωτόκολλο ασφαλείας είναι το WEP όσες φορές και να αλλάξει ο κωδικός πρόσβασης είναι θέμα 10 λεπτών κάποιος να βρει τον κωδικό και να έχει πρόσβαση στο δίκτυο ξανά.

Εικόνα 25: Συχνότητα αλλαγής του κωδικού πρόσβασης (Ερώτηση 10)

Η Ερώτηση 11 στόχευε σε πιο έμπειρους χρήστες και μάλιστα για αυτούς που έχουν επαρκείς γνώσεις για δίκτυα υπολογιστών. Αφορούσε το αν οι κάτοχοι του ασυρμάτου δικτύου πρόσθεσαν κάποια επιπλέον μέθοδο ασφάλειας στο δίκτυο τους. Επειδή δεν υπήρχε δυνατότητα απαρίθμησης όλων των μεθόδων στο ερωτηματολόγιο αναφέρθηκαν κυριότερες και απλούστερες.

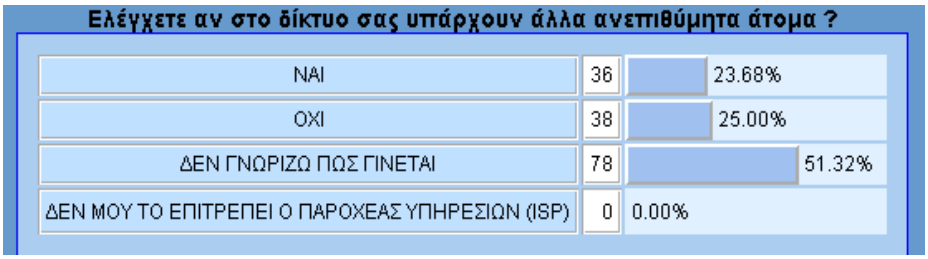
Το 56% των χρηστών απάντησαν ότι χρησιμοποιούν firewall αλλά αυτό είναι συνήθως προεγκατεστημένο στους δρομολογητές που αγοράζουμε άρα δεν ξέρουμε ακριβώς αν έκαναν αλλαγές στο firewall ή αν απλά γνωρίζουν ότι υπάρχει ήδη ενεργοποιημένο στο δρομολογητή. 9% απάντησαν ότι πρόσθεσαν φίλτρο με MAC addresses και 10% ότι έχουν ορίσει στατικά IP, μέθοδος που, κατά την γνώμη μου, είναι η καλύτερη για να προστατεύσεις το δίκτυο σου από ανεπιθύμητα άτομα. Το υπόλοιπο 24% του δείγματος απάντησε ότι πρόσθεσε κι άλλες μεθόδους ασφάλειας στο δίκτυο.



Εικόνα 26: Μέθοδοι ασφάλισης οικιακού ασυρμάτου δικτύου (Ερώτηση 11)

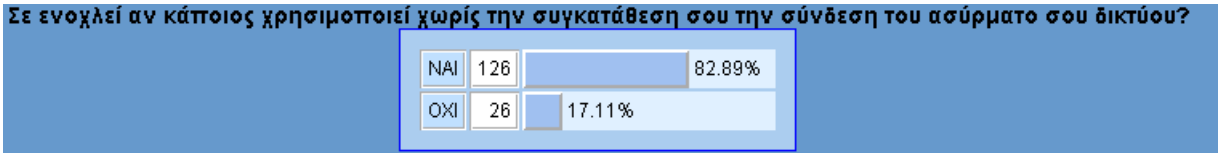
Η Ερώτηση 12 είναι από τις σημαντικότερες όσον αφορά την ασφάλεια των οικιακών ασυρμάτων δικτύων. Διερευνά το αν ελέγχουν οι ιδιοκτήτες του ασυρμάτου δικτύου αν υπάρχουν ανεπιθύμητα άτομα συνδεδεμένα σε αυτό. Δυστυχώς όμως το 51% του δείγματος μας απάντησε πως δεν γνωρίζει πως να ελέγχει αν ανεπιθύμητα άτομα βρίσκονται συνδεδεμένα στο δίκτυο τους. Το 25% απάντησε πως δεν ελέγχει και μόνο το 24% δήλωσε πως ελέγχει αν υπάρχουν ανεπιθύμητα άτομα. Συνολικά το ποσοστό αυτών που δεν

ελέγχουν ποιοι είναι συνδεδεμένοι στο δίκτυο τους ανέρχεται σε 76%. Το ποσοστό αυτό είναι πολύ μεγάλο και δημιουργεί ανησυχίες όσον αφορά την ασφάλεια των οικιακών ασυρμάτων δικτύων.



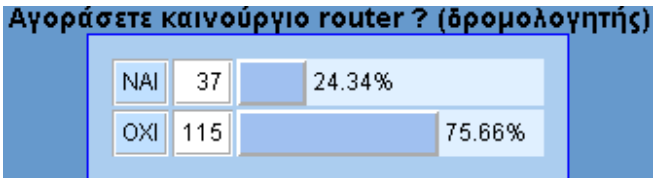
Εικόνα 27: Ερώτηση 12 του ερωτηματολογίου

Στην Ερώτηση 13 ρωτάμε τους χρήστες αν τους ενοχλεί να χρησιμοποιεί κάποιος το ασύρματο τους δικτύου χωρίς τη συγκατάθεση τους. Οι περισσότεροι (83%) δήλωσαν ότι τους ενοχλεί αλλά εντύπωση προκαλεί το 17% του δείγματος που δήλωσε πως δεν τους ενδιαφέρει αν κάποιος άλλος χρησιμοποιεί το ασύρματο τους δίκτυο.

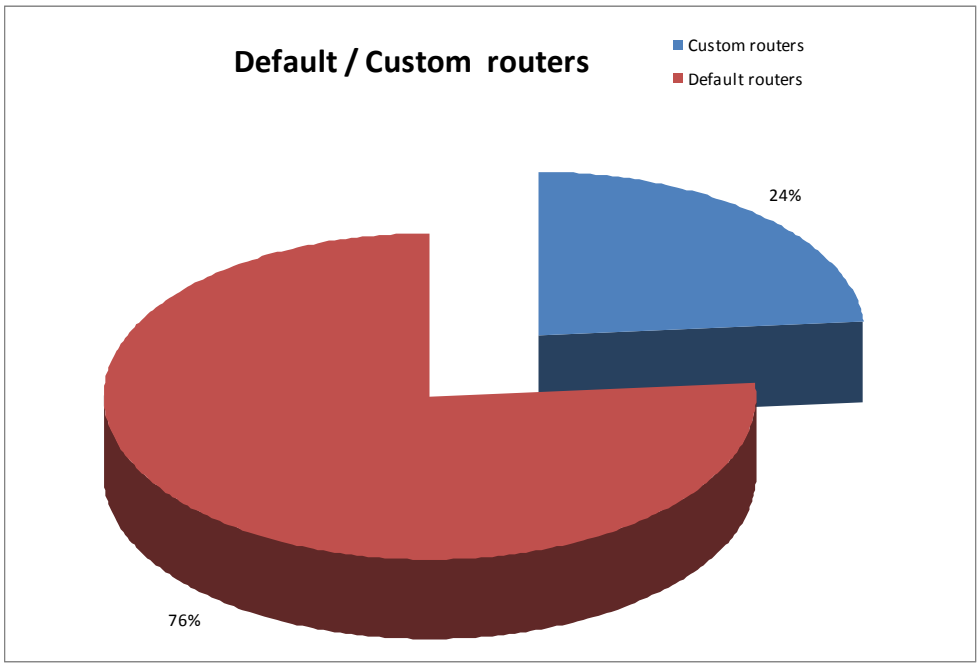


Εικόνα 28: Ερώτηση 13 του ερωτηματολογίου

Η Ερώτηση 14 διερευνά αν οι χρήστες αγόρασαν καινούργιο router, είτε γιατί θέλουν να έχουν τις δικές τους ρυθμίσεις είτε γιατί δεν τους αρκεί η συσκευή που τους δίνει ο πάροχος ISP. Οι περισσότεροι φαίνεται ότι μένουν ικανοποιημένοι με την συσκευή που τους παρέχεται δωρεάν. Μόνο 24% του δείγματος αγόρασαν καινούργιο δρομολογητή. Τα αποτελέσματα αυτά επιβεβαιώνονται πλήρως και από τη μελέτη wardriving όπως φαίνεται στο διάγραμμα της Εικόνας 30 (δες το 2ο μέρος της μελέτης για περισσότερες πληροφορίες).



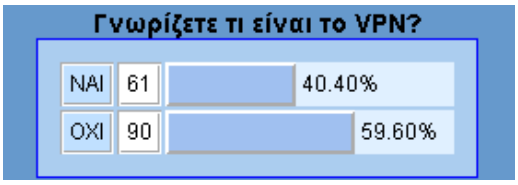
Εικόνα 29: Ερώτηση 14 του ερωτηματολογίου



Εικόνα 30: Ποσοστό δρομολογητών που παρέχονται από τις εταιρείες ISP και αυτών που αγοράζουν οι χρήστες

Στις Ερωτήσεις 15-18 ερευνούμε τις γνώσεις των χρηστών τεχνικές ονομασίες-θέματα που σχετίζονται με την ασφάλεια τόσο των ασυρμάτων δικτύων όσο και της μεταφοράς δεδομένων μέσα από αυτά.

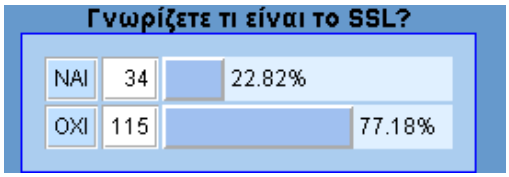
Η Ερώτηση 15 αφορά το VPN. Πολλά άτομα από το δείγμα το γνώριζαν ως μια μέθοδο σύνδεσης από το σπίτι στο δίκτυο του πανεπιστημίου, στη βιβλιοθήκη του πανεπιστημίου και στη δουλειά τους. Πολύ λίγοι γνωρίζουν ότι με το VPN τα δεδομένα μεταφέρονται με ασφάλεια στο δίκτυο χωρίς να μπορεί να τα υποκλέψει κάποιος. Το 60% του δείγματος δήλωσε ότι δε γνωρίζει τι είναι το VPN ποσοστό αρκετά υψηλό, αν και στην πράξη το ποσοστό αυτό να είναι μεγαλύτερο.



Εικόνα 31: Ερώτηση 15 του ερωτηματολογίου: VPN

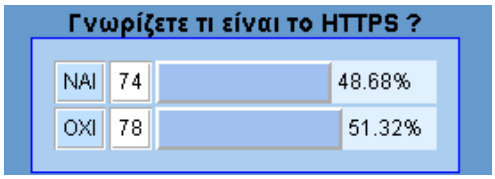
Η Ερώτηση 16 είχε θέμα το SSL το οποίο είναι το βασικότερο πρωτόκολλο κρυπτογράφησης ευαίσθητων δεδομένων για μεταφορά τους μέσω του Web. Συναλλαγές με τράπεζες αλλά και οποιαδήποτε εμπορική συναλλαγή (αγορά προϊόντων και υπηρεσιών) πραγματοποιούνται με την υποστήριξη του SSL. Δυστυχώς το 77% του δείγματος δεν γνωρίζει τι είναι το SSL. Τα άτομα αυτά θα μπορούσαν να παγιδευτούν από ιστότοπους

που ζητούν προσωπικά στοιχεία και δεν παρέχουν κρυπτογράφηση των δεδομένων που ανταλλάσσονται με συνέπειες που δύσκολα μπορεί κάποιος να αναλογιστεί.



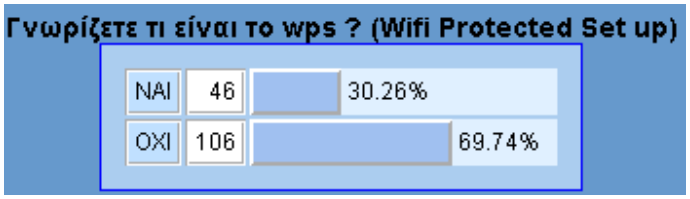
Εικόνα 32: Ερώτηση 16 του ερωτηματολογίου: SSL

Η Ερώτηση 17 αφορούσε το HTTPS το οποίο είναι στην ουσία επέκταση του απλού πρωτοκόλλου HTTP με ενσωμάτωση του SSL. Εδώ έχουμε το παράδοξο οι χρήστες να μην γνωρίζουν τι είναι το SSL και να γνωρίζουν τη είναι το HTTPS. Συγκεκριμένα στη προηγούμενη ερώτηση οι περισσότεροι δεν γνώριζαν τι είναι το SSL αλλά εδώ το 49% απάντησε ότι γνωρίζει τι είναι το HTTPS. Πιθανότατα είναι απλά εξοικειωμένοι με το https που απαντάται στα URL (https://www.....) αλλά είναι διαφορετικό πράγμα να έχεις δει κάτι από το να γνωρίζεις τι είναι.



Εικόνα 33: Ερώτηση 17 του ερωτηματολογίου: HTTPS

Η Ερώτηση 18 του ερωτηματολογίου αφορά μια τεχνολογία που είναι μεν βοηθητική για τους άπειρους χρήστες αλλά μπορεί να αφήσει ευάλωτους πολλούς χρήστες που έχουν ένα ασφαλισμένο δίκτυο. Παρά το γεγονός ότι το WPS σήμερα βρίσκεται σχεδόν σε όλες τις καινούργιες συσκευές ασύρματης δικτύωσης ελάχιστοι γνωρίζουν τη λειτουργία του. Αυτό αποδεικνύεται και από το δείγμα μας όπου το 70% απάντησε ότι δεν γνωρίζει τι είναι.

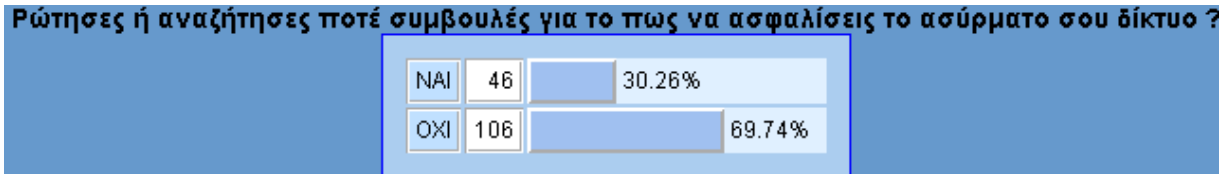


Εικόνα 34: Ερώτηση 18 του ερωτηματολογίου: WPS

Οι ερωτήσεις 19-21 αφορούν την διάθεση των χρηστών να ενημερωθούν σχετικά με τα θέματα ασφαλείας των ασυρμάτων δικτύων τους και κατά πόσο οι εταιρείες παροχής υπηρεσιών διαδικτύου έχουν προβλέψει τη συγκεκριμένη ανάγκη.

Από την Ερώτηση 19 προκύπτει ότι μόνο ένα 30% του δείγματος αναζήτησε πληροφορίες για την ασφάλεια του ασυρμάτου του δικτύου. Σε πρώτη ανάγνωση αυτό φαίνεται να

δείχνει αδιαφορία. Στην πραγματικότητα όμως, και με βάση τις απαντήσεις στις προηγούμενες ερωτήσεις, το ουσιαστικό πρόβλημα είναι η άγνοια των κινδύνων που δημιουργεί η χρήση ενός μη ασφαλισμένου ασυρμάτου δικτύου. Εφόσον δεν γνωρίζουμε το πρόβλημα φυσικό είναι να μην ρωτάμε και πληροφορίες για αυτό.

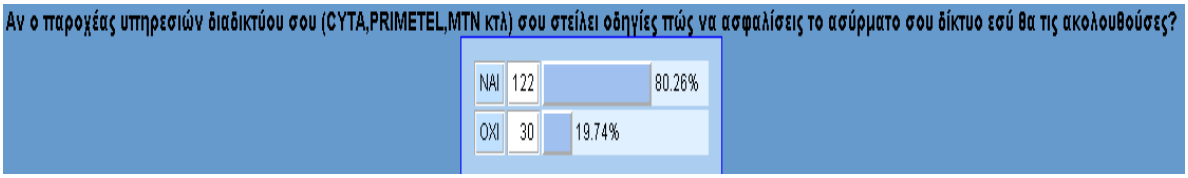


Εικόνα 35: Ερώτηση 19 του ερωτηματολογίου

Ερώτηση 20 ακολουθεί την 19: Οι χρήστες αμελούν να ρωτήσουν για την ασφάλεια του δικτύου τους αλλά τους δόθηκε η ευκαιρία να μάθουν από άλλες πηγές (πχ από τους ISP με σεμινάρια); Στην ερώτηση αν θέλουν να γνωρίσουν περισσότερα για την ασφάλεια των ασυρμάτων δικτύων το 83% απάντησε θετικά. Αυτό επιβεβαιώνει την προηγούμενη εκτίμηση που κάναμε ότι η άγνοια είναι το πρόβλημα και όχι οι αδιαφορία. Φαίνεται ότι οι άπειροι χρήστες χρειάζονται κάποια βοήθεια για να κτίσουν γνώση για το θέμα.

Εικόνα 36: Ερώτηση 20 του ερωτηματολογίου

Στην Ερώτηση 21 τα περισσότερα άτομα που ήταν θετικά στο να ενημερωθούν για το θέμα της ασφάλειας των ασυρμάτων δικτύων συμφώνησαν ότι αν πάρουν οδηγίες από την εταιρία που τους παρέχει πρόσβαση στο διαδίκτυο (ISP) θα τις ακολουθούσαν.



Εικόνα 37: Ερώτηση 21 του ερωτηματολογίου

Συμπεράσματα με βάση την έρευνα κοινής γνώμης

Συνοψίζοντας μπορούμε να παρατηρήσουμε ότι το δείγμα μας δεν ήταν επαρκώς ενημερωμένο όσον αφορά την ασφάλεια των ασυρμάτων δικτύων. Ο βασικότερος έλεγχος που θα μπορούσε κάποιος να κάνει για να ελέγξει την ασφάλεια του δικτύου του θα ήταν

να ελέγχει για ανεπιθύμητα άτομα που είναι συνδεδεμένα σε αυτό. έτσι ώστε να λάβει μέτρα. Στην περίπτωση του δείγματος μας αν υπολογίσουμε αυτούς που δεν γνωρίζουν πως γίνεται αυτό μαζί με αυτούς που γνωρίζουν αλλά δεν ελέγχουν φτάνουμε στο υψηλότατο ποσοστό του 76%! Ενδεχομένως αυτό να οφείλεται στο ότι δεν γνωρίζουν το ρίσκο το να υπάρχει κάποιος άγνωστος συνδεδεμένος στο δίκτυο τους. Οι εταιρίες ISP φαίνεται ότι δεν ενημερώνουν τους συνδρομητές τους για τους κινδύνους ενός ανασφάλιστου ασυρμάτου δικτύου και για μέτρα προστασίας. Προφανώς φοβούνται ότι ένα μέρος του κοινού θα τρομοκρατηθεί και ενδεχομένως να σταματήσει να είναι συνδρομητής. Επίσης το να εγείρεις ένα τέτοιο ζήτημα σημαίνει ότι είσαι διατεθειμένος να υποστηρίξεις τους χρήστες όταν ζητήσουν βοήθεια. Αυτό σημαίνει κόστος σε χρόνο και χρήμα. Όταν ρωτήσαμε το δείγμα στην ερώτηση 20 και 21 αν ήταν πρόθυμοι να γνωρίσουν περισσότερο και να λάβουν μέτρα αυτοί ήταν θετικοί. Άρα η έλλειψη ενημέρωσης οφείλεται στις εταιρίες και όχι στη διάθεση των χρηστών. Πολλοί παράγοντες μπορεί να επηρεάζουν την πολιτική των εταιρειών στο θέμα αυτό. Ένας από αυτούς είναι η αδυναμία των συσκευών που μας παρέχουν οι εταιρίες ISP να μας προστατεύουν χωρίς να πρέπει εμείς να παρέμβουμε και να κάνουμε αλλαγές. Σε πολλές περιπτώσεις άγνωστοι μπορούν να έχουν πρόσβαση σε δίκτυο, το οποίο παραμένει με τις εκ προοιμίου (default) ρυθμίσεις, μέσω λογισμικών που μετατρέπουν το όνομα του ασυρμάτου δικτύου (SSID) σε ανάλογο κωδικό. Το πώς αυτό επιτυγχάνεται θα μας απασχολήσει στην επόμενη ενότητα.

Μεγάλο ποσοστό του δείγματος μας δεν είχε βασικές γνώσεις για τα ασύρματα δίκτυα και την ασφάλεια τους. Πολύ λίγοι χρήστες αγόρασαν καινούργιο δρομολογητή για να αντικαταστήσουν αυτόν που τους παρείχε η εταιρία ISP, ο οποίος σε αρκετές περιπτώσεις δεν επιδέχεται αλλαγές στις ρυθμίσεις. Ακόμη όμως και τα άτομα που αγόρασαν καινούργιο δρομολογητή δεν επέλεξαν την καλύτερη πολιτική ασφάλειας. Το 50% των ατόμων που πρόσθεσαν δικό τους κωδικό χρησιμοποίησαν πρωτόκολλο κρυπτογράφησης το WEP το οποίο είναι πολύ εύκολο να παραβιαστεί.

Οι καινούργιοι δρομολογητές έρχονται με WPS προ-εγκατεστημένο. Αυτό είναι σε πολλές περιπτώσεις επικίνδυνο όσον αφορά την ασφάλεια του ασυρμάτου μας δικτύου. Εντούτοις το 70% του δείγματος (ερώτηση 18) δεν γνώριζε καν τον όρο WPS.

Στις ερωτήσεις 15-18 όπου μελετούσαμε τις βασικές γνώσεις που θα έπρεπε να έχει κάποιος για να έχει ασφαλή χρήση ασυρμάτων δικτύων είχαμε απογοητευτικά αποτελέσματα. Όταν το 77% των χρηστών δεν γνωρίζει τι είναι το SSL το πιο πιθανό να μην γνωρίζει ούτε τι είναι τα Phishing attacks όπου μια ψεύτικη σελίδα (πχ http://yahoorrr.com) κατασκευάζετε ώστε να μοιάζει με μία αληθινή (http://yahoo.com) με στόχο την υποκλοπή κωδικών από τους χρήστες οι οποίοι εισάγουν τα στοιχεία των προσωπικών τους λογαριασμών νομίζοντας πως βρίσκονται στην πραγματική σελίδα.

Ακόμη μεγαλύτερο προβληματισμό δημιουργούν τα αποτελέσματα στις Ερωτήσεις 5 και 6 όπου το δείγμα εμφανίζεται να μην γνωρίζει πως να αλλάξει τις ρυθμίσεις του δρομολογητή αλλά ούτε καν το όνομα του ασυρμάτου του δικτύου. Αν κάποιος δημιουργήσει δικό του δρομολογητή με το ίδιο όνομα και κάνει redirect του χρήστες στο δίκτυο του, το δείγμα μας δεν θα γνωρίζει ότι βρίσκεται σε άγνωστο δίκτυο και ότι τα

δεδομένα του μπορούν να κλαπούν αν δεν χρησιμοποιηθεί το πρωτόκολλο HTTPS και η τεχνολογία VPN (η γνώση των οποίων όπως προκύπτει από την έρευνα μας είναι περιορισμένη ανάμεσα στο δείγμα) μέσω της οποίας δημιουργείται ένα τρίτο κανάλι όπου μεταφέρονται τα δεδομένα με ασφάλεια.

Συνολικά μόνο το 20-30% του δείγματος μας μπορούμε να πούμε πώς βρίσκονται σε θέση να αντιμετωπίσουν τα θέματα ασφάλειας του ασυρμάτου τους δικτύου με επιτυχία. Το υπόλοιπο ποσοστό δυστυχώς δεν είχε τις γνώσεις και παραμένουν ευάλωτα τόσο τα άτομα όσο και τα ασύρματα τους δίκτυα.

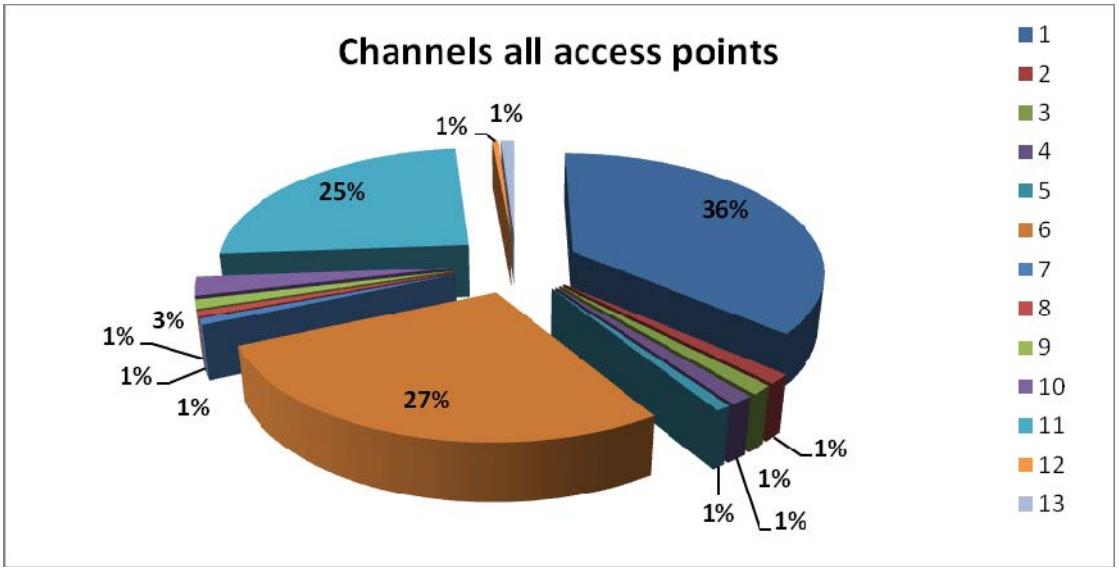
Τα αποτελέσματα που συλλέξαμε με το ερωτηματολόγιο μπορούν να απαντήσουν κάποια από τα ερευνητικά ερωτήματα αλλά προτού καταλήξουμε σε μια ολοκληρωμένη εικόνα θα πρέπει να μιλήσουμε για το πρακτικό μέρος όπου έλεγξα τα δίκτυα που βρίσκονταν στον αέρα και με περεταίρω μελέτη, ταξινόμηση και εφαρμογή τα παρουσίασα με τρόπο ώστε να φαίνονται όλα τα σημαντικά στοιχεία που χρειαζόμαστε για να μπορούμε να ολοκληρώσουμε τα συμπεράσματα μας.

Wardriving

Όπως αναφέρθηκε νωρίτερα στο πρακτικό μέρος της έρευνας καταγράφηκαν, με την τεχνική του wardriving, 7070 ασύρματα δίκτυα. Μετά την αφαίρεση των διπλών καταχωρήσεων, με την τεχνική που αναλύθηκε στην ενότητα της μεθοδολογίας. είχαμε 4932 διαφορετικά ασύρματα δίκτυα, αριθμός αρκετά υψηλός για να έχουμε αντιπροσωπευτικά συμπεράσματα, δεδομένου ότι η περιοχή που εξετάστηκε δεν πρέπει να περιλαμβάνει περισσότερα από 20000 νοικοκυριά, από τα οποία δεν έχουν όλα σύνδεση στο διαδίκτυο αλλά ακόμη και αν έχουν δεν έχουν υποχρεωτικά ασύρματο δίκτυο.

Χρήση ασυρμάτων καναλιών

Στην πρώτη εικόνα της μελέτης βλέπουμε τα κανάλια στα οποία χρησιμοποιούσαν τα ασύρματα δίκτυα στο δείγμα μας. Τα 3 κανάλια τα οποία βρίσκουμε πιο συχνά είναι 1, 6, και 11. Οι χρήστες που βρίσκονται στις συχνότητες αυτών των καναλιών προφανώς να έχουν διακοπές ή μη καθαρό σήμα με παρεμβολές. Αυτό παρατηρείτε όταν υπάρχουν πολλά σήματα στην ίδια συχνότητα και η καλύτερη λύση για αυτό το πρόβλημα είναι οι χρήστες να επιλέξουν άλλο κανάλι με διαφορετική συχνότητα (εκτός 1,6,11). Γεγονός που δεν παρατηρούμε να γίνεται γιατί τα υπόλοιπα κανάλια (εικόνα 1 από την μελέτη) έχουν μόνο ποσοστά του ενός τις εκατό. Αν συγκρίνουμε τα καινούργια αποτελέσματα (εικόνα 1 από την μελέτη) με αυτά που βρέθηκαν στην έρευνα του *Bestuzhev* (Εικόνα 1[α]) παρατηρούμε ότι είναι περίπου τα ίδια άρα δεν έχει αλλάξει κάτι σε αυτή την περίπτωση. Οι εταιρίες και οι δρομολογητές έχουν προεπιλεγμένα αυτά τα κανάλια και οι χρήστες δεν μπαίνουν στον κόπο να τα αλλάξουν.



Εικόνα 38: Χρήση των επιμέρους καναλιών στα ασύρματα δίκτυα με βάση την έρευνα μας

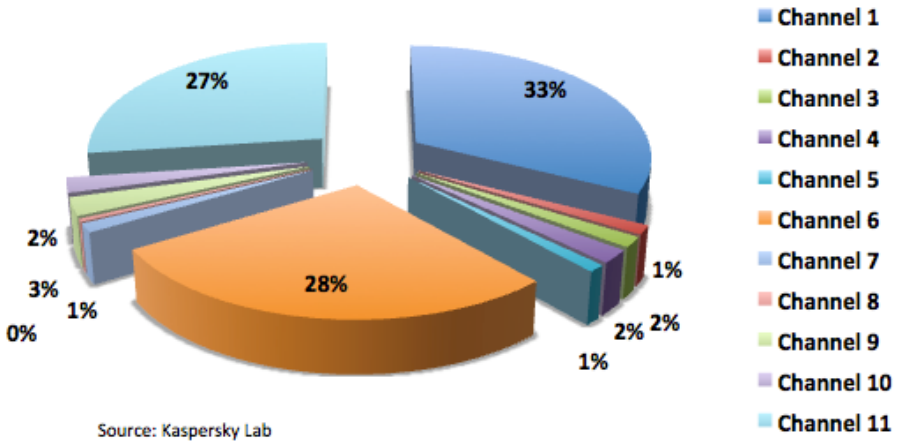


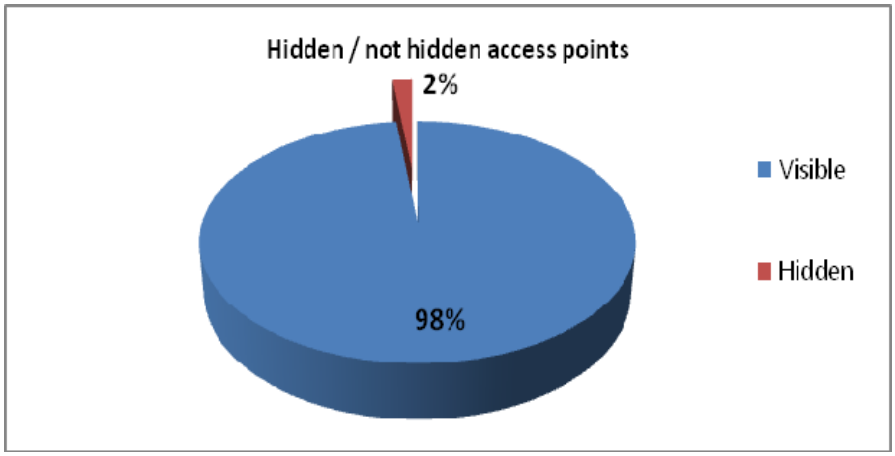
Image from: http://www.securelist.com/en/blog/2186/SAS2010_Wardriving_in_Limassol_Cyprus

Εικόνα 39: Χρήση των επιμέρους καναλιών στα ασύρματα δίκτυα με βάση την έρευνα του Bestuzhev [4]

Αόρατα και ορατά δίκτυα

Με βάση την έρευνα Wardriving μόνο 2% των ασυρμάτων δικτύων δεν κάνουν broadcast το SSID τους (είναι δηλαδή αόρατα – βλέπε Εικόνα 40). Όπως είδαμε νωρίτερα η απόκρυψη του SSID είναι μια μέθοδος προστασίας ενάντια σε ανεπιθύμητους χρήστες. Θα έπρεπε, επομένως, να υπάρχουν περισσότερα αόρατα δίκτυα κυρίως σε μεγάλες εταιρίες και φορείς υπηρεσιών.

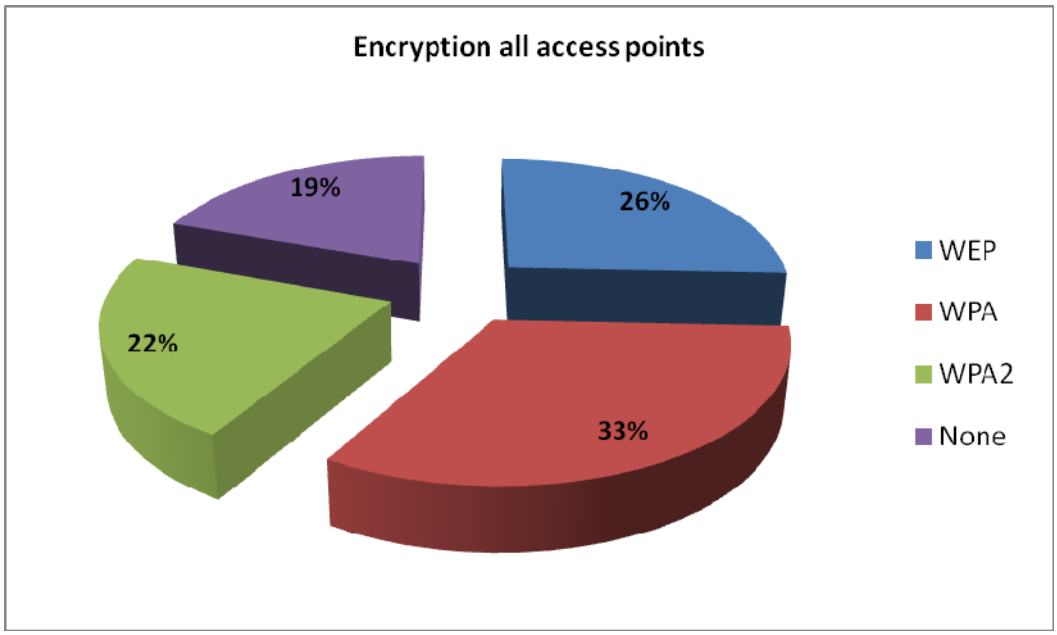
Συγκρίνοντας τα αποτελέσματα της μελέτης με αυτή του ερωτηματολογίου (Ερώτηση 8) παρατηρούμε μια μικρή απόκλιση όσον αφορά τους χρήστες που κάνουν απόκρυψη του SSID του δικτύου τους. Συγκεκριμένα ένα 6.58% (σε αντίθεση με το 2% που έδειξε η μελέτη) αυτών που απάντησαν το ερωτηματολόγιο δήλωσαν ότι χρησιμοποιούν απόκρυψη του SSID ως μέθοδο προστασίας. Προφανώς η συγκεκριμένη επιλογή στην Ερώτηση 8 δεν ήταν πλήρως κατανοητή στους χρήστες.



Εικόνα 40: Ποσοστό ορατών και αόρατων ασυρμάτων δικτύων

Πρωτόκολλα κρυπτογράφησης

Στο κομμάτι αυτό της μελέτης παρουσιάζουμε τα αποτελέσματα της μελέτης Wardriving όσον αφορά τα πρωτόκολλα κρυπτογράφησης που χρησιμοποιούνται στα ασύρματα δίκτυα. Με βάση την Εικόνα 41 παρατηρούμε τη χρήση των τριών διαφορετικών μεθόδων κρυπτογράφησης που υπάρχουν σήμερα (WEP, WPA, WPA2) καθώς και το ποσοστό των δικτύων που δεν χρησιμοποιούν καμία μέθοδο κρυπτογράφησης. Το 26% που χρησιμοποιεί WEP και το 19% που δεν χρησιμοποιεί κανένα πρωτόκολλο κρυπτογράφησης είναι ευάλωτοι σε επιθέσεις και υποκλοπή δεδομένων.



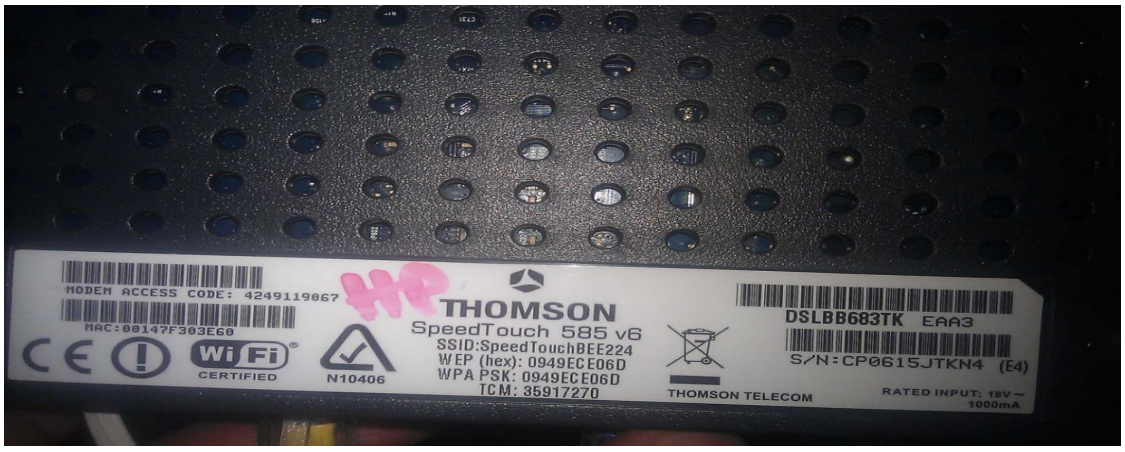
Εικόνα 41: Χρήση πρωτοκόλλων κρυπτογράφησης

Μεγάλος αριθμός δικτύων που φαίνεται ότι δεν χρησιμοποιούν κάποιο πρωτόκολλο κρυπτογράφησης αφορούν ασύρματα δίκτυα με τεχνολογία RADIOUS (δηλαδή hotspots). Αυτός είναι και ο λόγος που υπάρχει απόκλιση με τα αντίστοιχα αποτελέσματα από το ερωτηματολόγιο και την Ερώτηση 9. Επί της ουσίας πάντως η χρήση των hotspots χωρίς ενημέρωση για τους κινδύνους που αυτό σημαίνει δημιουργεί ένα σημαντικό θέμα υποβάθμισης ασφάλειας των χρηστών. Οι περισσότεροι από εμάς δεν γνωρίζουμε την επικινδυνότητα να συνδέεσαι σε ένα δίκτυο RADIOUS (πχ πανεπιστήμιο και αεροδρόμιο) ή σε δίκτυο που να μην είναι ασφαλισμένο με κωδικό, πχ σε κατάστημα ή καφετέρια. Τα δεδομένα μεταφέρονται χωρίς προστασία και αν δεν χρησιμοποιηθεί ένα είδος ασφαλούς σύνδεσης (πχ SSL, HTTPS, VPN) τότε τα δεδομένα είναι εύκολο να υποκλαπούν. Για το λόγο αυτό θα πρέπει να αποφεύγουμε να χρησιμοποιούμε ανοικτά δίκτυα που δεν γνωρίζουμε ποια άτομα είναι συνδεδεμένα σε αυτά ή όταν τα χρησιμοποιούμε να δημιουργούμε μια ασφαλή σύνδεση μέσω VPN.

Όσον αφορά τα πρωτόκολλα κρυπτογράφησης υπάρχει ακόμη ένα πρόβλημα στην Κύπρο (αλλά και σε άλλες χώρες). Πολλές εταιρίες ISP προμηθεύουν τους συνδρομητές τους με

δρομολογητές οι οποίοι έχουν όλες τις ρυθμίσεις προκαθορισμένες και είναι έτοιμοι για άμεση χρήση. Αυτό θεωρητικά δεν είναι πρόβλημα. Αν όμως δεν ενημερωθούν οι χρήστες να αλλάξουν τις ρυθμίσεις αυτές ή πώς να προστατεύονται τότε οι αρχικές ρυθμίσεις μπορεί να μην αλλάξουν ποτέ και να αποτελέσουν ένα αδύνατο σημεία ασφάλειας. Για παράδειγμα η CYTA, η πιο δημοφιλής εταιρία παροχής υπηρεσιών διαδικτύου στην Κύπρο, δίνει δρομολογητές στους συνδρομητές τους που έχουν καθορισμένες όλες τις ρυθμίσεις από πριν (το όνομα SSID του ασύρματου δικτύου, το κανάλι λειτουργίας, ο κωδικός πρόσβασης κτλ). Η CYTA προμηθεύεται δρομολογητές από την Thomson η οποία είναι μια Βελγική εταιρία που κατασκευάζει, ανάμεσα σε άλλα ηλεκτρονικά ήδη, συσκευές για διάφορες εταιρείες ISP σε διάφορες χώρες. Οι ρυθμίσεις στους δρομολογητές γίνονται αυτόματα από την εταιρία αυτή. Για παράδειγμα ο κωδικός πρόσβασης δημιουργείται με βάση τον σειριακό αριθμό του δρομολογητή. Άλλες εταιρείες χρησιμοποιούν το MAC address της συσκευής για να δημιουργήσουν τον κωδικό και το SSID κτλ. Στην περίπτωση όμως των δρομολογητών της Thomson η διαδικασία με την οποία παράγεται ο κωδικός και το όνομα του ασυρμάτου δικτύου έχει αποκωδικοποιηθεί από τον Kevin Devine, ο οποίος εφάρμοσε τεχνικές αντίστροφης μηχανικής (reverse engineering) σε ένα CD εγκατάστασης δρομολογητών της Thomson το οποίο χρησιμοποιείται για επανεγκατάσταση των ρυθμίσεων των δρομολογητών της Thomson[6].

Ο Kevin Devine μέσω του CD εγκατάστασης κατάφερε να βρει ότι ο κωδικός και η ονομασία του ESSID προέρχονται από μια συνάρτηση τεμαχισμού (hash function) που δημιουργείται από ένα τμήμα του σειριακού αριθμού (serial number) κάθε συσκευής. Για να γίνει αντιληπτή η συγκεκριμένη διαδικασία ας δούμε ένα συγκεκριμένο παράδειγμα από έναν δρομολογητή της CYTA (βλέπε Εικόνα 42):



Εικόνα 42: Το πίσω μέρος ενός δρομολογητή της THOMSON

Όπως παρατηρούμε υπάρχουν όλες οι λεπτομέρειες του δρομολογητή στο πίσω μέρος: Όνομα SSID (SpeedTouchBEE224), κωδικός ασυρμάτου δικτύου (0949ECE06D) και σειριακός

6 http://www.itwire.com/business-it-news/security/30338-every-bigpond-speedtouch-router-wifi-password-vulnerable?start=1

αριθμός (CP0615JTKN4(E4)). Στους νέους δρομολογητές της CYTA στο όνομα SSID το SpeedTouch έχει αντικατασταθεί CYTA (άρα στο παράδειγμα μας αν ο δρομολογητής ήταν καινούριος το SSID θα ήταν CYTABEE224 αντί SpeedTouchBEE224).

Ο σειριακός αριθμός χωρίζεται στα ακόλουθα μέρη

CP YY WW PP XXX (CC)

CP 06 15 JT KN4 (E4) < -- παράδειγμα μας

YY	είναι η χρονολογία που κατασκευάστηκε	(2006)
WW	είναι η εβδομάδα που κατασκευάστηκε	(15)
PP	είναι ο κωδικός παραγωγής	(JT)
CC	είναι ο κωδικός διαμόρφωσης/ρύθμισης της συσκευής	(E4)
XXX	είναι (μάλλον) ένας τυχαίος κωδικός	(KN4)

Σο παράδειγμα μας ο σειριακός αριθμός είναι: CP 06 15 JT KN4 (E4). Για να αρχίσουμε την μετατροπή σε κωδικό πρόσβασης και όνομα SSID αφαιρούμε το CC και PP από τον σειριακό αριθμό. Στην περίπτωση μας ο κωδικός θα γίνει CP0615KN4, στην συνέχεια μετατρέπουμε τον XXX κωδικό (KN4) σε δεκαεξαδικό (hexadecimal) αριθμό χρησιμοποιώντας των κώδικα ASCII (K=>4B, N=>4E, 4=>34)[7]. Το KN4 σε ASCII αναπαράσταση γίνεται 4B4E34 και το προσθέτουμε στο τέλος του CP YY WW. Έτσι έχουμε τον αριθμό CP06154B4E34. Στη συνέχεια ο αριθμός αυτός κρυπτογραφείται με την συνάρτηση τεμαχισμού SHA-1 (Secure Hash Algorithm)[8] η οποία είναι μία διαδεδομένη μέθοδος κρυπτογράφησης. Ο αριθμός CP06154B4E34 που έχουμε μέχρι τώρα αν κρυπτογραφηθεί με τη συνάρτηση SHA-1 γίνεται:

0949ECE06D16BA67DB537AD084123F93A6BEE224

Αν παρατηρήσουμε τον αριθμό τα πρώτα 10 bytes είναι ο κωδικός πρόσβασης του δρομολογητή (WEP και WPA) μας και τα τελευταία 6 byte είναι ο εξαψήφιος αριθμός μετά την ονομασία SpeedTouch ή CYTA. Η Εικόνα 42 το επιβεβαιώνει και η συγκεκριμένη μεθοδολογία ακολουθείται σε όλους τους δρομολογητές που έχει κατασκευάσει μέχρι σήμερα η Thomson.

Η μέθοδος που χρησιμοποιήσαμε για να βρούμε τον κωδικό πρόσβασης προήλθε από το σειριακό αριθμό του δρομολογητή. Άλλοι ερευνητές ασφάλειας κατάφεραν να χρησιμοποιούν την ονομασία SSID του ασυρμάτου δικτύου και έτσι να «σπάσουν» μέσω brouteforce ή με hash tables (μέσω dictionaries που έχουν μέσα έτοιμα hashes) τον σειριακό αριθμό (ανάποδη μέθοδος, reverse engineering) και να βρουν τον κωδικό από το SHA-1 hash που παράγεται.

---

7 http://www.asciitable.com/

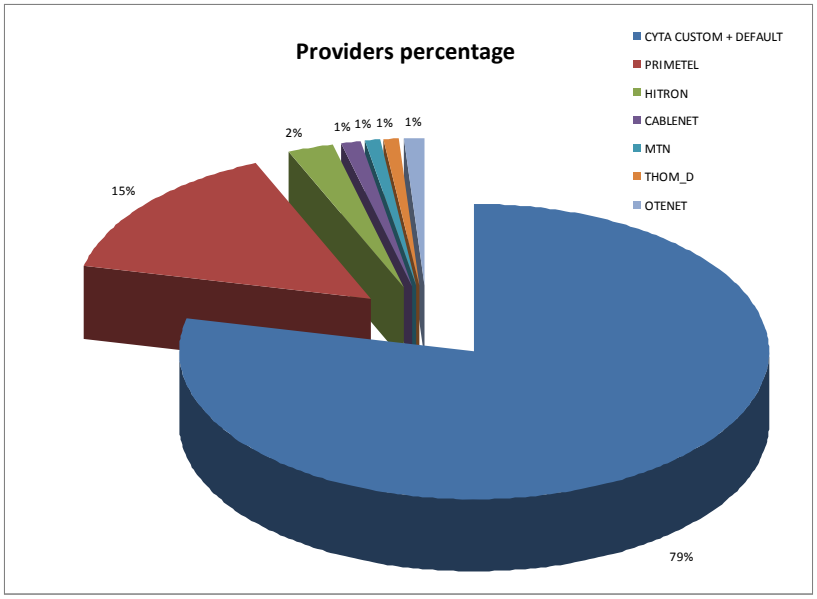
8 http://en.wikipedia.org/wiki/SHA-1

Το πρόβλημα είναι ότι η μέθοδος αυτή έχει γίνει πολύ πιο εύκολη με το χρόνο και έχουν δημιουργηθεί πολλά προγράμματα που μπορεί οποιοσδήποτε, ακόμη και με μηδενικές γνώσεις σε θέματα ασφάλειας ασυρμάτων δικτύων, να βρει τον κωδικό του δρομολογητή με ένα απλό πάτημα κουμπιού. Σκοπός των προγραμμάτων αυτών στην αρχή ήταν να ελέγχουν οι κάτοχοι ασυρμάτου δικτύου αν το δίκτυο τους ήταν ευάλωτο ή όχι μέσω του προγράμματος για να αλλάξουν τις ρυθμίσεις. Όμως τα περισσότερα άτομα το χρησιμοποιούν για να συνδεθούν σε ασύρματα δίκτυα χωρίς την συγκατάθεση των κατόχων τους. Όπως γίνεται εύκολα αντιληπτό στην Κύπρο το συγκεκριμένο πρόβλημα είναι οξύ γιατί οι περισσότεροι χρήστες ασυρμάτων δικτύων είναι συνδρομητές της CYTA. Επομένως βρίσκονται σε κίνδυνο αν δεν έχουν αλλάξει τις ρυθμίσεις του δρομολογητή τους.

Στο ερωτηματολόγιο που διεξήχθη το 70% των ερωτηθέντων δήλωσε ότι δεν γνώριζε να αλλάξει τις ρυθμίσεις του δρομολογητή (δες Ερώτηση 6 και Εικόνα 20) ενώ το 73% δήλωσε πως δεν έχει κάνει αλλαγές στον δρομολογητή (δες Ερώτηση 7 και Εικόνα 21). Όπως έχουμε δείξει ένας δρομολογητής ο οποίος παρέμεινε με τις εκ προοιμίου (default) ρυθμίσεις είναι ευάλωτος ακόμη και με το πάτημα ενός κουμπιού άσχετα αν ο κωδικός ασφαλείας ο οποίος χρησιμοποιείται είναι WEP ή WPA διότι όπως βλέπουμε στην Εικόνα 42 ο κωδικός είναι ο ίδιος τόσο στο WEP όσο και WPA.

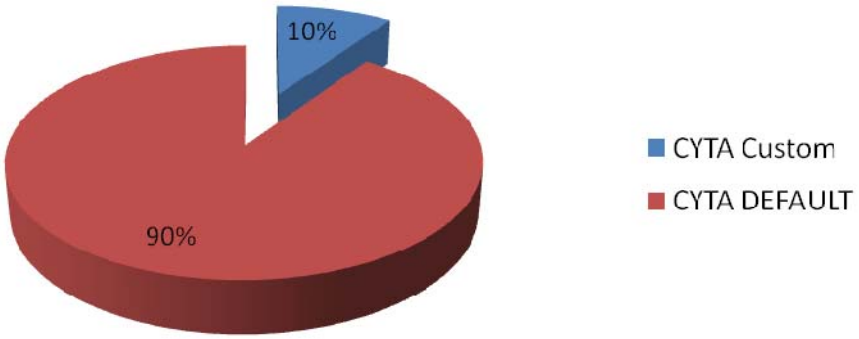
Επανερχόμενοι στα αποτελέσματα της Εικόνας 41 παρατηρούμε ότι πολλά από τα δίκτυα με πρωτόκολλα κρυπτογράφησης WPA και WEP ανήκουν στην CYTA και τα περισσότερα από αυτά πιθανότατα δεν έχουν τύχει αλλαγών διότι η ονομασία τους παραμένει CYTAXXXXXX (άρα υπολογίζουμε ότι το πιο πιθανόν να μην αλλάξει ούτε ο κωδικός πρόσβασης). Επομένως πολλά από αυτά τα δίκτυα είναι ευάλωτα άσχετα αν χρησιμοποιούν WPA το οποίο θεωρείται ασφαλές (λόγο των προγραμμάτων που βρίσκουν τον κωδικό από το SSID). Με μια απλή αλλαγή ονόματος SSID το πρόγραμμα εύρεσης κωδικού δεν μπορεί να λειτουργήσει αφού δεν έχει τα έξι ψηφία που χρειάζεται από τα τελευταία ψηφία του SHA-1 hash που δημιουργεί το όνομα SSID. Έτσι είναι πολύ πιο ασφαλές το δίκτυο. Από την άλλη αν ο χρήστης άλλαξε το όνομα SSID και χρησιμοποίησε πρωτόκολλο κωδικοποίησης WEP ή αν δεν χρησιμοποίησε καθόλου κωδικό τότε παραμένει ευάλωτος. Στο ερωτηματολόγιο μας παρατηρήθηκε κατ' επανάληψη η συγκεκριμένη περίπτωση αφού το 45% των χρηστών χρησιμοποίησαν WEP όταν άλλαξαν τις ρυθμίσεις του δρομολογητή (δες Ερώτηση 9 και Εικόνα 23).

Για να έχουμε καλύτερη εικόνα όσον αφορά την ασφάλεια του ασυρμάτου δικτύου συνδρομητών της CYTA χώρισα όλα τα ISP που είχαν καταγραφεί με το Wardriving ανάλογα με τον πάροχο υπηρεσιών διαδικτύου για να βρούμε πόσοι χρήστες της CYTA δεν άλλαξαν τις ρυθμίσεις (βλέπε Εικόνα 43).



Εικόνα 43: Εκτίμηση μεριδίου αγοράς εταιρειών ISP μέσω της πρακτικής μελέτης (wardriving)

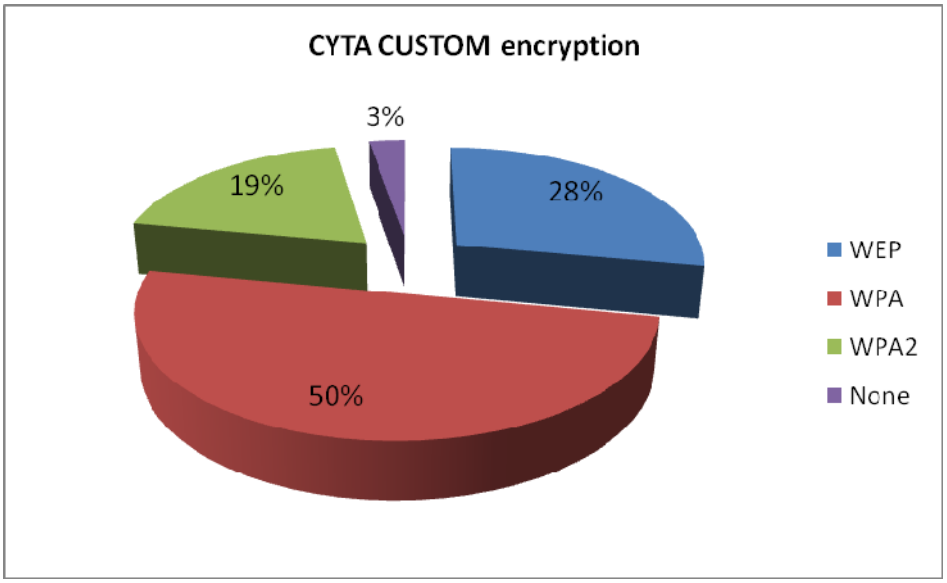
Από την Εικόνα 43 προκύπτει συντριπτική υπέρ της CYTA κατανομή του μεριδίου αγοράς ISP, γεγονός που δείχνει ότι το πρόβλημα με τις εκ προοιμίου ρυθμίσεις είναι πράγματι πολύ σοβαρό. Στην Εικόνα 44 της μελέτης χώρισα τα δίκτυα της CYTA σε αυτά που παραμένουν με τις εκ προοιμίου ρυθμίσεις και σε αυτά που στα οποία έχουν γίνει αλλαγές στην ονομασία SSID του δικτύου. Ο στόχος ήταν να έχουμε μια εκτίμηση όσον αφορά το ποσοστό των χρηστών που έχουν κάνει αλλαγές στους δρομολογητές της CYTA.



Εικόνα 44: Διατήρηση ή όχι του default ονόματος του δρομολογητή που παρέχει η CYTA

Με κόκκινο χρώμα στην Εικόνα 44 είναι τα δίκτυα της CYTA στα οποία οι χρήστες δεν έκαναν αλλαγές (SSID) στο ασύρματο τους δίκτυο (θεωρούνται ευάλωτα) και με μπλε χρώμα είναι τα δίκτυα στα οποία έχει αλλάξει τουλάχιστον το όνομα. Το συγκεκριμένο αποτέλεσμα είναι πράγματι ανησυχητικό: Μόνο το 10% των συνδρομητών της CYTA έχουν κάνει αλλαγές στους δρομολογητές τους (όπως αποδείχθηκε με έλεγχο του SSID για το όνομα και του MAC για τον κατασκευαστή του δρομολογητή).

Στην Εικόνα 45 διερεύνησα τις ρυθμίσεις των συνδρομητών της CYTA που έχουν κάνει αλλαγές στον δρομολογητή που τους παραχώρησε η εταιρεία.



Εικόνα 45: Πρωτόκολλα κρυπτογράφησης για τους συνδρομητές της CYTA που έχουν αλλάξει τις ρυθμίσεις του δρομολογητή τους.

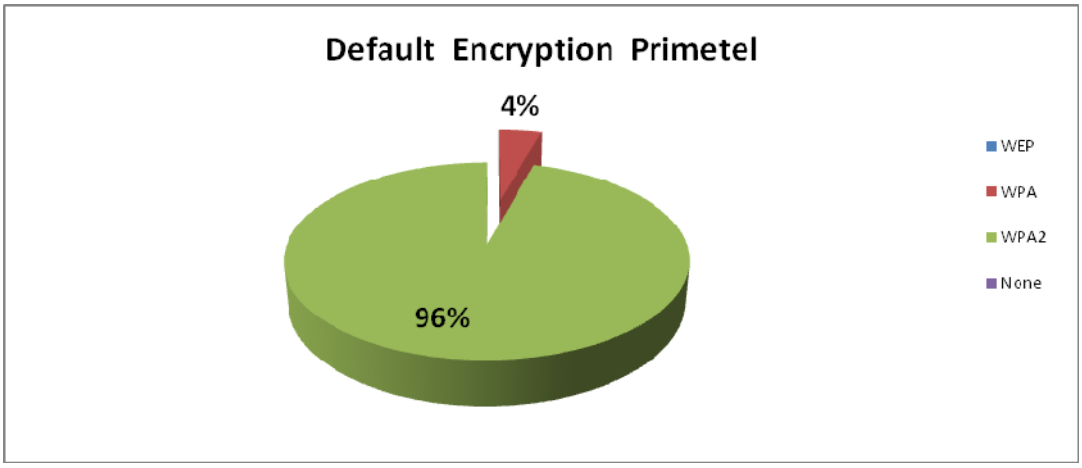
Τα αποτελέσματα σε αυτή την περίπτωση είναι θετικά, αλλά το δείγμα αυτό αφορά μόνο το 10% των ασυρμάτων δικτύων της CYTA. Ακόμη και σε αυτή την περίπτωση το 28% των συνδρομητών εξακολουθούν να χρησιμοποιούν WEP ενώ το 3% δεν χρησιμοποιεί κανένα κωδικό πρόσβασης.

Κλείνοντας με το θέμα των εκ προοιμίου ρυθμίσεων στους δρομολογητές των συνδρομητών της CYTA παρατηρούμε ένα μεγάλο κενό στην ασφάλεια των ασυρμάτων δικτύων: Σύμφωνα με το ερωτηματολόγιο το 74% του δείγματος μας δεν έχει αλλάξει τις ρυθμίσεις στο δρομολογητή ενώ στην καταγραφή με wardriving το 90% των συνδρομητών της CYTA δεν άλλαξε καν το όνομα του ασυρμάτου δικτύου του.

Ίσως μια εταιρεία της εμβέλειας της CYTA θα έπρεπε να ενημερώνει και να βοηθά τους χρήστες της για το περισσότερο σε θέματα ασφάλειας. Κατά τη διάρκεια της μελέτης μου με κάλεσαν τρεις συνδρομητές της CYTA να ελέγξω τον δρομολογητή τους γιατί το δίκτυο τους παρουσιαζόταν ασυνήθιστα “αργό” (χαμηλές ταχύτητες) και για κάποια άλλα προβλήματα. Όταν έλεγξα τον δρομολογητή για ανεπιθύμητα άτομα διαπίστωσα ότι διάφοροι άγνωστοι ήταν συνδεδεμένοι στο δίκτυο χωρίς την συγκατάθεση του κάτοχου. Αφού άλλαξα κωδικό και όνομα SSID στα ασύρματα δίκτυα οι άγνωστοι δεν μπόρεσαν να εισέλθουν σε αυτά διότι το πρόγραμμα εύρεσης κωδικού, που προφανώς χρησιμοποιούσαν, δεν μπορούσαν να διασπάσει το πρωτόκολλο κρυπτογράφησης WPA (σε συνδυασμό βέβαια με έναν δύσκολο κωδικό). Με αυτόν τον απλό τρόπο και στις τρεις περιπτώσεις τα προβλήματα λύθηκαν και οι χρήστες μετά από μια λιτή ενημέρωση ήταν σε θέση να

κατανοήσουν τα βασικά μέτρα προφύλαξης που πρέπει να λαμβάνονται ώστε να διατηρείται το δίκτυο τους ασφαλές και μη προσβάσιμο σε αγνώστους. Είναι σημαντικό επίσης να αναφερθεί ότι και οι τρεις συνδρομητές είχαν καλέσει τη CYTA για βοήθεια και τους είχαν αναφέρει πως ενδέχεται να υπήρχαν ανεπιθύμητα άτομα συνδεδεμένα στο δίκτυο τους αλλά δεν έλαβαν καμία πληροφορία / οδηγία πως θα μπορούσαν να το ασφαλίσουν. Οι τεχνικοί που έλεγξαν το δίκτυο δεν μπήκαν καν στον κόπο να αλλάξουν τις ρυθμίσεις του δρομολογητή και ούτε πληροφόρησαν τους συνδρομητές τους για θέματα ασφάλειας. Με το γεγονός αυτό μπορούμε να δούμε ότι, δυστυχώς, τα θέματα ασφαλείας των ασυρμάτων δικτύων δεν αντιμετωπίζονται ούτε από τις εταιρείες παροχής υπηρεσιών διαδικτύου με την απαιτούμενη σοβαρότητα. Είναι εμφανές ότι οι συνδρομητές θα έπρεπε να τυγχάνουν μεγαλύτερης ενημέρωσης σχετικά με τα θέματα ασφαλείας.

Το πρόβλημα αυτό δεν αφορά όμως μόνο την CYTA. Η Primetel, με βάση τα αποτελέσματα, θα μπορούσε να θεωρηθεί μια ασφαλής εταιρία όσον αφορά τα ασύρματα δίκτυα που παρέχει στους συνδρομητές της (δες Εικόνα 46). Δίνει δρομολογητές της εταιρείας Telsey με WPA2 πρωτόκολλο κρυπτογράφησης. Εντούτοις δεν παρέχει τη δυνατότητα στους συνδρομητές της να κάνουν αλλαγές στις ρυθμίσεις του δρομολογητή τους αλλά ούτε και να έχουν πρόσβαση σε αυτό για να ελέγχουν, για παράδειγμα, ποιοι είναι συνδεδεμένοι σε αυτόν. Αυτό οφείλεται στο γεγονός ότι χρησιμοποιεί στο ίδιο κουτί (δρομολογητή) RADIOUS δίκτυο (redwifi ή Primetel wifi) και δεν θέλει οι συνδρομητές της να μπορούν να τις αλλάζουν ρυθμίσεις και να βλέπουν ποια άτομα είναι συνδεδεμένα στο RADIOUS δίκτυο.



Εικόνα 46: Εκ προοιμίου πρωτόκολλα κρυπτογράφησης για τους συνδρομητές της εταιρείας Primetel

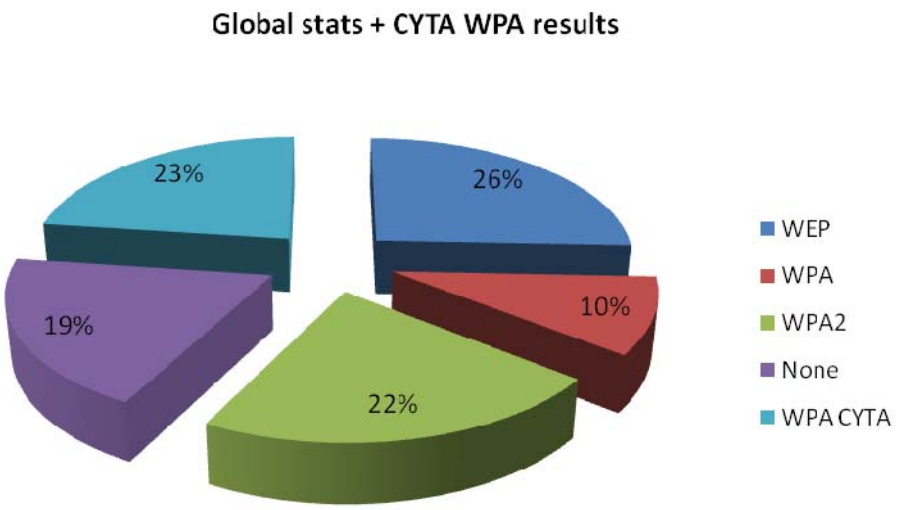
Η όλη προσέγγιση φαίνεται αρκετά ασφαλής αλλά τι θα γινόταν αν κάποιοι καταφέρουν και βρούνε τον αλγόριθμο από το οποίο παράγεται ο κωδικός πρόσβασης όπως συμβαίνει με τους δρομολογητές της Thomson (περίπτωση CYTA); Θα υπάρξει και εδώ τεράστιο πρόβλημα και ενδεχομένως πιο επικίνδυνο από αυτό των συνδρομητών της CYTA γιατί οι χρήστες δεν θα έχουν ούτε τη δυνατότητα αλλάξουν τις ρυθμίσεις του δρομολογητή τους

για να προστατευτούν. Αξίζει να σημειωθεί εδώ ότι δρομολογητές Telsey αποδείχθηκαν, σε άλλες χώρες, ευάλωτοι σε επιθέσεις.

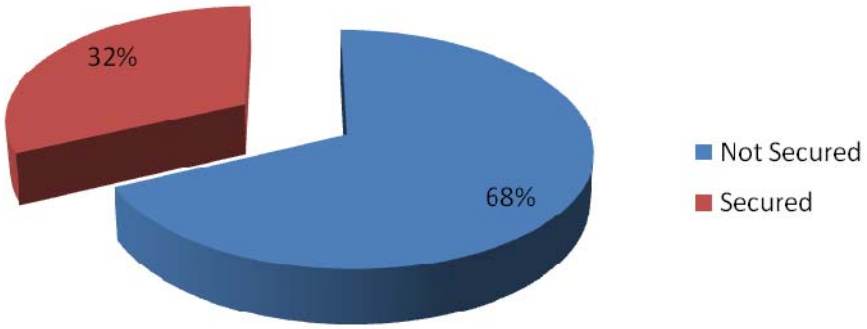
Οι δρομολογητές της Hitron και της MTN είναι επίσης ευάλωτοι εξαιτίας του WPS (βλέπε θεωρητικό πλαίσιο) κυρίως διότι όπως αποδείχθηκε από την έρευνα κοινής γνώμης οι χρήστες δεν είναι ενήμεροι για το τι είναι το WPS και πως λειτουργεί.

Επιστρέφοντας στην Εικόνα 41 όπου παρουσιάζεται η συχνότητα χρήσης των πρωτοκόλλων κρυπτογράφησης στο σύνολο των δικτύων που καταγράφηκαν με Wardirving παρατηρούμε ότι το 45% των δικτύων (WEP και χωρίς κωδικό) είναι ευάλωτα. Το υπόλοιπο 55% αφορά τα πρωτόκολλα κρυπτογράφησης WPA και WPA2 τα οποία θεωρούνται ασφαλή. Όπως ήδη αναφέρθηκε μεγάλο ποσοστό από τα δίκτυα αυτά αφορούν συνδρομητές της CYTA. Προσπαθώντας να βγάλω τα τελευταία συμπεράσματα συγκέντρωσα σε ένα πίνακα την κατανομή των πρωτοκόλλων WPA που ανήκουν στη CYTA σε σχέση με τις υπόλοιπες εταιρείες παροχής υπηρεσιών διαδικτύου. Η Εικόνα 47 μας δείχνει ότι 23% του WPA πρωτοκόλλου ανήκει στην CYTA και μόνο 10% είναι τα ασφαλισμένα WPA δίκτυα. Επομένως με βάση την πρακτική μελέτη (Wardriving) το 68% των ασυρμάτων δικτύων παρουσιάζουν προβλήματα ασφάλειας (βλέπε Εικόνα 48).

Οι δρομολογητές της Hitron και της MTN δεν υπολογιστήκαν ως ανασφαλείς (αν και υπάρχει αδυναμία στην ασφάλεια τους λόγω του WPS) επειδή χρειάζεται πολύ καλή γνώση των θεμάτων ασφάλειας για να μπορέσει κάποιος να τα παραβιάσει και επιπλέον η διαδικασία παραβίασης είναι χρονοβόρα (1-2 μέρες).



Εικόνα 47: Πρωτόκολλα κρυπτογράφησης και κατανομή του πρωτοκόλλου WPA στην εταιρεία CYTA και τις υπόλοιπες εταιρείες παροχής υπηρεσιών διαδικτύου



Εικόνα 48: Συνολική κατανομή ασφαλών και μη ασυρμάτων δικτύων με βάση τη μελέτη Wardriving

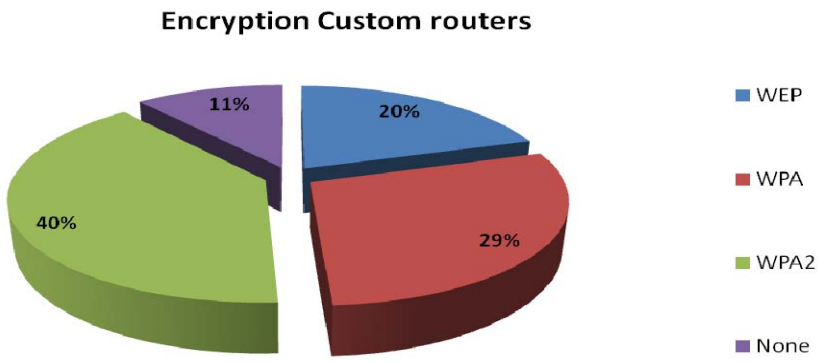
Συμπεράσματα

Επιστρέφοντας στα αρχικά ερωτήματα της μελέτης, έχουμε πλέον αρκετό υλικό για να δώσουμε τεκμηριωμένες απαντήσεις.

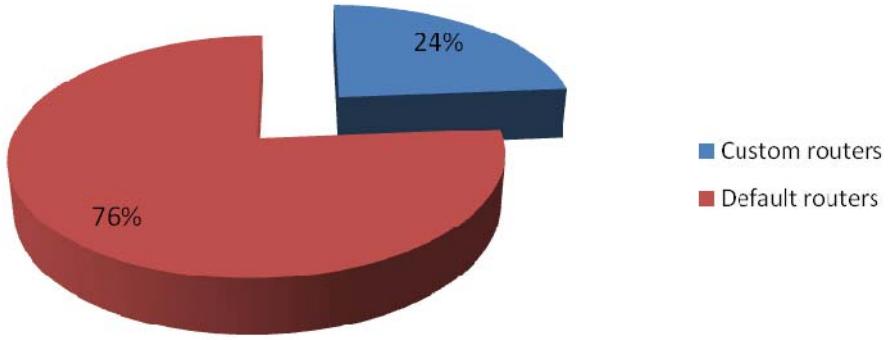
Στην πρώτη υπόθεση της έρευνας αναφέρουμε ότι οι Κύπριοι δεν λαμβάνουν μέτρα προστασίας για την ασφάλεια των ασύρματων οικιακών τους δικτύων. Από την έρευνα κοινής γνώμης προκύπτει ότι το 74% των ιδιοκτητών ασυρμάτων δικτύων δεν έχουν κάνει αλλαγές στον δρομολογητή τους και το 67% δήλωσε πως δεν γνωρίζει πως να το κάνει. Το 62% δεν γνώριζε ούτε το όνομα του ασυρμάτου του δικτύου ενώ το 76% δεν έλεγχε για ανεπιθύμητα άτομα στο δίκτυο τους. Επίσης οι περισσότεροι δεν γνώριζαν για τις βασικές μεθόδους ασφάλειας (WPS, HTTPS, VPN, SSL). Τα αποτελέσματα από την πρακτική μελέτη (Wardriving) επιβεβαιώνουν ότι οι χρήστες δεν αλλάζουν τις ρυθμίσεις του δρομολογητή τους: Μόνο 10% των ασυρμάτων δικτύων που καταγράφηκαν είχαν αλλαγμένο το SSID (όνομα του ασυρμάτου δικτύου). Η αμέλεια αυτή για τα θέματα ασφάλειας οδηγεί τους συνδρομητές σε πολλούς κινδύνους που πιθανότατα δεν γνωρίζουν. Οι χρήστες θα έπρεπε να είναι περισσότερο ενήμεροι για το θέμα. Από μόνοι τους δεν έψαξαν και ούτε ρώτησαν οδηγίες για το πως να ασφαλίσουν το ασύρματο τους δίκτυο (ερώτηση 19 του ερωτηματολογίου). Σε σχετική ερώτηση στην έρευνα κοινής γνώμης το 83% δήλωσε πως θα ήθελε να μάθει περισσότερα για το θέμα της ασφάλειας των ασυρμάτων δικτύων και μεγάλο ποσοστό δήλωσε πως θα ακολουθούσε τις οδηγίες από την εταιρία ISP. Το συμπέρασμα σε αυτήν την υπόθεση δεν είναι θετικό: οι χρήστες δεν λαμβάνουν μέτρα προστασίας του δικτύου τους και το ποσοστό των δρομολογητών των οποίων έχουν αλλαχθεί οι εκ προοιμίου (default) ρυθμίσεις θα έπρεπε να ήταν πολύ μεγαλύτερο. Οι χρήστες μένουν ευάλωτοι και τα ασύρματα δίκτυα ανοιχτά και εύκολα προσβάσιμα σε ανεπιθύμητους. Κανένα ασύρματο δίκτυο δεν μπορεί να θεωρηθεί ασφαλές όταν ο ιδιοκτήτης του δε γνωρίζει τα θέματα ασφάλειας. Σε σχετική ερώτηση στην έρευνα κοινής γνώμης το 62% δεν γνώριζε ούτε την ονομασία SSID του δικτύου τους. Αυτό δημιουργεί ένα πολύ μεγάλο κίνδυνο: Οποιοσδήποτε μπορεί να δημιουργήσει ένα «ψεύτικο» δίκτυο και να συγκεντρώσει ανυποψίαστες χρήστες που υπάρχουν στην συγκεκριμένη περιοχή στο δίκτυο

του. Με αυτό τον τρόπο μπορεί πολύ εύκολα να υποκλέπτει στοιχεία (προσωπικά e-mail, κωδικούς κλπ) με ανυπολόγιστες συνέπειες

Στο δείγμα χώρισα τα δίκτυα τα οποία έχουν εγκαταστήσει οι χρήστες μέσω άλλων δρομολογητών (αγορασμένων από τους συνδρομητές) από αυτά των εταιρειών (αυτά δηλαδή που παρέχουν οι εταιρείες με κάθε νέα συνδρομή) και τα RASIOUS δίκτυα. Το σχετικό αποτέλεσμα παρουσιάζεται στην Εικόνα 49. Οι χρήστες που αγόρασαν δικό τους δρομολογητή βρίσκονται σε σαφώς καλύτερη θέση καθώς το 69% των δικτύων θεωρούνται ασφαλή (πρωτόκολλα κρυπτογράφησης WPA και WPA2). Δυστυχώς όμως το ποσοστό των συνδρομητών που αγόρασαν δικό τους δρομολογητή είναι μόνο το 24% (βλέπε Εικόνα 50).



Εικόνα 49: Χρήση πρωτοκόλλων κρυπτογράφησης σε αγορασμένους από τους συνδρομητές δρομολογητές



Εικόνα 50: Ποσοστό αγορασμένων και παρεχόμενων από τις εταιρείες δρομολογητών

Η δεύτερη υπόθεση αφορούσε τις εταιρίες ISP και ότι δεν λαμβάνουν μέτρα προστασίας των συνδρομητών τους. Όπως έχουμε δει στα αποτελέσματα μας υπάρχουν διάφορες εταιρίες παροχής υπηρεσιών διαδικτύου στην Κύπρο. Η CYTA παραμένει η εταιρεία με τους περισσότερους συνδρομητές. Ως εκ τούτου ασχολήθηκα επισταμένως στην μελέτη μου με την περίπτωση των συνδρομητών της.

Η CYTA δεν ενημερώνει τους συνδρομητές της για τα θέματα ασφαλείας (ίσως θέλοντας να αποφύγει απώλειες αλλά και πιθανό πανικό που θα οδηγούσε σε καταιγισμό αιτημάτων

υποστήριξης τα οποία δύσκολα θα μπορούσε να υποστηρίξει χωρίς κόστος) και οι δρομολογητές οι οποίοι παρέχει στους συνδρομητές, της σε συνδυασμό με την άγνοια τους σε σχέση με τα θέματα ασφαλείας, είναι εξαιρετικά ευάλωτοι σε ανεπιθύμητη πρόσβαση από τρίτους. Οι συνδρομητές της CYTA όπως άλλωστε και των υπολοίπων εταιρειών δεν γνωρίζουν πως να ασφαλίσουν το ασύρματο τους δίκτυο. Σε τρεις περιπτώσεις που εξέτασα προσωπικά διαπίστωσα ότι άγνωστοι είχαν εισβάλει στα ασύρματα δίκτυα των συνδρομητών της CYTA, η οποία παρότι ενημερώθηκε δεν έλαβε μέτρα να διορθώσει το πρόβλημα. Υπάρχουν αρκετοί τρόποι να λυθεί το συγκεκριμένο πρόβλημα: το πιο απλό θα ήταν να αλλάζουν οι τεχνικοί της κατά την εγκατάσταση του ασυρμάτου δικτύου το SSID. Εναλλακτικά θα μπορούσαν να ενημερώσουν με σεμινάρια και παρουσιάσεις τους συνδρομητές τους ή να δημιουργήσουν μία ιστοσελίδα με αντικείμενο την ασφάλεια των οικιακών δικτύων και να παρουσιάζουν όσο πιο εύκολα γίνεται τα προβλήματα και τις λύσεις. Επιπλέον, αφού το πρόβλημα προέρχεται από τους δρομολογητές, θα πρέπει να βρουν διάφορους τρόπους να μειωθεί, τουλάχιστον, η πιθανότητα να υπάρχουν ανεπιθύμητα άτομα στα ασύρματα δίκτυο. Οι νέες εταιρίες όπως η Primetel, MTN, Cablenet κτλ έχουν κάνει καλή δουλεία για να ασφαλίσουν τους δρομολογητές τους και δεν βρίσκονται σε μεγάλο κίνδυνο. Αν και στην μελέτη μου η MTN και Cablenet βρέθηκαν ευάλωτες λόγω του WBS εντούτοις ο κίνδυνος για τους συνδρομητές τους είναι μικρός καθώς η διαδικασία εύρεσης του κωδικού πρόσβασης είναι χρονοβόρα, δύσκολη και απαιτεί εξειδικευμένες γνώσεις και ειδικό εξοπλισμό.

Κλείνοντας με τη συγκεκριμένη υπόθεση εργασίας θα λέγαμε πως αν η CYTA καταφέρει να λύσει το πρόβλημα με τους δρομολογητές της τότε το πρόβλημα της ασφάλειας των ασυρμάτων δικτύων συνολικά θα αμβλυνθεί και το ποσοστό των ασφαλισμένων ασυρμάτων δικτύων θα αυξηθεί κατακόρυφα.

Η τρίτη και τελευταία υπόθεση της μελέτης αφορούσε την ασφάλεια των οικιακών ασύρματων δικτύων στην Κύπρο. Τα ασύρματα δίκτυα, όπως έχουμε αναφέρει σε πολλά σημεία της παρούσας μελέτης, παρουσιάζονται με ελλείψεις όσον αφορά την ασφάλεια τους. Η αμέλεια ή η αδυναμία των χρηστών να ασφαλίσουν το δίκτυο τους οδηγεί σε ένα ευάλωτο και ελεύθερα προσβάσιμο ασύρματο δίκτυο.

Προβλήματα και προτάσεις

Μερικά από τα προβλήματα που αντιμετώπισα στην παρούσα μελέτη ήταν ο χρόνος ο οποίος δεν ήταν επαρκής για μεθοδικότερη και αποτελεσματικότερη ανάλυση των στοιχείων ιδιαίτερα όσον αφορά την πρακτική μελέτη (Wardriving). Θα μπορούσα επίσης να επεκτείνω την καταγραφή στοιχείων και σε άλλες αστικές και αγροτικές περιοχές ώστε τα αποτελέσματα να είναι περισσότερο αντιπροσωπευτικά. Ένα άλλο σημαντικό πρόβλημα ήταν ότι το δείγμα των συνδρομητών της CYTA ήταν τόσο μεγάλο που με υποχρέωνε να την μελετήσω ως συγκεκριμένη περίπτωση. Αυτό οδήγησε σε κάποια συμπεράσματα που φαίνονται «επιθετικά» προς τη συγκεκριμένη εταιρεία. Θα ήθελα επομένως να βεβαιώσω ότι δεν υπήρχε καμία τέτοια πρόθεση από μέρους μου.

Ένα άλλο πρόβλημα ήταν ότι δεν μπορούσα να συγκρίνω / αντιπαραβάλω την παρούσα μελέτη με αυτή που πραγματοποιήθηκε το 2010 από τον Bestuzhev διότι η τελευταία ήταν ελλιπής (τουλάχιστον το τμήμα της το οποίο είναι προσβάσιμο μέσω του διαδικτύου) και δεν γνωρίζαμε ποιες εταιρείες ISP καταγράφηκαν τότε.

Δεν μπόρεσα επίσης να ασχοληθώ περισσότερο με το θέμα των χρηστών όσον αφορά την έρευνα κοινής γνώμης. Θα έπρεπε να κάνω και συνεντεύξεις πέραν του ερωτηματολογίου. Επίσης το δείγμα θα μπορούσε να είναι πολύ μεγαλύτερο και καλύτερα στρωματοποιημένο όσον αφορά την ηλικιακή κατανομή και τη μόρφωση (στην έρευνα κοινής γνώμης μεγάλο ποσοστό αυτών που συμπλήρωσαν το ηλεκτρονικό ερωτηματολόγιο ήταν φοιτητές).

Τα αποτελέσματα που εμφανίζονται στην παρούσα μελέτη δεν είναι 100% ακριβή διότι δεν είχαμε άμεση πρόσβαση (με την άδεια δηλαδή του ιδιοκτήτη) στα ασύρματα δίκτυα για να μπορέσουμε να τα ελέγξουμε ένα-ένα. Από την άλλη προσπάθησα να πάρω όσες περισσότερες λεπτομέρειες ήταν δυνατό μέσω της καταγραφής στοιχείων στον αέρα (Wardriving) ώστε οι εκτιμήσεις μου να προσεγγίζουν όσο το δυνατόν περισσότερο την πραγματικότητα. Για παράδειγμα στην περίπτωση της CYTA όποτε τα δίκτυα είχαν όνομα CYTAXXXXXX και όχι διαφορετικό ESSID (πχ “wifi home”) τα θεωρούσα ευάλωτα σε επιθέσεις υποθέτοντας ότι εφόσον δεν είχε αλλαχθεί το όνομα του ασυρμάτου δικτύου δεν θα είχε αλλαχθεί και ο κωδικός πρόσβασης (εφόσον το δεύτερο είναι σαφώς πιο δύσκολο).

Ένα άλλο πρόβλημα που είχα ήταν ότι δεν μπόρεσα να πάρω πληροφορίες από τις εταιρίες ISP λόγω έλλειψης χρόνου. Θα ήταν πολύ καλή ευκαιρία να ακούσω από τις ίδιες τις εταιρείες τις απόψεις τους σχετικά με το συγκεκριμένο θέμα και να κατανοήσω την πολιτική τους. Ειδικά στην περίπτωση της CYTA η οποία αντιμετωπίζει το πρόβλημα με τους δρομολογητές της θα ήθελα να γνωρίζω αν είναι σε γνώση τους και αν όντως είναι για πιο λόγο δεν προσπαθούν να το αντιμετωπίσουν. Εντούτοις μπόρεσα να μιλήσω με υπάλληλους των εταιρειών Primetel και MTN οι οποίοι μου έδωσαν πληροφορίες για τις εταιρείες τους και με ποιο τρόπο ασφάλισαν τα ασύρματα δίκτυα στους συνδρομητές τους.

Βιβλιογραφία

[1]. Alliance. (2007, January 3). Introducing Wi-Fi Protected Setup. *Wi Fi Certified™ makes it Wi-Fi*. Retrieved March 3, 2012, from www.wi-fi.org/files/kc_80_20070104_Introducing_Wi-Fi_Protected_Setup.pdf

[2]. Alliance. (2006, January 3). Frequently Asked Questions: Wi-Fi Protected Setup. *Frequently Asked Questions: Wi-Fi Protected Setup*. Retrieved March 3, 2012, from http://www.wi-fi.org/files/WFA%20Wi-Fi%20Protected%20Setup%20FAQ.pdf

[3]. Mitchell, B. (n.d.). MAC Addressing - Introduction to the MAC Address. *Networking - Computer and Wireless Networking Basics - Home Networks Tutorials*. Retrieved December 20, 2011, from http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm

[4]. Bestuzhev, D. (2010, June 2). SAS2010: Wardriving in Limassol, Cyprus - Securelist. *Securelist - Information about Viruses, Hackers and Spam*. Retrieved December 19, 2011, from http://www.securelist.com/en/blog/2186/SAS2010_Wardriving_in_Limassol

[5]. *Briere, D. D., & Hurley, P. J. (2005). Wireless network hacks & mods for dummies. Hoboken, N.J.: Wiley.*

[6]. Hurley, C. (2004). *WarDriving: drive, detect, defend: a guide to wireless security*. Rockland, Mass.: Syngress

[7]. Jackson, C. (n.d.). How Does HTTPS Work?. *EzineArticles*. Retrieved March 27, 2012, from http://ezinearticles.com/?How-Does-HTTPS-Work?&id=4963448

[8]. ip.gr. (n.d.). VPN (Virtual Private Network). *Web hosting in Greece Register greek .gr .eu .com .net .org .biz .info .com.gr .net.gr .org.gr .edu.gr .gov.gr domains ip.gr* . Retrieved March 26, 2012, from http://www.ip.gr/el/dictionary/136-VPN_Virtual_Private_Network

[9]. Phifer, L. (2003, December 1). Using RADIUS For WLAN Authentication, Part I. *Wi-Fi Planet - The Source for Wi-Fi Business and Technology*. Retrieved December 20, 2011, from http://www.wi-fiplanet.com/tutorials/article.php/3114511

[10]. Viehböck, S. (2011, December 26). Brute forcing Wi-Fi Protected Setup. *Wi-Fi Protected Setup*. Retrieved March 3, 2012, from sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[11]. Roshan, K. (2011, August 28). What is Https and SSL? and how it works? Explained in Simple English. *Techie Inspire - The Technology Blog*. Retrieved March 27, 2012, from http://www.techieinspire.com/https-and-ssl-and-how-it-works/

[12]. Theodorou, V. (2007, June 27). VPN Explained - The Basics of VPN Simplified. *EzineArticles Submission*. Retrieved March 26, 2012, from http://ezinearticles.com/?VPN-Explained---The-Basics-of-VPN-Simplified&id=624480

[13]. Selecting Between Infrastructure and Ad Hoc Wireless Modes. (n.d.). *Support Home Page*. Retrieved December 20, 2011, from

http://support.netgear.com/app/answers/detail/a_id/954/~/selecting-between-infrastructure-and-ad-hoc-wireless-modes

[14]. What is an Access Point?. (n.d.). *Support Home Page*. Retrieved December 20, 2011, from http://support.netgear.com/app/answers/detail/a_id/235/~/what-is-an-access-point%3F

[15]. *WiGLE - Wireless Geographic Logging Engine - Plotting WiFi on Maps*. Retrieved December 20, 2011, from http://wigle.net/gps/gps/main/faq/

[16]. IEEE. (n.d.). Mac addresses.standards. Retrieved April 28, 2012, from standards.ieee.org/develop/regauth/oui/oui

[17]. Williams, D. (2010, January 6). iTWire - Every BigPond Speedtouch router WiFi password vulnerable. iTWire - IT and Telecommunications news views and jobs. Retrieved April 30, 2012, from http://www.itwire.com/business-it-news/security/30338-every-bigpond-speedtouch-router-wifi-password-vulnerable?start=1