

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



- Πτυχιακή Εργασία -

Επιθέσεις σε δίκτυα Wi-Fi και WPA2

ΜΟΥΣΤΑΚΑΣ ΙΩΑΝΝΗΣ

Π2016174

Επιβλέπων καθηγητής : Χριστόφορος Νταντογιάν

Κέρκυρα, Ιούνιος 2023

Επιβλέπων καθηγητής:

Χριστόφορος Νταντογιάν, Επίκουρος Καθηγητής

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Τριμελής Επιτροπή:

Εμμανουήλ Μάγκος, Καθηγητής

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Ελένη Χριστοπούλου, Εργαστηριακό Διδακτικό Προσωπικό

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Χριστόφορος Νταντογιάν, Επίκουρος Καθηγητής

Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Οι Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω των επιβλέποντα καθηγητή μου, τον κ. Χριστόφορο Νταντόγιαν, για τη συνεχή βοήθεια και υποστήριξη τους σε όλα τα στάδια αυτής της διατριβής. Τέλος, θα ήθελα να ευχαριστήσω τους φίλους μου για την βοήθειά τους στην συλλογή των δεδομένων και την Οικογένεια μου για τη βοήθεια και την υποστήριξη τους.

Περίληψη

Το θέμα της πτυχιακής είναι η μελέτη της ασφάλειας σε ασύρματα δίκτυα με πρωτόκολλο WPA2 με έναν νέο τρόπο επίθεσης που ονομάζεται PMKID και η σύγκριση του με τον παλαιότερο τρόπο που χρησιμοποιείτε γνωστό ως handshake. Το συγκεκριμένο θέμα επιλέχτηκε μιας και ο τομέας της ασφάλειας στα δίκτυα είναι κάτι σημαντικό μιας και στις μέρες μας χρησιμοποιείτε από όλους καθώς επίσης επειδή μετά από πολλά χρόνια βρέθηκε μια επίθεση που δεν επηρεάζει καθόλου τον χρήστη οπότε είναι σχεδόν αδύνατο να καταλάβει ο ιδιοκτήτης ότι έχει γίνει απόπειρα επίθεσης και το κυριότερο ότι είναι γρήγορη και μπορεί να κάνει πολλαπλές επιθέσεις σε πολλαπλά δίκτυα. Η μεθοδολογία που χρησιμοποιήθηκε για την εργασία ήταν αρχικά η μελέτη της επίθεσης και το στήσιμο ενός μηχανήματος με τα κατάλληλα προγράμματα. Για τα πειραματικά αποτελέσματα, πραγματοποιήθηκε μια επίδειξη της επίθεσης σε εργαστηριακό περιβάλλον στο Ιόνιο Πανεπιστήμιο για να μελετήσουμε κατά πόσο εφικτό είναι να πραγματοποιήσουμε την επίθεση PMKID με την βοήθεια των προγραμμάτων aircrack & hashcat. Επίσης, έγινε απλή καταγραφή δειγμάτων του ονόματος των Wifi routers με ένα laptop και έναν αντάπτορα Wi-Fi από την πόλη της Νάουσας και από την Θεσσαλονίκη για να μελετηθεί κατά πόσο οι πολείς διαθέτουν router που είναι ευάλωτο στην επίθεση.

Περιεχόμενα

Περίληψη	4
Κεφάλαιο 1 Εισαγωγή	8
1.1 Σκοπός της Πτυχιακής Εργασίας	8
1.2 Στόχος της Εργασίας.....	8
1.3 Δομή της Εργασίας	8
Κεφάλαιο 2 Επιθέσεις και Πρωτόκολλα	9
2.1 Χαρακτηριστικά ασφαλείας	9
2.2 Επικύρωση και Μυστικότητα	9
2.3 Κρυπτογράφηση WEP	10
2.3.1 Επαλήθευση Ταυτότητας	10
2.3.2 Κατακερματισμός	11
2.3.3 Διάνυσμα Αρχικοποίησης και κλειδιά.....	11
2.3.4 Διανομή κλειδιού	12
2.3.5 Τιμή Ελέγχου Ακεραιότητας.....	12
2.3.6 Αλγόριθμος κρυπτογράφησης RC4	13
2.3.7 Η κρυπτογράφηση.....	13
2.3.8 Προβλήματα του WEP.....	14
2.4 WPA Protocol	17
2.4.1 AES (Advanced Encryption Standard).....	17
2.4.2 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)	18
2.3 Τι είναι το πρωτόκολλο WPA2	20
2.4 Handshake	21
2.5 PMKID	23
2.5.1 PMK Caching and PMKID	23
2.5.2 PMKID επίθεση.....	25
Κεφάλαιο 3 Ανάλυση Προγραμμάτων	27
3.1 Hcxdump tool	27
3.2 Aircrack.....	27

3.3 Hashcat	27
Κεφάλαιο 4 Δείγματα.....	28
4.1 Διαδικασία συλλογής δειγμάτων.....	28
4.2 Προβλήματα στην συλλογή δειγμάτων.....	28
4.3 Πρακτικό μέρος – Εργαστηριακό περιβάλλον	28
Κεφάλαιο 5 Αποτελέσματα δειγματοληψίας	33
5.1 Νάουσα	33
5.2 Θεσσαλονίκη	33
5.3 Σύγκριση Αποτελεσμάτων.....	34
Κεφάλαιο 6 Τελικά συμπεράσματα και λύσεις.....	35
6.1 Συμπεράσματα	35
6.2 WPA3 Protocol	35
6.2.1 Λειτουργίες ασφαλείας WPA3.....	38
6.2.1.1 WPA3-Personal.....	38
6.2.1.2 WPA3-Enterprise	38
6.2.1.3 WPA3-Enterprise με λειτουργία 192-bit.....	39
6.2.2 Διάφορες με WPA2	40
6.2.3 SAE και Dragonfly handshake.....	42
6.2.4 handshake attack.....	44
Βιβλιογραφία	46

Περιεχόμενα Εικόνων

Εικόνα 1 wep encryption [63]	14
Εικόνα 2 AES [64].....	18
Εικόνα 3 CCMP encryption diagram [43]	19
Εικόνα 4 Diagram of the CCMP encapsulation process.png [35]	19
Εικόνα 5 WPA 2 encryption and integrity check [65].....	21
Εικόνα 6 wpa2 key hierarchy [2]	21
Εικόνα 7 handshake [32]	23
Εικόνα 8 hcxtools.git	29
Εικόνα 9 iwconfig	29
Εικόνα 10 airmon	30
Εικόνα 11 capture pmkid	30
Εικόνα 12 tcpdump	31
Εικόνα 13 aircrack cap	31
Εικόνα 14 cracked network	32
Εικόνα 15 wpa3 solved attacks [44]	35
Εικόνα 16 GCM Galois Counter Mode [37]	37
Εικόνα 17 wpa3 new features [28].....	37
Εικόνα 18 wpa3 types.....	40
Εικόνα 19 wpa3 types [27]	40
Εικόνα 20 Διαφορές wpa version 2 με 3[66].....	41
Εικόνα 21 wpa3 handshake [35]	43

Κεφάλαιο 1 Εισαγωγή

1.1 Σκοπός της Πτυχιακής Εργασίας

Ο σκοπός της παρούσας πτυχιακής εργασίας είναι να δούμε έναν καινούργιο τρόπο που υπάρχει στην συλλογή και αποκρυπτογράφηση κωδίκων δικτιών και να την συγκρίνουμε με τον γνωστότερο τρόπο που υπάρχει μέχρι και σήμερα και χρησιμοποιείται από πάρα πολλούς χρήστες ώστε να ξέρουμε κατά πόσο είμαστε ασφαλείς στο ιδιωτικό μας δίκτυο αλλά και τι κίνδυνοι παραμονεύουν.

1.2 Στόχος της Εργασίας

Οι στόχος της εργασίας είναι να μελετήσουμε κατά πόσο εφικτό είναι να πραγματοποιήσουμε την επίθεση PMKID με την βοήθεια των προγραμμάτων `aircrack` & `hashcut`. Όλες οι δοκιμές έχουν πραγματοποιηθεί σε εργαστηριακό περιβάλλον. Ένας δεύτερος στόχος ήταν η μελέτη του πλήθους των routers που μπορεί πιθανόν να είναι ευάλωτα στη συγκεκριμένη επίθεση.

1.3 Δομή της Εργασίας

Τα επόμενα κεφάλαια της πτυχιακής εργασίας διαμορφώνονται ως εξής: Στο δεύτερο κεφάλαιο παρουσιάζεται ο τρόπος που δουλεύουν τα πρωτόκολλα `wep`, `wpa` και `wpa2` και αναλύουμε τον αλγόριθμο κρυπτογράφησης που χρησιμοποιούν και πως στο `wpa2` πατάνε πάνω σε αυτόν οι δυο επιθέσεις που βλέπουμε, τι εκμεταλλεύονται και πως δουλεύουν. Επίσης αναλύουμε τι είναι και πως δουλεύει το `handshake` και το `pmkid` με μαθηματικούς τύπους και θεωρία. Στο τρίτο κεφάλαιο αναλύουμε τα εργαλεία που θα πρέπει να χρησιμοποιήσουμε. Στο τέταρτο κεφάλαιο μιλάμε για το πως κάναμε την συλλογή δειγμάτων και τις δυσκολίες που αντιμετωπίσαμε και κάναμε και μια ανάλυση αναλυτικά με τα βήματα που χρειάζεται. Στο πέμπτο κεφάλαιο βλέπουμε τα αποτελέσματα στις δυο πόλεις και κάνουμε μια σύγκριση μεταξύ τους. Τέλος στο τελευταίο κεφάλαιο βγάζουμε τα συμπεράσματα της πτυχιακής που κάνουμε και δίνουμε και κάποιες ιδέες για μελλοντικές βελτιώσεις ή μελλοντικές εργασίες πάνω στην υπάρχον και μια λύση για να αποτραπούν αυτές οι επιθέσεις που είναι το νέο πρωτόκολλο `wpa3` και εμβαθύνουμε στις ιδιότητες του και στους τρόπους - σημεία που είναι άτρωτο σε αυτές τις επιθέσεις .

Κεφάλαιο 2 Επιθέσεις και Πρωτόκολλα

2.1 Χαρακτηριστικά ασφαλείας

Οι ιδιότητες για να πούμε ότι μια επικοινωνία είναι ασφαλής αποτελούνται από τα παρακάτω στοιχεία :

- **Επικύρωση:** Πριν από την μετάδοση των δεδομένων, οι κόμβοι αναγνωρίζονται και ανταλλάσσουν επικυρωμένα πιστοποιητικά.
- **Κρυπτογράφηση:** Πριν από την αποστολή ενός ασύρματου πακέτου δεδομένων, ο κάθε υπολογιστής που το στέλνει θα πρέπει να το κρυπτογραφήσει.
- **Ακεραιότητα:** Διασφαλίζει ότι το στοιχείο που μεταδίδεται δεν έχει υποστεί καμία τροποποίηση.
- **Μυστικότητα:** Ο όρος αυτός χρησιμοποιείται για να περιγράφει τα δεδομένα που προστατεύονται ενάντια στην ανάγνωση από αναρμόδια συμβαλλόμενα μέρη.

2.2 Επικύρωση και Μυστικότητα

Η έννοια της επικύρωσης αφορά τον έλεγχο πρόσβασης. Για να πραγματοποιήσουμε την επικύρωση πρέπει να αποκτήσουμε πρώτα πρόσβαση στο μέσο και στην περίπτωση μας στο ασύρματο δίκτυο. Αρχικά ελέγχονται τα διαθέσιμα ασύρματα δίκτυα και ακολούθως το δίκτυο επικυρώνει το σταθμό και ο σταθμός επικυρώνει το δίκτυο. Τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται beacons - πλαίσια διαχείρισης (υπάρχει και η περίπτωση να μην στείλει beacons επειδή έχει κρυφό ssid όπου σε αυτή την περίπτωση περιμένει να λάβει αίτηση για να απαντήσει). Τα beacons είναι αυτά τα οποία ανακοινώνουν την ύπαρξη του δικτύου. Το κάθε beacon περιλαμβάνει ένα Service Set Identifier (SSID) ή αλλιώς όνομα δικτύου. Ένας σταθμός μπορεί να επιλέξει να συνδεθεί σε ένα δίκτυο είτε παθητικά είτε ενεργητικά. Στην παθητική σάρωση ο σταθμός ελέγχει τα κανάλια προσπαθώντας να βρει beacons από τα σημεία πρόσβασης και στην ενεργητική σάρωση στέλνει αιτήσεις διερεύνησης (είτε σε ένα συγκεκριμένο SSID είτε με το SSID ρυθμισμένο στο 0), σε όλα τα κανάλια ένα προς ένα. Όλοι οι σταθμοί που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση. Στο πρότυπο 802.11 έχουμε δυο τρόπους επικύρωσης, την επικύρωση ανοιχτού κλειδιού (Open System Authentication - OSA) και την επικύρωση μοιρασμένου κλειδιού (Shared Key Authentication - SKA). Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στο μήνυμα της αίτησης επικύρωσης. Το δίκτυο μπορεί να δεχτεί ή να απορρίψει αυτή την πρόταση ανάλογα με τις ρυθμίσεις ασφαλείας. Χρησιμοποιώντας επικύρωση ανοιχτού κλειδιού οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης όμως όχι και να επικοινωνήσει. Η συσκευή μπορεί να επικοινωνεί μόνο αν τα WEP κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης. Η

επικύρωση μοιρασμένου κλειδιού βασίζεται στο σύστημα πρόσκλησης -απάντησης. Για να χρησιμοποιήσουμε αυτή τη μέθοδο επικύρωσης , προϋποθέτει ότι το σημείο πρόσβασης και ο σταθμός είναι συμβατοί με τη λειτουργία WEP (Wired Equivalent Privacy) και ότι έχουν μεταξύ τους ένα προ-μοιρασμένο κλειδί. Αυτό σημαίνει ότι ένα κοινό κλειδί πρέπει να μοιραστεί σε όλους τους σταθμούς που τους έχει επιτραπεί να έχουν πρόσβαση στο δίκτυο, πριν επιχειρήσουν την διαδικασία της επικύρωσης.

2.3 Κρυπτογράφηση WEP

Κρυπτογράφηση καλείται η διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή, μεταμφιέζονται προκειμένου να επιτευχτεί η ασφαλής μετάδοση πληροφοριών (Encryption, συμβολίζεται με E). Τα δεδομένα πριν από την κρυπτογράφηση ονομάζονται plaintext (και συμβολίζεται με P), ενώ τα δεδομένα μετά την κρυπτογράφηση αποτελούν το cipher text (και συμβολίζεται με C). Η αντίστροφη διαδικασία μετατροπής ονομάζεται αποκρυπτογράφηση (decryption). Ο αλγόριθμος κρυπτογράφησης είναι η μαθηματική ακολουθία που χρησιμοποιείται για την μεταμφίεση και την αποκάλυψη των δεδομένων. Συνήθως οι αλγόριθμοι κρυπτογράφησης εμπεριέχουν ακολουθίες κλειδιών για να τροποποιήσουν τα εξαγόμενα τους. Η πιο γνωστή επιλογή παροχής ασφάλειας για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11 είναι το Wired Equivalent Privacy (WEP). Με την επιλογή του WEP ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν θέλουμε εμπιστευτικότητα , μπορούμε να χρησιμοποιήσουμε την επιλογή του WEP και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν. Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία όσο και την ακεραιότητα των δεδομένων. Με τη βοήθεια ενός συμμετρικού αλγορίθμου κρυπτογράφησης, RC4, επιτυγχάνεται η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω του δικτύου.

2.3.1 Επαλήθευση Ταυτότητας

Σε ένα ασύρματο δίκτυο, μια κινητή συσκευή προκειμένου να συνδεθεί στο δίκτυο μέσω ενός σημείου πρόσβασης, θα πρέπει να αποδείξει την ταυτότητα της. Αυτό θα μπορούσε να γινόταν και από το σημείο πρόσβασης. Στην επαλήθευση ταυτότητας WEP, η συσκευή θα πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει το μυστικό κλειδί της κρυπτογράφησης. Αρχικά υποβάλλεται αίτηση επαλήθευσης ταυτότητας από την κινητή συσκευή προς το σημείο πρόσβασης. Το σημείο πρόσβασης με τη σειρά του στέλνει ένα τυχαίο αριθμό μήκους 128 bit προς κρυπτογράφηση στην ασύρματη συσκευή. Ο αριθμός κρυπτογραφείται από την συσκευή με το μυστικό κλειδί WEP και αποστέλλεται πίσω. Τέλος , το σημείο πρόσβασης ελέγχει εάν η κρυπτογράφηση έγινε με το σωστό κλειδί. Ωστόσο η μέθοδος αυτή αποτελεί ένα μεγάλο

πρόβλημα για την ασφάλεια της κρυπτογράφησης γιατί δίνει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης όσο και της μη κρυπτογραφημένης πληροφορίας.

2.3.2 Κατακερματισμός

Σε ένα ασύρματο δίκτυο, το πακέτο δεδομένων που καταφθάνει περιέχει τις κατάλληλες πληροφορίες για την αποστολή του. Το συγκεκριμένο πακέτο δεδομένων ονομάζεται MSDU (Mac Service Data Unit). Τα δεδομένα καταφθάνουν στο επίπεδο MAC του προορισμού και σκοπός είναι να περάσουν στο λειτουργικό σύστημα και να μετατεθούν στην κατάλληλη εφαρμογή. Παρόλα αυτά, πριν από αυτή τη διαδικασία τα δεδομένα πρέπει να χωριστούν σε μικρότερα κομμάτια, για να υποστούν τη διαδικασία του θραυσματισμού (fragmentation). Στη συνέχεια το κάθε κομμάτι ακολουθεί τη δική του πορεία στην κρυπτογράφηση WEP. Επομένως το αρχικό πακέτο δεδομένων χωρίζεται σε μικρότερα μηνύματα, MPDU (Mac Protocol Data Unit) στα οποία προστίθενται και αλλα bytes.

2.3.3 Διάνυσμα Αρχικοποίησης και κλειδιά

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στην κρυπτογράφηση WEP έχουν μήκος 40 ή 104 bits, ωστόσο συχνά μιλούν για 68 ή 128 bits. Αυτό συμβαίνει επειδή κάποιοι παραλείπουν να αναφέρουν τα επιπλέον 24 bits που χρησιμοποιούνται από το διάνυσμα αρχικοποίησης (Initialization Vector -IV). Το IV ουσιαστικά αλλάζει για κάθε πακέτο και συνδυάζεται με το μυστικό κλειδί. Το αποτέλεσμα αυτών των δυο κρυπτογραφείται. Έτσι, ακόμα και αν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική. Το IV δεν είναι μυστικό, ενώ στέλνεται σε μη κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή IV.

Τα κλειδιά που χρησιμοποιούνται στο WEP

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στο WEP έχουν τα εξής χαρακτηριστικά:

- Σταθερό μήκος: Συνήθως 40 ή 104 bit.
- Στατικά: Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.
- Διαμοιραζόμενα (shared): Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
- Συμμετρικά: Γίνεται χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

Σύμφωνα με το πρότυπο 802.11, η διάθεση των κλειδιών στα σημεία πρόσβασης και στις ασύρματες συσκευές πρέπει να γίνεται με ασφαλείς μεθόδους. Η επαναχρησιμοποίηση των κλειδιών είναι μια αδυναμία των κρυπτογραφικών πρωτοκόλλων. Για αυτό το λόγο το WEP,

έχει μια δεύτερη κατηγορία κλειδιών τα οποία χρησιμοποιούνται για τα ζευγάρια επικοινωνιών. Τα κλειδιά αυτά μοιράζονται μόνο μεταξύ των δυο σταθμών επικοινωνίας. Οι δυο σταθμοί μοιράζονται ένα κλειδί και έχουν μια σχέση χαρτογράφησης κλειδιού. Ένα 128-bit WEP κλειδί σχεδόν πάντα εισάγεται από τους χρήστες σαν μια ακολουθία 26 δεκαεξαδικών (με βάση το 16) χαρακτήρων (0-9 και A-F). Κάθε χαρακτήρας αντιπροσωπεύει 4 bit του κλειδιού. 26 ψηφία τεσσάρων bit δίνουν 104 bit και η προσθήκη του 24 bit IV παράγει το τελικό 128 - bit WEP κλειδί. Ένα 256 - bit σύστημα WEP είναι διαθέσιμο από μερικούς προμηθευτές και όπως με το 128 - bit WEP , τα 24 bit είναι για το IV, αφήνοντας 232 πραγματικά bit για την προστασία. Αυτά τα 232 bit εισάγονται χαρακτηριστικά ως 58 δεξαεξαδικοί χαρακτήρες. $58 * 4 = 232 \text{ bit} + 24 \text{ IV bit} = 256 \text{ bit WEP κλειδί}$. Ωστόσο, το μέγεθος του κλειδιού δεν είναι ο μόνος σημαντικός περιορισμός ασφάλειας στο WEP. Το WEP έχει αρκετά μειονεκτήματα και τα πρόσθετα bit στο κλειδί δεν έχουν ιδιαίτερη σημασία. Η καλύτερη δημόσια επίθεση ενάντια στο WEP μπορεί να ανακτήσει το κλειδί μέσα σε λίγα δευτερόλεπτα.

2.3.4 Διανομή κλειδιού

Το βασικότερο μειονέκτημα του WEP είναι το πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το πρότυπο 802.11 δεν μας παρέχει ένα μηχανισμό παραγωγής κλειδιού με αποτέλεσμα ο καθένας μας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή να έχει πρόσβαση σε συσκευές με το χέρι. Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι οι εξής:

- Τα κλειδιά δεν είναι ουσιαστικά μυστικά, αφού εισάγονται στους οδηγούς software της ασύρματης κάρτας. Έτσι ένας τοπικός χρήστης μπορεί να έχει πρόσβαση στο "μυστικό" κλειδί.
- Εάν τα κλειδιά είναι προσιτά στους χρήστες, αυτά θα πρέπει να αλλάζουν συχνά. Η γνώση των κλειδιών WEP επιτρέπει σε ένα χρήστη να φτιάξει έναν 802.11 σταθμό και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί.
- Οι επιχειρήσεις με ένα μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύουν το κλειδί στους χρήστες και πλέον δεν υφίσταται η "μυστικότητα" του κλειδιού.

2.3.5 Τιμή Ελέγχου Ακεραιότητας

Η τιμή ελέγχου ακεραιότητας (Integrity Check Value - ICV) συνεισφέρει στην αποφυγή από την τροποποίηση του μηνύματος κατά τη μετάδοση. Γενικότερα, σε κρυπτογραφημένα και μη κρυπτογραφημένα μηνύματα , συνηθίζεται έλεγχος για την αλλαγή των bits κατά τη μετάδοση. Το σύνολο των Bytes του μηνύματος συνενώνονται στον έλεγχο κυκλικού πλεονασμού (Cyclic Redundancy Check -CRC) . Η τιμή αυτή, μήκους τεσσάρων bytes, προστίθεται στο τέλος του

πλαισίου πριν την επεξεργασία για μετάδοση. Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή CRC από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα. Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη, δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι σε θέση να υπολογίσει τη νέα τιμή CRC και να αντικαταστήσει την αρχική. Το ICV λειτουργεί όπως το CRC, αλλά υπολογίζεται και εφαρμόζεται πριν την διαδικασία της κρυπτογράφησης. Ωστόσο το CRC μπορεί να προστεθεί και μετά την κρυπτογράφηση. Επομένως, ο εισβολέας δεν μπορεί να υπολογίσει εκ νέου το μήνυμα. Έτσι το ICV υπολογίζεται ως ένας συνδυασμός όλων των δεδομένων και προκύπτει ως μια τιμή μήκους τεσσάρων bytes , η οποία προστίθεται στο τέλος.

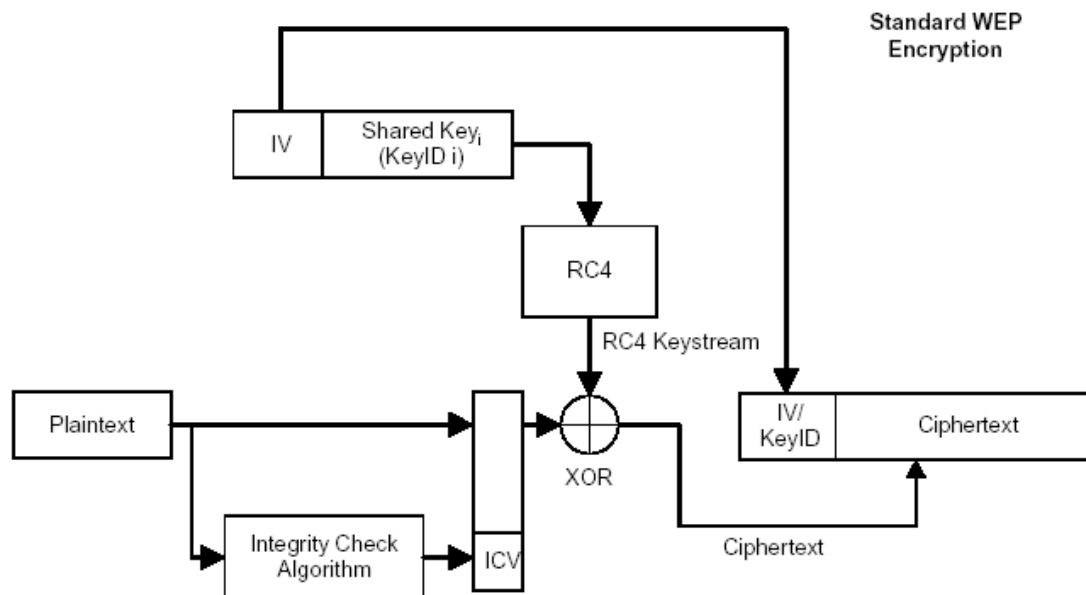
2.3.6 Αλγόριθμος κρυπτογράφησης RC4

Ο αλγόριθμος RC4 χρησιμοποιείται κατά τη διαδικασία της κρυπτογράφησης WEP. Ο RC4 είναι απλός στην υλοποίηση του και ισχυρός. Βασική ιδέα είναι η δημιουργία μιας τυχαίας ακολουθίας bytes , που ονομάζεται ροή κλειδιού (key stream) και έχει ως στόχο το συνδυασμό της με τα δεδομένα μέσω της λογικής πράξης του αποκλειστικού Η (XOR). Η τυχαία ακολουθία κλειδιού ονομάζεται «ψευδοτυχαία» διότι θα πρέπει να δείχνει τυχαία σε εισβολέα αλλά τα δυο άκρα της ζεύξης που επικοινωνούν θα πρέπει να παράγουν την ίδια τυχαία τιμή για κάθε byte που επεξεργάζονται. Η πράξη XOR είναι εύκολα υλοποιήσιμη οπότε το πιο δύσκολο είναι ο υπολογισμός μιας καλής «ψευδοτυχαίας» ροής bytes. Δηλαδή χρειαζόμαστε ένα «ψευδοτυχαίο» byte για κάθε byte του μηνύματος προς κρυπτογράφηση. Ο αλγόριθμος RC4 παράγει μια ροή αυτής της μορφής.

2.3.7 Η κρυπτογράφηση

Αρχικά, το μυστικό κλειδί συνδέεται με το διάνυσμα έναρξης IV και το αποτέλεσμα τους εισάγεται στον αλγόριθμο RC4. Ο αλγόριθμος RC4 παράγει μια ακολουθία κλειδιού key stream από «ψευδοτυχαία» bits ίσα στο μήκος με τον αριθμό bits δεδομένων που πρέπει να διαβιβαστούν συν 4. Στην συνέχεια, για προστασία από αναρμόδια τροποποίηση δεδομένων , εφαρμόζεται ο αλγόριθμος ακεραιότητας στα δεδομένα και παράγεται το ICV. Η κρυπτογράφηση ολοκληρώνεται με τη λογική πράξη του αποκλειστικού Η (XOR) μεταξύ της ακολουθίας κλειδιού και των δεδομένων που μετατράπηκαν σε ICV. Το αποτέλεσμα της διαδικασίας είναι ένα μήνυμα το οποίο περιέχει το IV και το κρυπτογράφημα. Ο αλγόριθμος RC4 είναι ένας από τους σημαντικότερους παράγοντες της κρυπτογράφησης WEP, αφού μεταμορφώνει ένα σύντομο μυστικό κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού. Αυτή η μέθοδος κάνει απλή τη διαδικασία διανομής κλειδιού, αφού το μόνο που θα πρέπει να μεταδοθεί μεταξύ των σταθμών είναι το μυστικό κλειδί. Το διάνυσμα αρχικοποίησης επεκτείνει τη διάρκεια ζωής του μυστικού κλειδιού. Στη μέθοδο WEP λοιπόν το μόνο που αλλάζει ανά συχνά διαστήματα είναι το διάνυσμα αρχικοποίησης ενώ το μυστικό κλειδί παραμένει πάντα ίδιο. Κάθε νέο IV καταλήγει σε μια νέα ακολουθία κλειδιού. Το IV δεν είναι

μυστικό αφού δεν παρέχει πληροφορίες για το μυστικό κλειδί. Για την αποκρυπτογράφηση πρέπει να το διάνυσμα αρχικοποίησης να αποσταλεί μαζί με το κρυπτογραφημένο πακέτο. Όταν ο παραλήπτης αποκρυπτογραφήσει το πακέτο υπολογίζει ξανά την τιμή ελέγχου ακεραιότητας και τη συγκρίνει με αυτή που περιείχε το πακέτο που παρέλαβε. Αν οι δυο τιμές ταυτίζονται, τότε το πακέτο θεωρείται έγκυρο. Γενικά χρησιμοποιούνται στατικά κλειδιά μήκους 40 bits και ενός IV μήκους 24 bits. Νεότερες εκδόσεις του WEP υποστηρίζουν μήκος κλειδιού 104 bits και μήκος IV 24 bits. Το κλειδί και το IV ενώνονται για να σχηματίσουν το κλειδί μήκους 64 bits ή 128 bits αντίστοιχα, το οποίο χρησιμοποιείται ως είσοδος για τον αλγόριθμο RC4. Ο αλγόριθμος RC4 είναι πολύ σημαντικός παράγοντας για την αποδοτικότητα του WEP, όσο αναφορά την εμπιστευτικότητα των δεδομένων, αφού αυτός είναι η μηχανή κρυπτογράφησης. Το μυστικό κλειδί είναι στατικό, οπότε το IV είναι αυτό που καθορίζει κάθε φορά την ψευδοτυχαία ακολουθία. Οπότε, ο αλγόριθμος εξαρτάται μόνο από το IV.



Εικόνα 1 wep encryption [63]

2.3.8 Προβλήματα του WEP

Οι αδυναμίες του WEP είναι αρκετές. Μερικά από τα προβλήματα του WEP αναφέρονται παρακάτω:

Το θέμα της διανομής των κλειδιών είναι ιδιαίτερα σημαντικό θέμα. Όταν κάποιος αποχωρήσει από το σύστημα, τα κλειδιά θα πρέπει να αλλάξουν. Για να επιτύχει μια επίθεση sniffing

χρειάζεται μόνο τα μυστικά κλειδιά τα οποία σπάνια αλλάζουν. Συνήθως το WEP χρησιμοποιεί ένα δημόσιο μυστικό κλειδί 40 bit. Η καταλληλότητα αυτού του κλειδιού δεν έχει κριθεί ιδιαίτερα καλή, για το λόγο αυτό, πολλοί συστήνουν τη χρήση των 128 bit κλειδιών. Η σπάνια νέα εισαγωγή κλειδιών επιτρέπει στους επιτιθέμενους να αποκτήσουν αποθέματα κρυπτογραφημένων δεδομένων δηλαδή, μεγάλες συλλογές των πλαισίων που κρυπτογραφούνται με τα ίδια κλειδιά.

Προβληματική φαίνεται να είναι και η διαδικασία της επαλήθευσης ταυτότητας. Η επαλήθευση ταυτότητας στηρίζεται σε μια μέθοδο πρόκλησης - απόκρισης. Αρχικά στέλνεται μια τυχαία ακολουθία bits, η οποία κρυπτογραφείται, μετά αποστέλλεται πίσω και τέλος το σημείο πρόσβασης την αποκρυπτογραφεί και τη συγκρίνει με την αρχική ακολουθία. Το κλειδί που χρησιμοποιείται σε αυτή τη διαδικασία είναι το ίδιο με αυτό της κρυπτογράφησης, παρέχοντας έτσι την ευκαιρία σε έναν επιτιθέμενο να αποκτήσει στοιχεία. Η όλη διαδικασία δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί στα κλειδιά κρυπτογράφησης. Αυτό συμβαίνει διότι οποιοσδήποτε παρακολουθεί τη διαδικασία της επαλήθευσης έχει πρόσβαση σε ένα κρυπτογραφημένο και μη κρυπτογραφημένο μήνυμα.

Ο έλεγχος πρόσβασης συνίσταται στην απαγόρευση ή όχι της επικοινωνίας μιας συσκευής με το δίκτυο. Η πρόσβαση ελέγχεται συνήθως διατηρώντας μια λίστα με τις επιτρεπόμενες συσκευές ή με ένα ηλεκτρονικό πιστοποιητικό. Στο πρότυπο 802.11 δεν έχουμε κάποιο συγκεκριμένο μηχανισμό υλοποίησης πρόσβασης. Οι συσκευές αναγνωρίζονται συνήθως από τις διευθύνσεις MAC, όμως αυτό δεν είναι και η καλύτερη προσέγγιση γιατί οι διευθύνσεις αυτές μπορούν να αντιγραφούν εύκολα. Έτσι, το μόνο που απομένει για το WEP είναι τα κλειδιά κρυπτογράφησης ξανά.

Ένα άλλο μεμπτό σημείο του WEP είναι η αδυναμία του να διαχειριστεί επιθέσεις μέσω αναπαραγωγής μηνυμάτων. Όταν ένας επιτιθέμενος παρακολουθεί και καταγράφει τα πλαίσια που ανταλλάσσονται σε μια νόμιμη επικοινωνία (sniffing), μπορεί να συνδεθεί στο δίκτυο χρησιμοποιώντας τη MAC διεύθυνση της κινητής συσκευής. Στέλνοντας έτσι ένα αντίγραφο παλιού μηνύματος μπορεί να αποκτήσει πρόσβαση στον εξυπηρετητή. Η προστασία από τέτοιου είδους επιθέσεων στο WEP δεν είναι μόνο ελλιπής αλλά ανύπαρκτη.

Ιδιαίτερη βαρύτητα έχει η επαναχρησιμοποίηση της τιμής του διανύσματος αρχικοποίησης IV. Εάν μαζευτούν πολλά δείγματα επαναλαμβανόμενου IV τότε μπορεί κάποιος να τα υποθέσει ως τμήματα της ροής του κλειδιού και να προχωρήσει στην αποκρυπτογράφηση. Όταν κάποιος γνωρίζει το keystream για ένα συγκεκριμένο IV, μπορεί να αποκρυπτογραφήσει κάθε πλαίσιο που χρησιμοποιεί το ίδιο. Ωστόσο ο κίνδυνος αυτός δεν είναι και τόσο μεγάλος επειδή δεν υπάρχει κάποιο αυτοματοποιημένο εργαλείο που θα μπορούσε να καταφέρει να διαχειριστεί τον προσδιορισμό ενός κρυπτογραφήματος με την μέθοδο αυτή.

Η τιμή του διανύσματος αρχικοποίησης όπως αναφέραμε , δεν είναι μυστική, όμως αυτό δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα αδύναμο σχετικά κλειδί. Τα πρώτα bytes ενός μη κρυπτογραφημένου μηνύματος είναι γνωστά συνήθως , επειδή αποτελούν μια επικεφαλίδα 802.11. Με την παρακολούθηση της μετάδοσης αναζητείται ένα αδύναμο κλειδί . Υπάρχει σχέση ανάμεσα στο κρυπτογραφημένο , στο μη κρυπτογραφημένο μήνυμα και στο μυστικό κλειδί. Έχοντας καταγράψει έναν μεγάλο αριθμό από τέτοια μηνύματα, ο εισβολέας μπορεί να ανακαλύψει το πρώτο byte του κλειδιού. Η μέθοδος αυτή μπορεί να εφαρμοστεί για κάθε byte και έτσι να αποκαλυφθεί το μυστικό κλειδί.ptk .

Μετά από τη συνειδητοποίηση της κρισιμότητας της κατάστασης και του κενού ασφαλείας που άφηνε τα WEP, ανακαλύφθηκε η λύση του TKIP (Temporal Key Integrity Protocol - TKIP). Το TKIP προσφέρει μεγαλύτερη ασφάλεια καθώς παρέχει ανάμιξη κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος και μηχανισμό αναπαραγωγής κλειδιών , ο οποίος επιδιορθώνει τα ελαττώματα του WEP. Αυτό που απαιτούσε όταν ξεκίνησε ήταν η αναβάθμιση του firmware και πιθανώς του λογισμικού (driver) της συσκευής. Αρχικά το TKIP χρησιμοποιήθηκε πάνω στο WEP για να ενισχύσει την ασφάλεια και για να μειώσει τον αριθμό των επιθέσεων του WEP. Το πρώτο βήμα στη διαδικασία της κρυπτογράφησης TKIP είναι ο υπολογισμός του κώδικα ακεραιότητας δεδομένων MIC, που γίνεται με τον αλγόριθμο Michael. Με τον αλγόριθμο αυτό προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και του παραλήπτη. Αυτά και ένα κλειδί MIC είναι οι είσοδοι στον αλγόριθμο. Στο τέλος προκύπτουν 8 bytes , τα οποία προστίθενται στο αρχικό μήνυμα το οποίο στη συνέχεια κρυπτογραφείται. Η TKIP κρυπτογράφηση λειτουργεί σε δυο φάσεις. Η πρώτη φάση χρησιμοποιεί ένα μη γραμμικό πίνακα αντικατάστασης (S - Box) και συνδυάζει το κλειδί συνόδου TK , τη MAC διεύθυνση του αποστολέα (TA), και τα τέσσερα πιο σημαντικά bytes της τιμής του μετρητή ακολουθίας (TKIP Sequence Counter), ο οποίος αυξάνεται για κάθε τμήμα δεδομένων που τεμαχίζεται. Το κλειδί συνόδου αποτελείται από μια τιμή 128 bit , παρόμοια με την τιμή του WEP κλειδιού. Ο TKIP μετρητής ακολουθίας (TSC) είναι φτιαγμένος από την πηγαία διεύθυνση SA , την διεύθυνση προορισμού DA, την ιεραρχία και τα δεδομένα. Στην έξοδο παράγεται μια ενδιάμεση τιμή TTAK. Η τιμή αυτή μπορεί να αποθηκευτεί προσωρινά και να χρησιμοποιηθεί μέχρι και για 216 πακέτα. Εφόσον λαμβάνεται υπόψη η διεύθυνση του αποστολέα η συνάρτηση παράγει διαφορετική ενδιάμεση τιμή για κάθε συσκευή, ακόμα και αν χρησιμοποιηθεί το ίδιο κλειδί κρυπτογράφησης από όλες τις συσκευές. Η δεύτερη φάση «ανακατεύει» την τιμή TTAK με τα δυο λιγότερο σημαντικά bytes της τιμής του μετρητή ακολουθίας TSC και το κλειδί συνόδου TK για την εξαγωγή του κλειδιού κρυπτογράφησης. Τέλος κατά τα γνωστά από το WEP, υπολογίζεται το IV και γίνεται η κρυπτογράφηση από τον αλγόριθμο RC4.

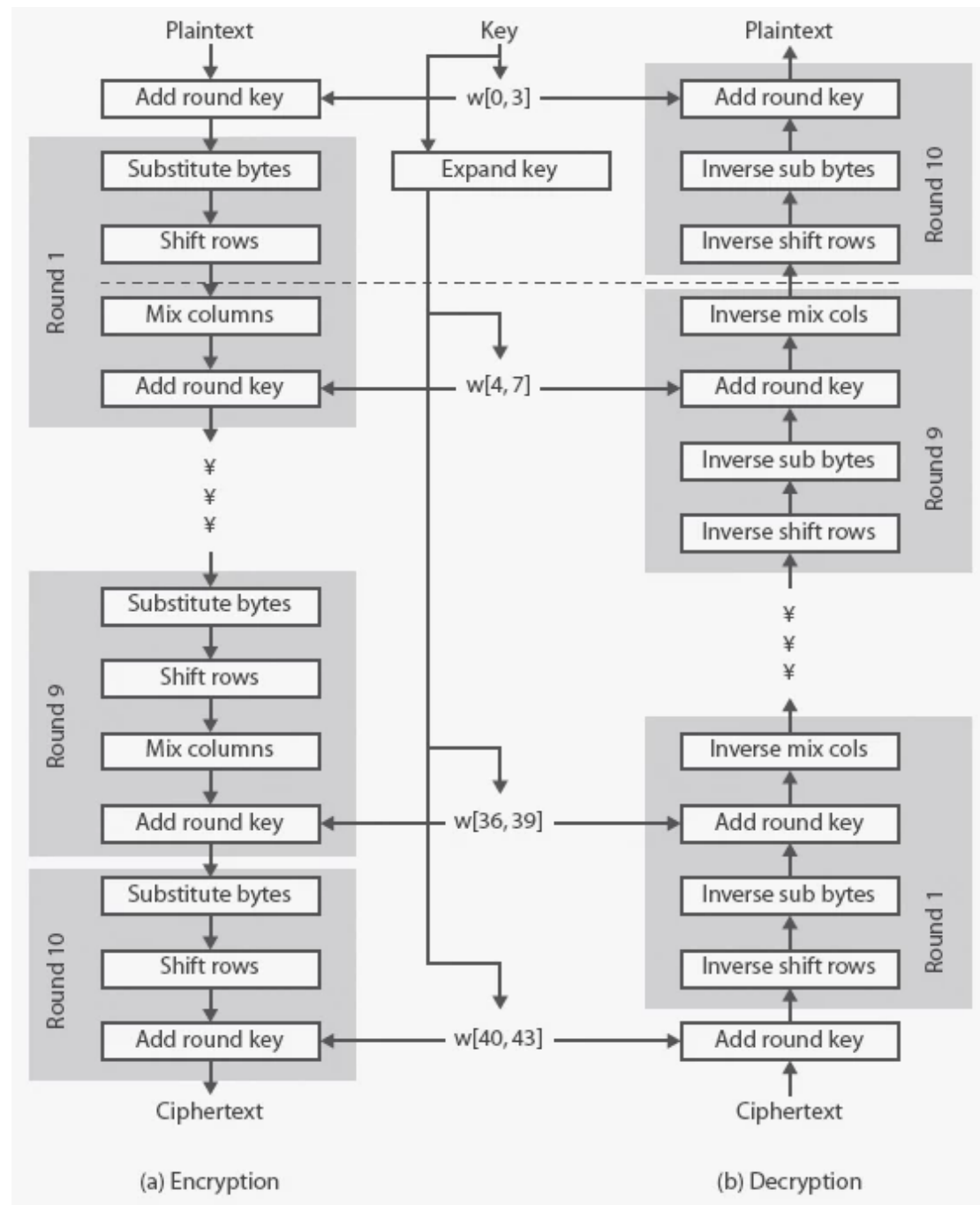
2.4 WPA Protocol

Το 2003, όταν άρχισε να γίνεται εμφανές το κενό ασφάλειας που είχε αφήσει η κρυπτογράφηση WEP, η Wi-Fi Alliance ανέπτυξε το Wi-Fi Protected Access (WPA). Το WPA προέρχεται από το πρότυπο 802.11 και αποτελεί μια ενδιάμεση λύση ασφάλειας των WLAN και μπορεί να συμπεριληφθεί με κάποιες αναβαθμίσεις στις ήδη υπάρχουσες WLAN ασύρματες συσκευές. Το WPA κάνει χρήση της μεθόδου TKIP και αυξάνει σημαντικά το επίπεδο ασφάλειας και ελέγχου πρόσβασης στα ασύρματα συστήματα LAN. Το WPA παρέχει σε κάθε πακέτο το κλειδί, έναν έλεγχο ακεραιότητας μηνύματος (MIC) που ονομάζεται Michael και ένα διάνυσμα ακολουθίας (Initialization Vector - IV). Επίσης, για τους οικιακούς χρήστες, το WPA παρέχει ένα μηχανισμό προ-μοιρασμένου κλειδιού τον PSK (Pre - Shared Key). Για να μπορέσει να εκμεταλλευτεί κάποιος την δυνατότητα του PSK θα πρέπει να εισάγει μια λέξη κωδικό και στο σημείο πρόσβασης και στο σταθμό. Αυτή η λέξη κωδικός χρησιμοποιείται για να μπορεί να επικυρώνει οποιονδήποτε σταθμό προσπαθεί να συνδεθεί στο συγκεκριμένο δίκτυο. Ο κωδικός θα πρέπει να αποτελείται από 8 έως 63 χαρακτήρες σε ASCII. Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το Pre - Shared Key WPA είναι ανθεκτικό στις επιθέσεις σπασίματος του κωδικού πρόσβασης εάν χρησιμοποιείται ένας αδύναμος κωδικός. Για να προστατευτεί από μια επίθεση ένας τυχαίος κωδικός 13 χαρακτήρων είναι πιθανώς αρκετός. Τα προϊόντα που αναγράφουν ότι έχουν "WPA Personal" σημαίνει ότι υποστηρίζουν τον PSK μηχανισμό επικύρωσης. Το πρότυπο WPA επίσης ορίζει τη χρήση του προτύπου AES (Advanced Encryption Standard) ως επιπλέον αντικατάσταση για την κρυπτογράφηση WEP. Η υποστήριξη του προτύπου AES είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο προμηθευτής, ανάλογα με τα προγράμματα οδήγησης.

2.4.1 AES (Advanced Encryption Standard)

Το WPA παρέχει τη δυνατότητα για κρυπτογράφηση με δυο αλγόριθμους, τον RC4 και τον AES (Advanced Encryption Standard) για την εμπιστευτικότητα των δεδομένων και την ακεραιότητα. Ο AES αποτελεί την νεότερη μέθοδο κρυπτογράφησης που έχει επιλεγεί από την κυβέρνηση των Ηνωμένων Πολιτειών. Ο AES χρησιμοποιεί έναν αλγόριθμο γνωστό ως Rijndael. Ο αλγόριθμος Rijndael πήρε το όνομα του από τους δυο Ελβετούς εφευρέτες του , Joan Daemen και Vincent Rijmen. Πρόκειται για έναν αλγόριθμο κρυπτογράφησης ομάδας (block) , που σημαίνει ότι λειτουργεί σε μια ομάδα σταθερού μεγέθους bits , η οποία ονομάζεται block. Αρχικά ο Rijndael παίρνει σαν είσοδο ένα μπλοκ συγκεκριμένου μεγέθους , συνήθως 128, και παράγει ένα αντίστοιχο μπλοκ εξόδου ίδιου μεγέθους. Ο μετασχηματισμούς απαιτεί μια δεύτερη είσοδο ,η οποία είναι το μυστικό κλειδί. Είναι σημαντικό να αναφέρουμε ότι το μυστικό κλειδί δεν έχει συγκεκριμένο μέγεθος και ότι ο AES χρησιμοποιεί τρία βασικά

μεγέθη : 128, 192 και 256 bytes. Η χρησιμοποίηση του προτύπου AES μας προστατεύει από τις ενεργές ασύρματες επιθέσεις.

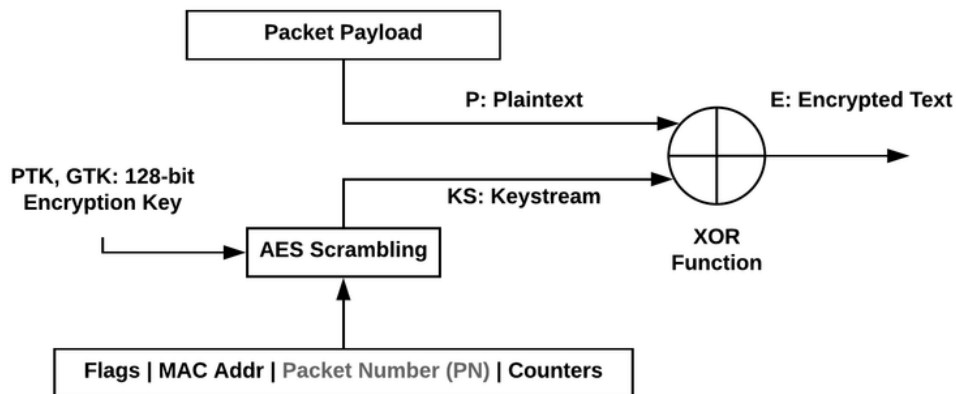


Εικόνα 2 AES [64]

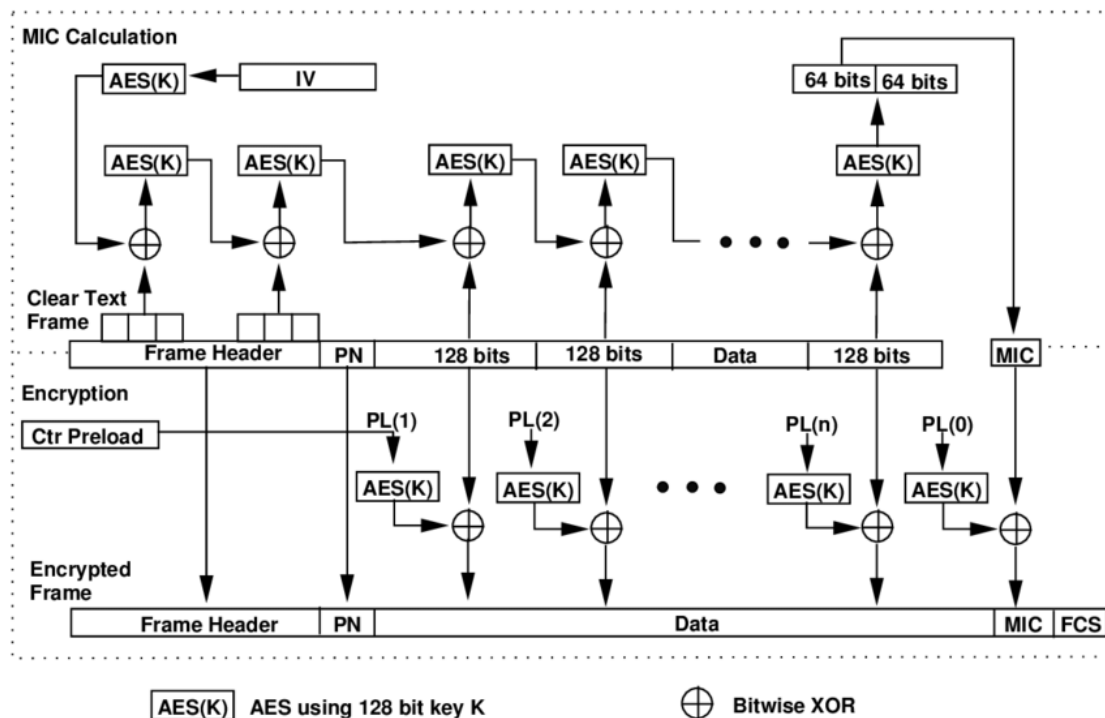
2.4.2 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

Η προσθήκη στο πρότυπο 802.11 που ορίζει την ασφάλεια της επόμενης γενιάς για τα ασύρματα δίκτυα ονομάζεται 802.Hi. Το πρότυπο αυτό εκδόθηκε το 2004. Το πρότυπο αυτό

ορίζει μια νέα μέθοδο, για την ασφάλεια των δεδομένων στο επίπεδο MAC. Η μέθοδος CCMP λειτουργεί σύμφωνα με τον αλγόριθμο κρυπτογράφησης AES. Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη των πακέτων. Το CCMP χρησιμοποιεί μέγεθος κλειδιού 128 bit και μέγεθος μπλοκ 128 bit. Μετά το CCMP το μέγεθος του πακέτου έχει επεκταθεί κατά 16 bytes, τα 8 bytes για την επικεφαλίδα του CCMP και τα άλλα 8 bytes για την ψηφιακή υπογραφή MIC (Message Integrity Code). Τα δεδομένα του πακέτου και το MIC μεταδίδονται κρυπτογραφημένα , αφού προστεθεί η αρχική επικεφαλίδα του πακέτου και η επικεφαλίδα του CCMP.



Εικόνα 3 CCMP encryption diagram [43]



Εικόνα 4 Diagram of the CCMP encapsulation process.png [36]

2.3 Τι είναι το πρωτόκολλο WPA2

Το 2004 εμφανίστηκε η προστατευμένη πρόσβαση Wi-Fi ή αλλιώς WPA και είχε την δυνατότητα να λειτουργεί σε λογισμικό που χρησιμοποιούσε WEP. Σε αντίθεση με το WEP, το WPA χρησιμοποιεί το πρωτόκολλο TKIP (Temporal Key Integrity Protocol) για τη δυναμική δημιουργία ενός νέου κλειδιού για κάθε πακέτο. Το WPA2(ή αλλιώς Wi-Fi Protected Access 2) είναι μια αναβάθμιση του WPA η οποία εξασφαλίζει ισχυρότερη ασφάλεια από την προκάτοχο της με χρήση του ακόμα πιο προχωρημένου AES ή προηγμένου πρωτοκόλλου κρυπτογράφησης, περιλαμβάνει υποχρεωτική υποστήριξη για το πρωτόκολλο CCMP, που βασίζεται στο AES. Εναλλακτικές εκδόσεις του είναι τα WPA2-PSK και WPA2-Personal. Κάθε χρήστης που συνδέεται σε ένα ασύρματο δίκτυο χρησιμοποιώντας τις μεθόδους WPA και WPA2 PSK γνωρίζει ήδη το Pre-Shared Key. Το PSK έχει μέγεθος 256 bit και προκύπτει ως εξής:

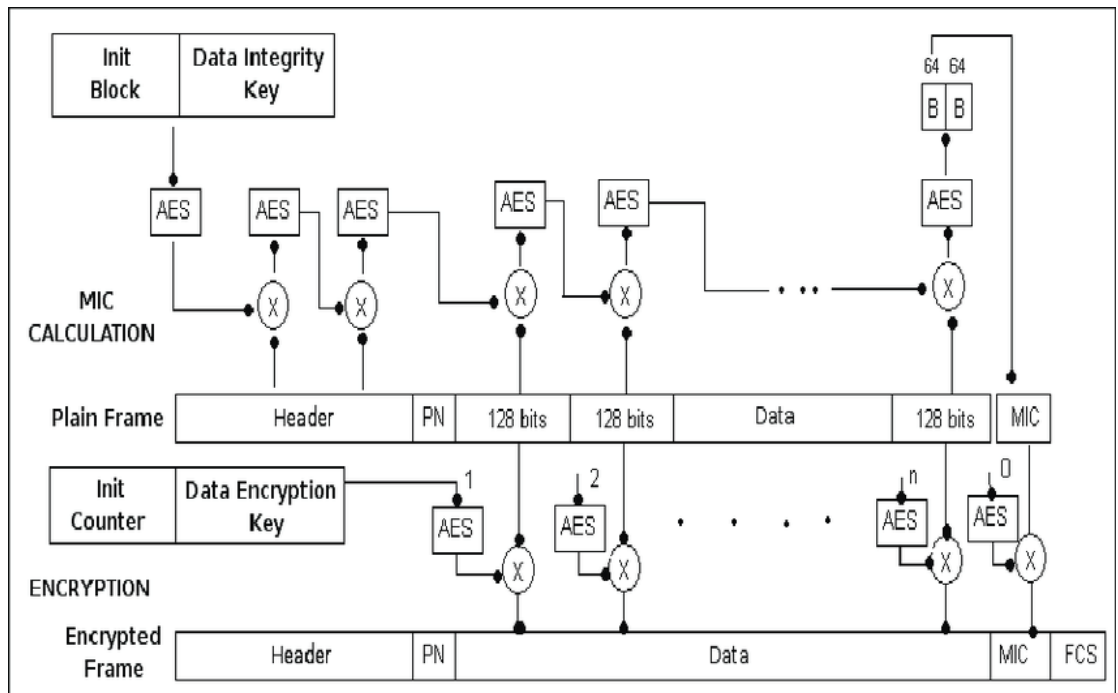
- (κωδικός πρόσβασης Wi-Fi (συνθηματική φράση) + Wi-Fi SSID, μήκος SSID + 4096 επαναλήψεις SHA1).
- Το PBKDF2_SHA1 είναι απλώς ένα παράδειγμα συνάρτησης κατακερματισμού που μπορεί επίσης να προσαρμοστεί.

Στο WPA2 PSK, το Pre-Shared Key είναι το ίδιο με το Pairwise Master Key (PMK).

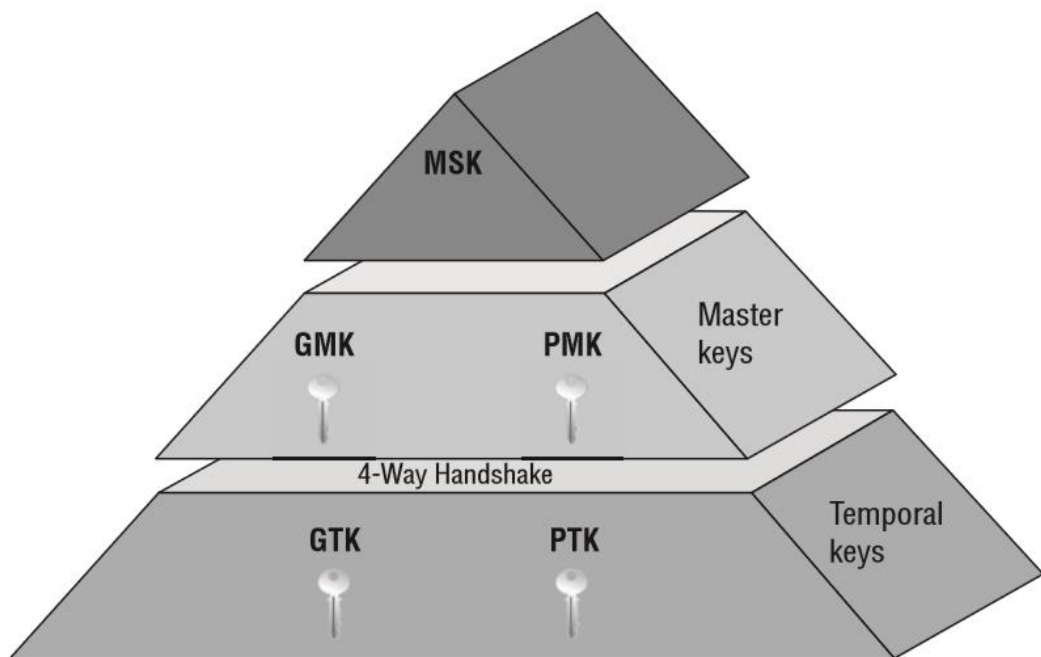
Τα κλειδιά κρυπτογράφησης προέρχονται από το PSK σε αυτή τη μέθοδο και έχουν άλλες μεταβλητές σε αυτά. Το κλειδί κρυπτογράφησης που χρησιμοποιείται για την κρυπτογράφηση όλων των δεδομένων κατά τη διαμετακόμιση μεταξύ ενός πελάτη και ενός σημείου πρόσβασης (Unicast) ονομάζεται Pairwise Transit Key (PTK). Έτσι, $PTK = PSK \text{ ή } PMK + Anonce + Snonce + MAC$ (αυθεντικοποιητής) και MAC (αιτών).

Εδώ,

- Αυθεντικοποιητής= AP
- Supplicant= πελάτης
- Anonce = τιμή 1 χρόνου για κάθε πακέτο που παράγεται από το σημείο πρόσβασης και ονομάζεται Authenticator nonce
- Snonce = τιμή 1 χρόνου που παράγεται για κάθε πακέτο από τον αιτούντα και ονομάζεται Supplicant nonce.



Εικόνα 5 WPA 2 encryption and integrity check [65]



Εικόνα 6 wpa2 key hierarchy [2]

2.4 Handshake

Για να γίνει η σύνδεση σε ένα δίκτυο πρέπει πρώτα να γίνει η αυθεντικοποίηση στην οποία κάποιο υλικό κλειδώματος πηγής μετατρέπεται σε υλικό κρυπτογράφησης

δεδομένων που θα χρησιμοποιηθεί για την κρυπτογράφηση πλαισίων δεδομένων. Αυτή η διαδικασία έχει 4 στάδια και ονομάζεται 4-way handshake.

1. Δημιουργία PTK:

Το Σημείο πρόσβασης(AP) στέλνει ένα μήνυμα με το Anonce σε αυτό. Το Anonce είναι μια τιμή εφάπαξ χρήσης ανά πακέτο.

Ο πελάτης δημιουργεί το δικό του PTK τώρα που έχει όλες τις εισόδους (και τα δύο MAC, PMK, Snonce (που δημιουργήθηκε από τον εαυτό του) και Anonce).

$$PTK = PRF (PMK + Anonce + SNonce + Mac (AA) + Mac (SA))$$

2. Δημιουργία PTK του AP (γνωστού και ως Authenticator):

Supplicant στέλνει ένα μήνυμα στο AP πίσω με το Snonce του, έτσι ώστε το AP να μπορεί να δημιουργήσει το ίδιο PTK επίσης.

Αυτό το μήνυμα αποστέλλεται με το πεδίο MIC να έχει την τιμή 1 ως έλεγχο για να διαπιστωθεί αν αυτό το μήνυμα είναι κατεστραμμένο ή όχι ή αν το κλειδί έχει αλλάξει από κάποιον άνθρωπο στη μέση ή για κάποιο άλλο λόγο.

Ο αιτών στέλνει επίσης ένα RSN IE (ή PMKID).

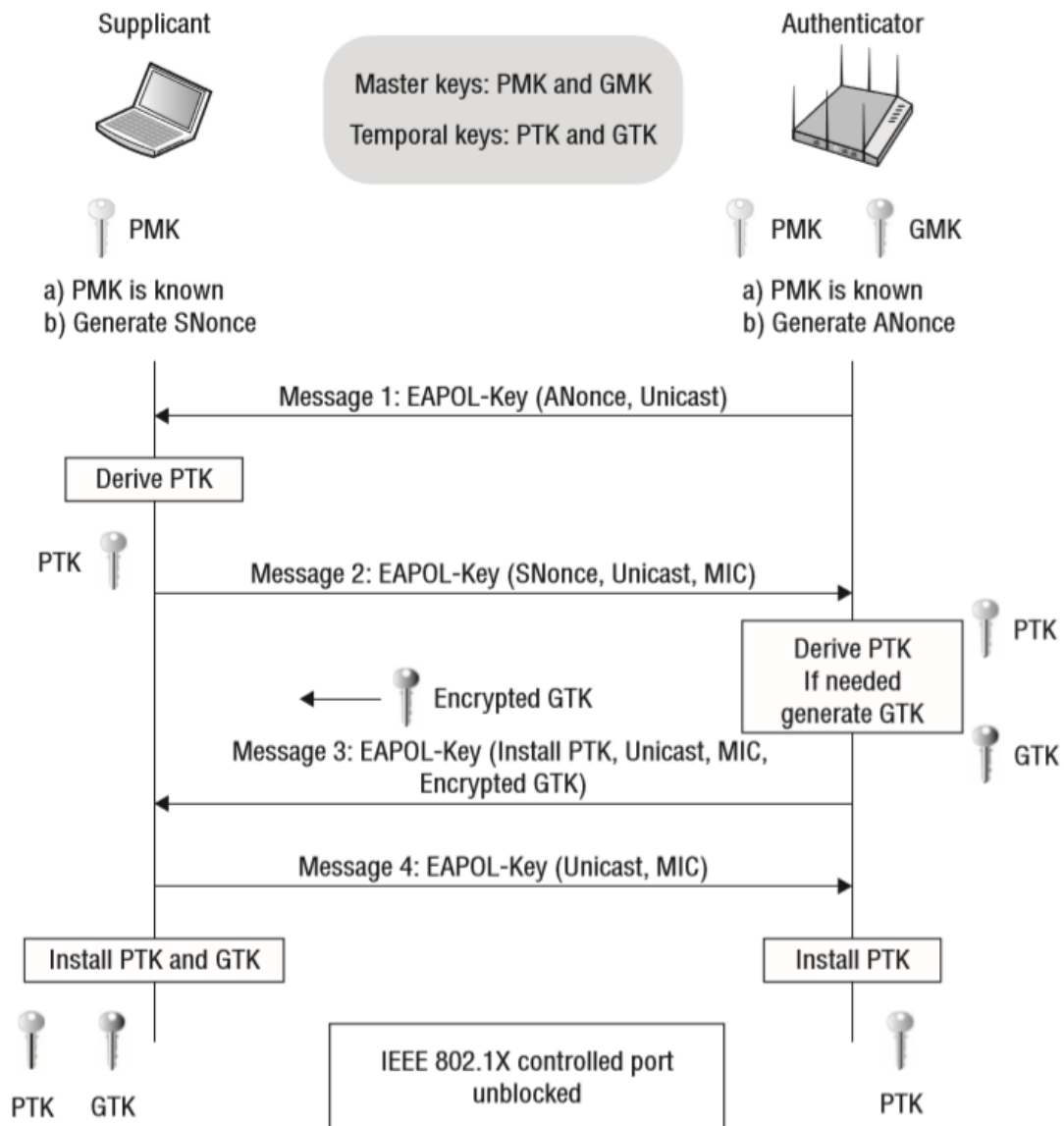
3. Δημιουργία κλειδιών ομάδας και μεταφορά από το AP στον Supplicant:

Αφού επαληθευτούν τα PTK, το Access Point αντλεί το GTK από το GMK (για επικοινωνία μετάδοσης και πολλαπλής διανομής). Το GTK παραδίδεται στον αιτούντα, το οποίο είναι κρυπτογραφημένο με το PTK.

Το μήνυμα αποστέλλεται στον supplicant για την εγκατάσταση των χρονικών κλειδιών και ένα πακέτο RSN IE αποστέλλεται επίσης στο πλαίσιο.

4. Επιβεβαίωση της εγκατάστασης των κλειδιών: Ο supplicant επιβεβαιώνει στον authenticator ότι τα κλειδιά έχουν εγκατασταθεί.

Στην επίθεση αυτή ο επιτιθέμενος στέλνει πακέτα σε έναν χρήστη που έχει πρόσβαση στο δίκτυο με αποτέλεσμα να τον διώξει από το δίκτυο και να πρέπει να ξανά κάνει το handshake με το router. Το πρόβλημα με αυτήν την επίθεση είναι ότι αρχικά θα πρέπει να υπάρχει κάποιος χρήστης μέσα στο δίκτυο και ότι είναι πολύ εύκολο να εντοπιστεί η επίθεση μιας και στέλνουμε πακέτα για να πετύχουμε την αποσύνδεση.



Εικόνα 7 handshake [32]

2.5 PMKID

2.5.1 PMK Caching and PMKID

Κάθε φορά που ο χρήστης κάνει αποσύνδεση από έναν AP η απομακρύνετε αρκετά από αυτόν τότε θα πρέπει να ξανασυνδεθεί με αποτέλεσμα να ξανακάνει 4way handshake και αυτό να έχει ως αποτέλεσμα μια χρονική καθυστέρηση .

Για να κάνουμε αυτή τη μεταβίβαση χωρίς υστέρηση, διαθέτουμε ένα χαρακτηριστικό που ονομάζεται προσωρινή αποθήκευση PMK.

Πολλοί δρομολογητές αποθηκεύουν το PMKID της διαδικασίας ανταλλαγής σε μια συλλογή πληροφοριών PMKSA, έτσι ώστε την επόμενη φορά που ο πελάτης αποσυνδέετε και επαναπιστοποιεί την ταυτότητα δεν θα γίνει ξανά χειραψία 4 κατευθύνσεων και ο δρομολογητής θα ζητήσει απευθείας από τον πελάτη το PMKSA, θα το επαληθεύσει και θα τον επανασυνδέσει με ένα σημείο πρόσβασης.

- $PMKSA = PMKID + \text{διάρκεια ζωής του PMK} + \text{διευθύνσεις MAC} + \text{άλλες μεταβλητές.}$

Το PMKID είναι μια κατακερματισμένη τιμή μιας άλλης κατακερματισμένης τιμής (PMK) με 2 MAC και μια σταθερή συμβολοσειρά.

- $PMKID = \text{HMAC-SHA1-128}(PMK, \text{"PMK Name"} + \text{MAC (AP)} + \text{MAC(Suppllicant)})$

Η HMAC-SHA1 είναι και πάλι απλώς ένα παράδειγμα ψευδοτυχαίας συνάρτησης. Το PMKID είναι ένα πεδίο στο πλαίσιο RSN IE (Robust Security Network Information Element). Το RSN IE είναι ένα προαιρετικό πλαίσιο που βρίσκεται στους δρομολογητές. Το "PMK Name" είναι μια σταθερή ετικέτα συμβολοσειράς που σχετίζεται με το SSID. Τώρα, αυτό το PMKID έχει αποθηκευτεί στον δρομολογητή και την επόμενη φορά που ο πελάτης μου θα συνδεθεί στο AP, το AP και ο πελάτης θα επαληθεύσουν απλά αυτό το PMKID και δεν απαιτείται ξανά καθεστώς χειραψίας 4 κατευθύνσεων. Η προσωρινή αποθήκευση του PMKID γίνεται σε διάφορα δίκτυα IEEE 802.11 με δυνατότητα περιαγωγής. Πολλοί πωλητές παρέχουν πρόσθετα χαρακτηριστικά ασφαλείας RSN αυτές τις μέρες, καθώς η προβολή των επιθέσεων PMKID αυξάνεται.

Το PMKID υπολογίζεται χρησιμοποιώντας το HMAC-SHA1 όπου το κλειδί είναι το PMK και το τμήμα δεδομένων είναι η συνένωση μιας ετικέτας σταθερής συμβολοσειράς "PMK Name", η διεύθυνση MAC του σημείου πρόσβασης και η διεύθυνση MAC του σταθμού. Το PMKID είναι το μοναδικό αναγνωριστικό κλειδιού που χρησιμοποιείται από το AP για να παρακολουθεί το PMK που χρησιμοποιείται για τον πελάτη. Το PMKID είναι ένα παράγωγο των AP MAC, Client MAC, PMK και PMK Name. ($PMKID = \text{HMAC-SHA1-128}(PMK, \text{"PMK Name"} | \text{MAC_AP} | \text{MAC_STA})$).

2.5.2 PMKID επίθεση

Παρατηρήστε πώς αν είμαστε σε θέση να ανακτήσουμε το PMKID από ένα Access Point, θα πάρουμε στα χέρια μας μια κατακερματισμένη τιμή που περιέχει τον κωδικό πρόσβασης. Η επίθεση PMKID στοχεύει άμεσα σε ένα μόνο πλαίσιο RSN IE. Δεδομένου ότι το PMKID προέρχεται από το PMK, μια σταθερή συμβολοσειρά και 2 MACs ορίζεται ως "ιδανικός φορέας επίθεσης" από το Hashcat. Γνωρίζουμε τώρα πώς δημιουργείται το PMK. Έτσι, για να κάνουμε brute force το PMKID, χρειαζόμαστε τις ακόλουθες παραμέτρους:

- Κωδικός πρόσβασης WiFi (passphrase) - μαντέψτε.
- WiFi SSID - γνωστό
- Μήκος του SSID - γνωστό
- MAC του Authenticator και του Supplicant - γνωστό
- Όνομα PMK - γνωστό

Έτσι, χρειαζόμαστε μόνο:

Μαντέψτε τη φράση πρόσβασης Wi-Fi χρησιμοποιώντας λεξικό -> δημιουργήστε κατακερματισμό PMK -> δημιουργήστε κατακερματισμό PMKID και συγκρίνετε με τον ανακτηθέντα κατακερματισμό PMKID.

Σύμφωνα με το αρχικό άρθρο του Hashcat εδώ, τα κύρια πλεονεκτήματα είναι τα εξής:

- Δεν απαιτούνται πλέον τακτικοί χρήστες - επειδή ο επιτιθέμενος επικοινωνεί απευθείας με το AP (γνωστή και ως επίθεση "χωρίς πελάτη").
- Δεν υπάρχει πλέον αναμονή για μια πλήρη χειραψία 4 κατευθύνσεων μεταξύ του κανονικού χρήστη και του AP.
- Δεν υπάρχουν πλέον ενδεχόμενες επαναμεταδόσεις των πλαισίων EAPOL (που μπορεί να οδηγήσουν σε μη παραβιάσιμα αποτελέσματα).
- Τέρμα οι ενδεχόμενοι άκυροι κωδικοί πρόσβασης που αποστέλλονται από τον κανονικό χρήστη.
- Τέρμα οι απώλειες πλαισίων EAPOL όταν ο κανονικός χρήστης ή το AP βρίσκεται πολύ μακριά από τον επιτιθέμενο.
- Δεν απαιτείται πλέον καθορισμός των τιμών nonce και replaycounter (με αποτέλεσμα ελαφρώς υψηλότερες ταχύτητες).
- Δεν υπάρχει πλέον ειδική μορφή εξόδου (pcap, hccapx κ.λπ.) - τα τελικά δεδομένα θα εμφανίζονται ως κανονική δεκαεξαδική κωδικοποιημένη συμβολοσειρά.

Με λίγα λόγια στην επίθεση αυτή ο επιτιθέμενος απλά με ένα πρόγραμμα συλλέγει δεδομένα μέχρι να βρει το pmkid το οποίο σε αντίθεση με την προηγούμενη επίθεση δεν χρειάζεται να υπάρχει κάποιος στο δίκτυο γιατί το pmkid το δίνει το ρούτερ και έτσι δεν μπορεί να γίνει αντιληπτή η επίθεση.

Κεφάλαιο 3 Ανάλυση Προγραμμάτων

3.1 Hcxdumpptool

Το hcxdumpptool χρησιμοποιήθηκε για να την συλλογή των δειγμάτων της εργασίας. Είναι ένα πρόγραμμα το οποίο δημιουργήθηκε για να μπορεί να μαζεύει data που περιέχουν το pmkid αλλά μπορεί να κάνει ταυτόχρονα και την διαδικασία που χρειάζεται για το handshake εύκολη και γρήγορη καθώς με ένα πρόγραμμα μπορείς να κάνεις επίθεση στο δίκτυο και να καταγράφει τα δεδομένα ενώ κανονικά θέλει 3 διαφορετικά προγράμματα και η διαδικασία γίνεται μεμονωμένα για κάθε δίκτυο ενώ με το hcxdumpptool μπορείς να τα κάνεις όλα αυτά αυτοματοποιημένα γλιτώνοντας χρόνο και πόρους.

3.2 Aircrack

Το Aircrack-ng είναι μια πλήρης σουίτα εργαλείων για την αξιολόγηση της ασφάλειας του δικτύου WiFi. Επικεντρώνεται σε διάφορους τομείς ασφάλειας WiFi:

Παρακολούθηση: Λήψη πακέτων και εξαγωγή δεδομένων σε αρχεία κειμένου για περαιτέρω επεξεργασία από εργαλεία τρίτων

- Επίθεση: Επιθέσεις επανάληψης, εξακρίβωση ταυτότητας, πλαστά σημεία πρόσβασης και άλλα μέσω εισαγωγής πακέτων
- Δοκιμή: Έλεγχος καρτών WiFi και δυνατοτήτων προγραμμάτων οδήγησης (σύλληψη και έγχυση)
- Σπάσιμο: WEP και WPA PSK (WPA 1 και 2)

Εμείς για την επίθεση μας χρησιμοποιήσαμε το aircrack για να σπάσουμε τα δίκτυα και αυτό το κάναμε με είσοδο την λίστα των δειγμάτων μας και την λίστα με τους κωδικούς.

3.3 Hashcat

Το Hashcat είναι ένα προηγμένο βοηθητικό πρόγραμμα ανάκτησης κωδικού πρόσβασης που βασίζεται σε CPU/GPU και υποστηρίζει επτά μοναδικούς τρόπους επίθεσης για περισσότερους από 100 βελτιστοποιημένους αλγόριθμους κατακερματισμού. Το πρόγραμμα αυτό μας βοηθάει να σπάσουμε γρηγορότερα κωδικούς σε σχέση με το aircrack μιας και το σπάσιμο κωδικών με κάρτα γραφικών είναι γρηγορότερο επειδή περιέχει περισσότερους πυρήνες οπότε έχει μεγαλύτερες ταχύτητες και επεξεργάζεται περισσότερους κωδικούς ταυτόχρονα.

Κεφάλαιο 4 Δείγματα

4.1 Διαδικασία συλλογής δειγμάτων

Η συλλογή δειγμάτων έγινε σε 2 διαφορετικές πόλεις, την Νάουσα Ημαθίας και την Θεσσαλονίκη. Σε ένα laptop περάστηκε ένας δίσκος με λογισμικό kali Linux και εκεί περάστηκε το hcxdumpptool, το Wireshark για την ανάγνωση των πακέτων. Έπειτα χρησιμοποιήθηκε ως κάρτα δικτύου η tplink tl-wn722n v2 και μια κεραία 6 dbi και αφού στήθηκε το σύστημα ενσωματώθηκε σε ένα τροποποιημένο backpack ώστε να μην φαίνεται και να είναι βολικό στο κουβάλημα αλλά και να είναι και ο πομπός στο πάνω μέρος για καλύτερη εμβέλεια και δυνατή συλλογή δειγμάτων. Η συλλογή δειγμάτων έγινε σε κατοικημένες περιοχές και κυρίως σε βραδινές ώρες ώστε να μην υπάρχουν άνθρωποι στους δρόμους με κινητά τηλέφωνα ή μαγαζιά με εκτυπωτές και έξυπνες συσκευές που εκπέμπουν το δικό τους σήμα wifi και θα μπορούσαν να καθυστερήσουν την διαδικασία και να επηρεάσουν τα δεδομένα της δειγματοληψίας.

4.2 Προβλήματα στην συλλογής δειγμάτων

Κατά την συλλογή δειγμάτων αντιμετωπίσαμε πολλά προβλήματα τα οποία καθιστούσαν τα δεδομένα μας άχρηστα για την δειγματοληψία μας. Αρχικά το κύριο πρόβλημα είναι ότι σε πολλά πακέτα δεν μπορούσε να βρει το ssid ακόμα και αν έβρισκε handshake το οποίο δεν μπορεί να τρέξει στο μηχάνημα μας γιατί ο αλγόριθμος είναι τυφλός χωρίς αυτό μιας και είναι μια από της μεταβλητές που χρειάζεται. Επίσης το μεγαλύτερο πρόβλημα που αντιμετωπίσαμε κυρίως στην Θεσσαλονίκη είναι ότι πολλά από τα δίκτυα ήταν από hotspot είτε smartphones είτε εκτυπωτών και άλλων έξυπνων συσκευών με αποτέλεσμα να παρεμβάλουν σε άλλα σήματα και να βγάζουν δίπλες ενδείξεις μιας και από την αρχή μας είναι αχρείαστα για την επίθεσή μας.

4.3 Πρακτικό μέρος – Εργαστηριακό περιβάλλον

Σε αυτήν την ενότητα δείχνουμε τα βήματα που χρειάζονται για να σπάσουμε έναν κωδικό. Στο συγκεκριμένο πείραμα ο σκοπός δεν είναι να σπάσουμε άγνωστο κωδικό (στην ουσία εμείς θέσαμε των κωδικό), αλλά να δείξουμε τα βήματα που χρειάζονται για την συγκεκριμένη διαδικασία.

Βήμα 1 Αρχικά θα πρέπει να γίνει η εγκατάσταση το πρόγραμμα για να μπορούμε να κάνουμε capture τα δίκτυα από το GitHub repository με την εντολή `git clone https://github.com/ZerBea/hcxttools.git` κατεβάζουμε το repo και μετά με την εντολή `cd`

hcxtools πάμε στον φάκελο που έχει κατεβεί και κάνουμε *make && make install* για να φτιάξουμε το make file και να το τρέξουμε ώστε να γίνει η εγκατάσταση του hcxtool που έχει εργαλεία για να μπορούμε με τροποποιήσουμε το αρχείο μας.

```
(kali㉿kali)-[~/Desktop]
$ sudo git clone https://github.com/ZerBea/hcxtools.git
Cloning into 'hcxtools' ...
remote: Enumerating objects: 9358, done.
remote: Counting objects: 100% (163/163), done.
remote: Compressing objects: 100% (86/86), done.
remote: Total 9358 (delta 84), reused 123 (delta 76), pack-reused 9195
Receiving objects: 100% (9358/9358), 2.86 MiB | 978.00 KiB/s, done.
Resolving deltas: 100% (6452/6452), done.
```

Εικόνα 8 hcxtools.git

Βήμα 2 Με την εντολή *git clone* κατεβάζουμε το repo και μετά με την εντολή *cd hcxdumpool* πάμε στον φάκελο που έχει κατεβεί και κάνουμε *make && make install* για να φτιάξουμε το make file και να το τρέξουμε ώστε να γίνει η εγκατάσταση του hcxdumpool που έχει εργαλεία για να μπορούμε με τροποποιήσουμε το αρχείο μας.

Βήμα 3 Με την εντολή *iwconfig* μπορούμε να δούμε όλα τους ασύρματους δέκτες που έχουμε και εκεί βλέπουμε την κάρτα δικτύου μας που θέλουμε να χρησιμοποιήσουμε.

```
(kali㉿kali)-[~/Desktop/hcxtools]
$ iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

wlan0       IEEE 802.11  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Power Management:off
```

Εικόνα 9 iwconfig

Βήμα 4 Ενεργοποιούμε την κάρτα δικτύου μας σε capture mode ώστε να μπορεί να κάνει capture χωρίς κανένα πρόβλημα με την εντολή *sudo airmon-ng start name* και όπου name βάζουμε το wlan πχ.(wlan0 wlan1) και με την εντολή *kill number* (number ότι pid μας βγάζει από πάνω) σταματάμε της εξτρά λειτουργίες που κάνει και μπορούν να μας δημιουργήσουν προβλήματα.

```
(kali@kali)-[~/Desktop/hcxtools]
$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    548 NetworkManager
    2178 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0             ath9k_htc   Qualcomm Atheros Communications AR9271 802.11n
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

Εικόνα 10 airmon

Βήμα 5 Χρησιμοποιούμε την εντολή `sudo hcxdumpool -o test.pcapng -i wlan0mon --enable_status=1` (όπου wlan0mon βάζουμε το δικό μας) ώστε να αρχίσει να ψάχνει για handshake και pmkid data και να τα αποθηκεύσει στο αρχείο test.pcapng.

```
TIME      FREQ/CH  MAC_DEST  MAC_SOURCE  ESSID [FRAME TYPE]
20:58:18  2437/6   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:283 RC:
62155 KDV:2]
20:58:19  2437/6   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:302 RC:
62155 KDV:2]
20:58:19  2437/6   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2 EAPOLTIME:2815 RC:1 KD
V:2]
20:58:19  2437/6   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M2M3 EAPOLTIME:12964 RC:2 K
DV:2]
20:58:19  2437/6   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M3M4ZEROED EAPOLTIME:2811 R
C:2 KDV:2]
20:58:22  2442/7   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:1131 RC
:62155 KDV:2]
20:58:22  2442/7   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:16 RC:6
2155 KDV:2]
20:58:22  2442/7   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:12 RC:6
2155 KDV:2]
20:58:22  2442/7   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:265 RC:
62155 KDV:2]
20:58:23  2442/7   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:236 RC:
62155 KDV:2]
20:58:23  2442/7   [REDACTED] [REDACTED] [EAPOL:300 [EAPOL:M1M2ROGUE EAPOLTIME:143 RC:
62155 KDV:2]
20:58:39  2462/11  [REDACTED] [REDACTED] [EAPOL:300 38E7C6 [PMKIDROGUE:430091e8f1ffe806
1f99c39fa65201cc KDV:2]
^C
terminating ...
```

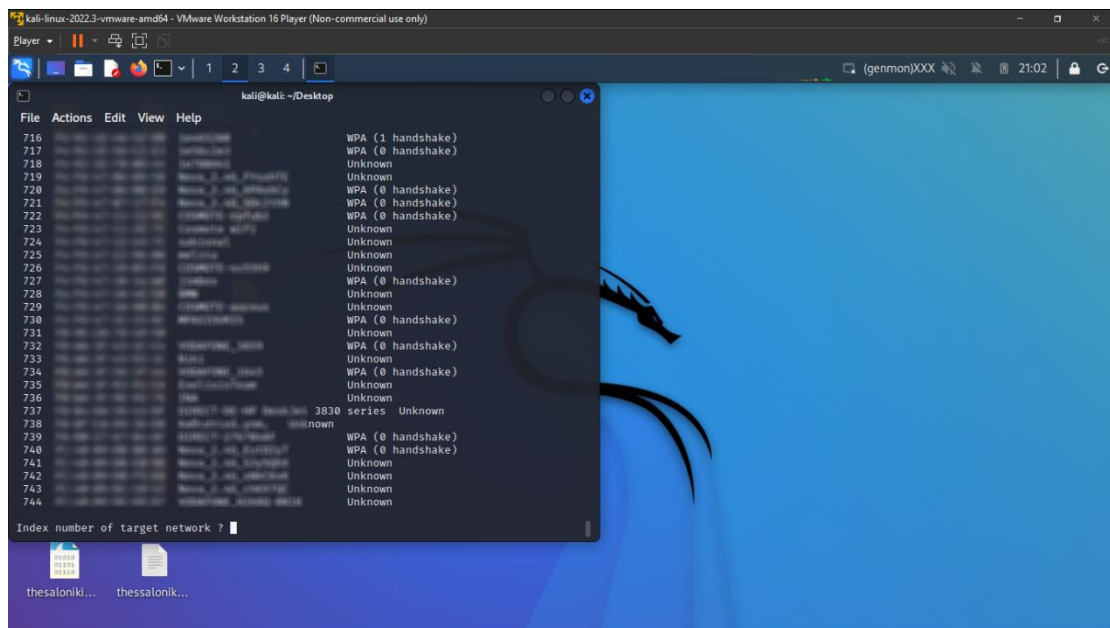
Εικόνα 11 capture pmkid

Βήμα 6 Θα πρέπει να μετατρέψουμε το αρχείο που δημιουργήθηκε από .pcapng σε .pcap και αυτό το κάνουμε με την εντολή `tcpdump -r test.pcapng -w test.pcap` και πλέον το αρχείο μας είναι έτοιμο να μπει στο aircrack.

```
(kali@kali)-[~/Desktop/hcxtools]
$ sudo tcpdump -r test12.pcapng -w test.pcap
reading from file test12.pcapng, link-type IEEE802_11_RADIO (802.11 plus radiotap header), snapshot length 65535
```

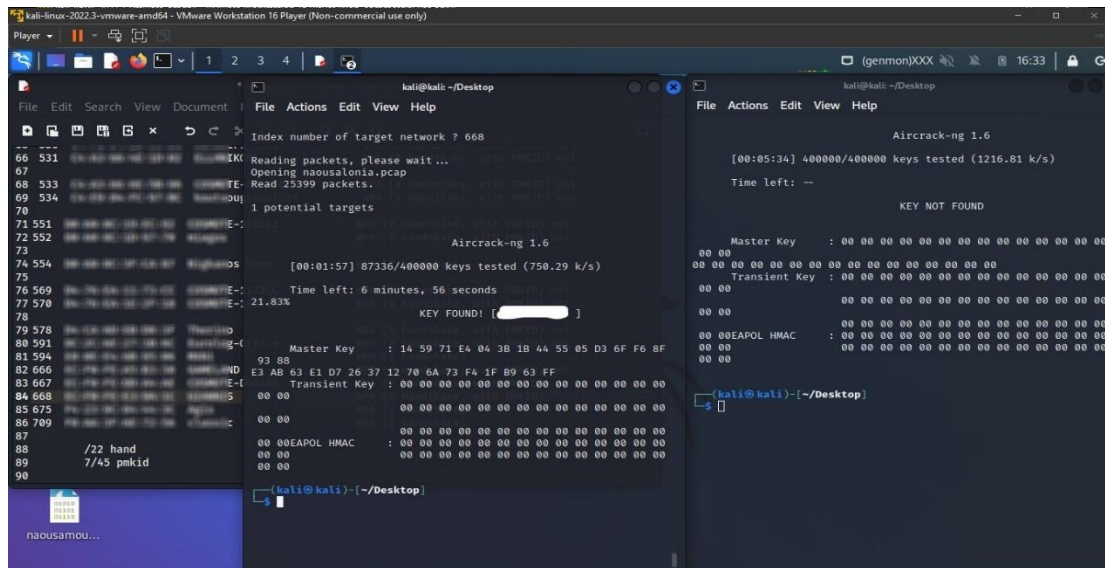
Εικόνα 12 tcpdump

Βήμα 7 Με την εντολή `aircrack-ng test.pcap` μπορούμε να δούμε την λίστα με όλα τα δίκτυα που έχουμε κάνει capture στο terminal και κάνοντας copy-paste σε ένα note με την βοήθεια της αναζήτησης μπορούμε να βρούμε όλα τα pmkid και handshake και να κρατήσουμε τον αριθμό του πακέτου.



Εικόνα 13 aircrack cap

Βήμα 8 Με την εντολή `aircrack-ng -w test.dic test.pcap` θα μας βγάλει την λίστα με τα πακέτα όπως και πριν και θα μας ζητάει να βάλουμε τον αριθμό του πακέτου ώστε να αρχίσει το brute force με την λίστα test.dic που έχουμε η που μπορούμε να φτιάξουμε με το crunch.

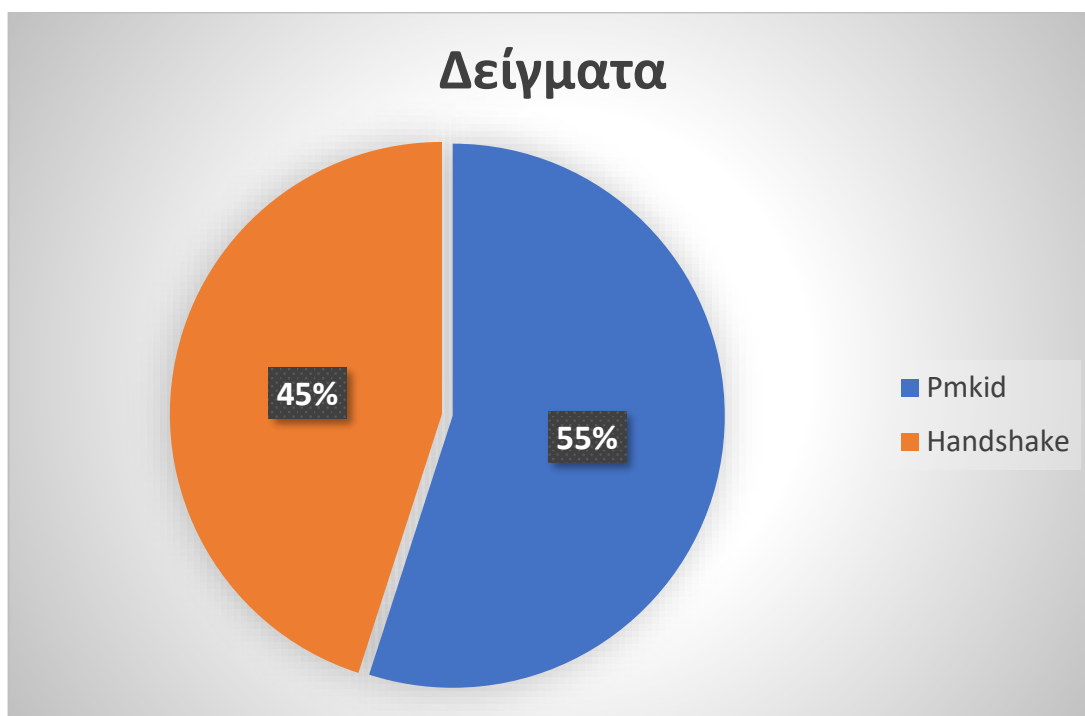


Εικόνα 14 cracked network

Κεφάλαιο 5 Αποτελέσματα δειγματοληψίας

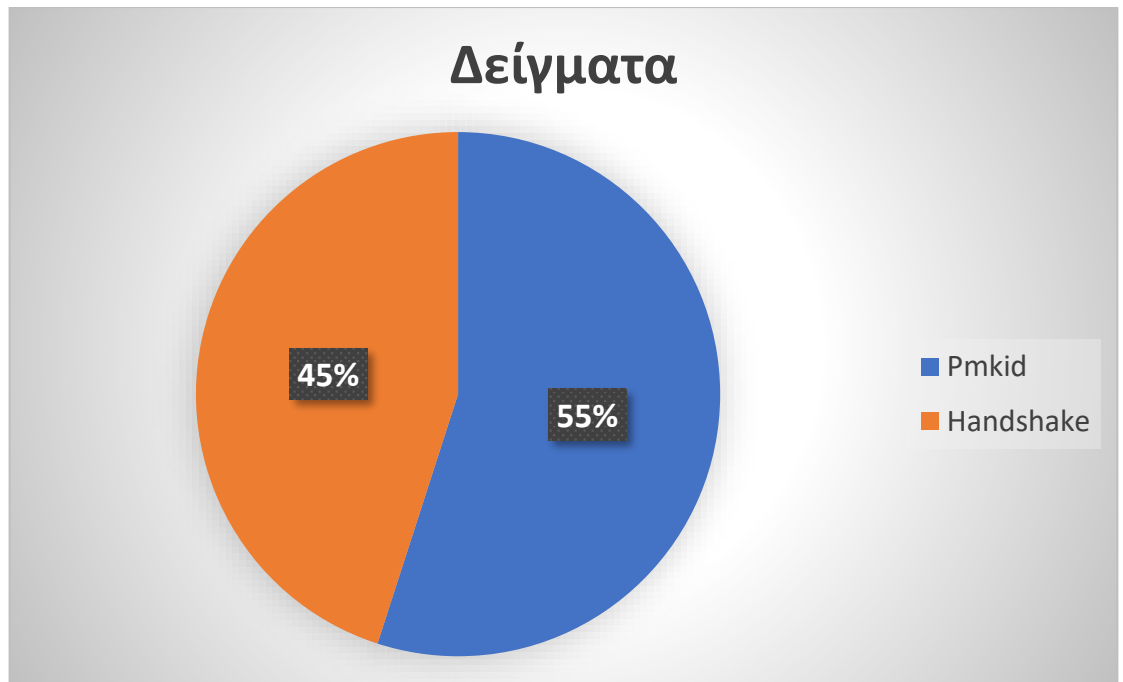
5.1 Νάουσα

Στην πόλη της Νάουσας τα καθαρά δήγματα ήταν 440 , από τα οποία τα 233 ήταν pmkid και τα 207 ήταν handshake. Η πόλη της Νάουσας δεν έχει σε πολλά σημεία vdsl οπότε ήταν λογικά τα αποτελέσματα μας.



5.2 Θεσσαλονίκη

Στην Θεσσαλονίκη τα καθαρά δείγματα μας ήταν 533 από τα οποία τα 293 ήταν pmkid και τα 240 ήταν handshake. Η πόλη της Θεσσαλονίκης είχε πολύ θόρυβο στα δεδομένα λόγω πληθυσμού και τεχνολογίας με αποτέλεσμα από τα 7000 δήγματα μόνο τα 533 ήταν καθαρά δήγματα.



5.3 Σύγκριση Αποτελεσμάτων

Και στις 2 πόλεις τα δείγματα pmkid ήταν περισσότερα από το handshake και έχει και το μειονέκτημα ότι είναι μόνο για vdsl router. Αναλυτικότερα στην Νάουσα η διαφορά είναι στα 26 δίκτυα ενώ στην Θεσσαλονίκη η διαφορά είναι στα 53 δίκτυα. Τα αποτελέσματα από τα δείγματα μας έδειξαν ότι το 70% των δικτύων ήταν της cosmote το 20% είχαν αλλαγμένο όνομα και το υπόλοιπο 10% ήταν από wind/Vodafone/inalan. Αυτό οφείλετε στο γεγονός ότι η cosmote έχει ADSL/VDSL router οπότε η επίθεση δουλεύει και σε αυτούς που έχουν adsl και σε vdsl μιας και το router είναι το ίδιο.

Κεφάλαιο 6 Τελικά συμπεράσματα και λύσεις

6.1 Συμπεράσματα

Τα συμπεράσματα που βγάλαμε από αυτήν την πτυχιακή εργασία σχετικά με την επίθεση pmkid είναι ότι σαν επίθεση είναι αρκετά γρήγορη στην συλλογή των πακέτων , δεν αφήνει αποτύπωμα πίσω της οπότε οι χρήστες δεν μπορούν να καταλάβουν ότι έχει γίνει αυτή η επίθεση με το μοναδικό μειονέκτημα της επιθέσεις ότι μπορεί να γίνει μόνο σύγχρονα routers όπως είναι τα vdsl routers αν και το vdsl ανεβαίνει πολύ στην χώρα μας και ο κυρίως πάροχος της Ελλάδας είναι η cosmote η οποία έχει ευπάθεια σε όλα της τα router ανεξαρτήτως γραμμής. Με λίγα λόγια λόγω της εξέλιξης τον ρούτερ για να παρέχουν vdsl ταχύτητες έχουν δημιουργηθεί και νέες ευπάθειες γι' αυτό και είναι καλό να πάμε στην εξελιγμένη έκδοση του wpa που είναι η version 3.

Attack	Solved by WPA3
<i>Deauthentication</i>	Yes
<i>Handshake Capture Dictionary Attack</i>	Yes
<i>PMKID Hash Dictionary Attack</i>	Yes
<i>Rogue Access Point</i>	Partially
<i>Evil Twin Attack</i>	No
<i>Handshake Capture En/Decryption</i>	Yes
<i>KRACK Exploit</i>	Yes
<i>ARP Spoofing</i>	Partially
<i>SSL Stripping</i>	No
<i>DNS Spoofing</i>	No

Εικόνα 15wpa3 solved attacks [44]

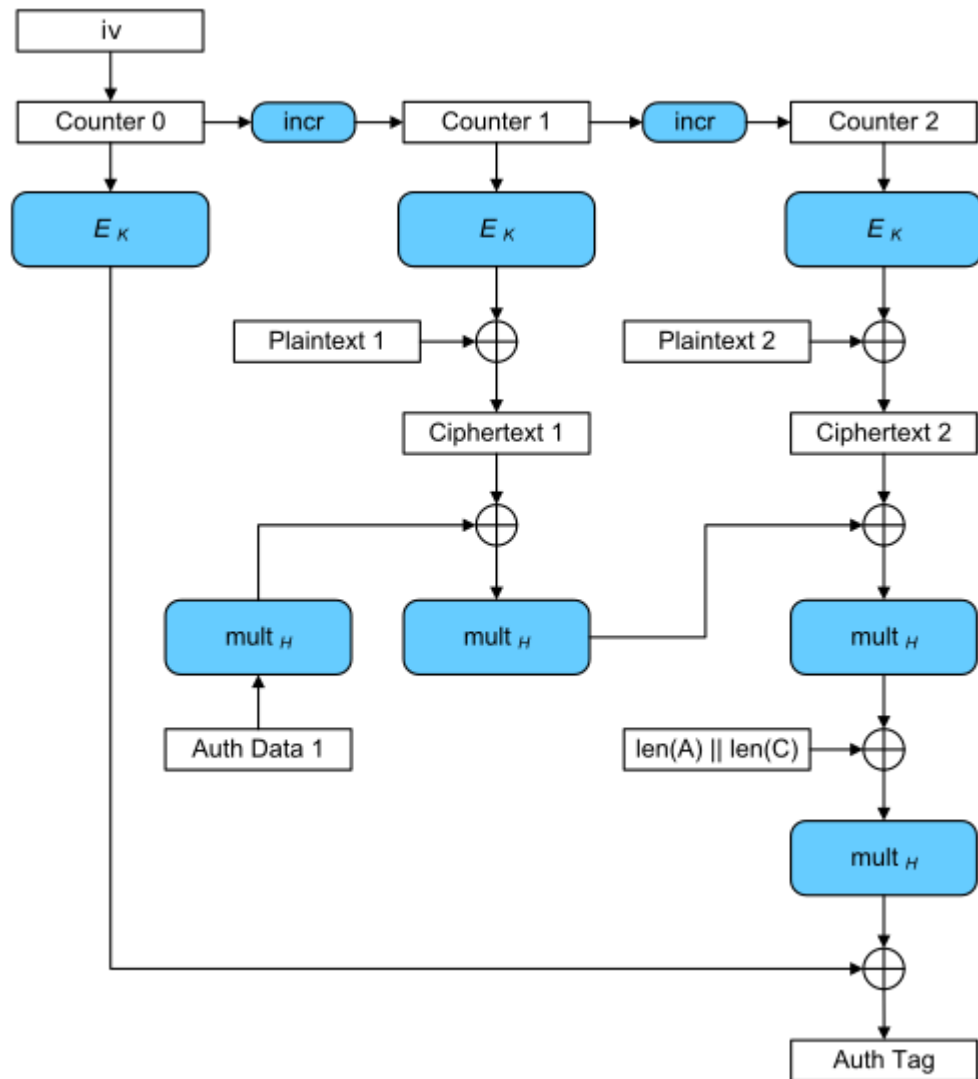
6.2 WPA3 Protocol

Το WPA3, επίσης γνωστό ως Wi-Fi Protected Access 3, είναι η τρίτη επανάληψη ενός προτύπου πιστοποίησης ασφάλειας που αναπτύχθηκε από τη Wi-Fi Alliance. Το WPA3 είναι η πιο πρόσφατη επικαιροποιημένη εφαρμογή του WPA2, το οποίο χρησιμοποιείται από το 2004. Η Wi-Fi Alliance άρχισε να πιστοποιεί προϊόντα εγκεκριμένα με WPA3 το 2018. Το WPA3 έχει σχεδιαστεί για να βελτιώσει την ασφάλεια των ασύρματων δικτύων. Αποτελεί σημαντική βελτίωση σε σχέση με το WPA2, καθώς παρέχει αυξημένη προστασία των δεδομένων που διακινούνται σε προσωπικά και εταιρικά δίκτυα Wi-Fi. Οι ενημερώσεις του

WPA3 περιλαμβάνουν καλύτερη προστασία για απλούς κωδικούς πρόσβασης, κρυπτογράφηση για προσωπικά και ανοικτά δίκτυα και ασφαλέστερη κρυπτογράφηση για δίκτυα επιχειρήσεων. Το πρωτόκολλο WPA3 παρέχει νέα χαρακτηριστικά για προσωπική και επιχειρηματική χρήση, όπως ένα πρωτόκολλο Galois/Counter Mode 256-bit (GCMP-256) που είναι πιο δύσκολο να παραβιαστεί, 384-bit Hashed-based Message Authentication Code (HMAC) και 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256). Το πρωτόκολλο WPA3 υποστηρίζει επίσης μέτρα ασφαλείας όπως η τέλεια μυστικότητα προς τα εμπρός, η οποία παράγει μια προσωρινή ανταλλαγή ιδιωτικών κλειδιών μεταξύ πελατών και διακομιστών. Ένα μοναδικό κλειδί συνόδου δημιουργείται για κάθε μεμονωμένη σύνοδο που ξεκινά ένας χρήστης. Ωστόσο, η υποστήριξη WPA3 δεν προστίθεται αυτόματα σε κάθε συσκευή. Οι χρήστες που επιθυμούν να χρησιμοποιήσουν συσκευές εγκεκριμένες με WPA3 πρέπει είτε να αγοράσουν έναν δρομολογητή που υποστηρίζει WPA3 είτε να ελπίζουν ότι η συσκευή τους υποστηρίζει το νέο πρωτόκολλο.

Τα βασικά χαρακτηριστικά του WPA3 περιλαμβάνουν τα εξής:

- Το Management Frame Protection (MFP) προστατεύει τα πλαίσια διαχείρισης unicast και broadcast και κρυπτογραφεί τα πλαίσια διαχείρισης unicast. Αυτό σημαίνει ότι τα ασύρματα συστήματα ανίχνευσης εισβολών και πρόληψης εισβολών έχουν πλέον λιγότερους τρόπους ωμής βίας για την επιβολή πολιτικών πελατών.
- Simultaneous Authentication of Equals (SAE) επιτρέπει τον έλεγχο ταυτότητας με βάση τον κωδικό πρόσβασης και έναν μηχανισμό συμφωνίας κλειδιών. Αυτό προστατεύει από επιθέσεις brute-force.
- Η λειτουργία μετάβασης (Transition mode) είναι μια μικτή λειτουργία που επιτρέπει τη χρήση του WPA2 για τη σύνδεση πελατών που δεν υποστηρίζουν το WPA3.



Εικόνα 16GCM Galois Counter Mode [37]



More Secure Technologies



Protection against Brute-Force Attacks

More secure handshakes when devices connect to access points, using the SAE protocol



Advanced Enterprise Security

Increased security for enterprise environments with 192-bit key-based encryption



More Secure Applications



Improved System for Adding Wi-Fi Devices

Simplify and secure the process of adding IoT devices with DPP



Worry-Free Open Public Networks

Enhance the security of open public networks using OWE

Εικόνα 17 wpa3 new features [28]

6.2.1 Λειτουργίες ασφαλείας WPA3

6.2.1.1 WPA3-Personal

Το WPA3-Personal προσφέρει καλύτερη προστασία στους μεμονωμένους χρήστες, παρέχοντας πιο ισχυρή πιστοποίηση με βάση τον κωδικό πρόσβασης, ακόμη και όταν οι χρήστες επιλέγουν κωδικούς πρόσβασης που υπολείπονται των τυπικών συστάσεων πολυπλοκότητας. Η δυνατότητα αυτή ενεργοποιείται μέσω της ταυτόχρονης πιστοποίησης ταυτότητας ίσων (Simultaneous Authentication of Equals - SAE). Η τεχνολογία είναι ανθεκτική στις επιθέσεις λεξικού χωρίς σύνδεση, όπου ένας αντίπαλος προσπαθεί να προσδιορίσει έναν κωδικό πρόσβασης δικτύου δοκιμάζοντας πιθανούς κωδικούς πρόσβασης χωρίς περαιτέρω αλληλεπίδραση με το δίκτυο.

- Φυσική επιλογή κωδικού πρόσβασης: Επιτρέπει στους χρήστες να επιλέγουν κωδικούς πρόσβασης που θυμούνται ευκολότερα
- Ευκολία χρήσης: Παρέχει ενισχυμένη προστασία χωρίς αλλαγή στον τρόπο σύνδεσης των χρηστών σε ένα δίκτυο
- Μυστικότητα προς τα εμπρός: Προστατεύει την κυκλοφορία δεδομένων ακόμη και αν ένας κωδικός πρόσβασης παραβιαστεί μετά τη μετάδοση των δεδομένων.

6.2.1.2 WPA3-Enterprise

Το WPA3-Enterprise βασίζεται στα θεμέλια του WPA2-Enterprise με την πρόσθετη απαίτηση χρήσης προστατευμένων πλαισίων διαχείρισης σε όλες τις συνδέσεις WPA3.

- Αυθεντικοποίηση: πολλαπλές μέθοδοι Extensible Authentication Protocol (EAP)

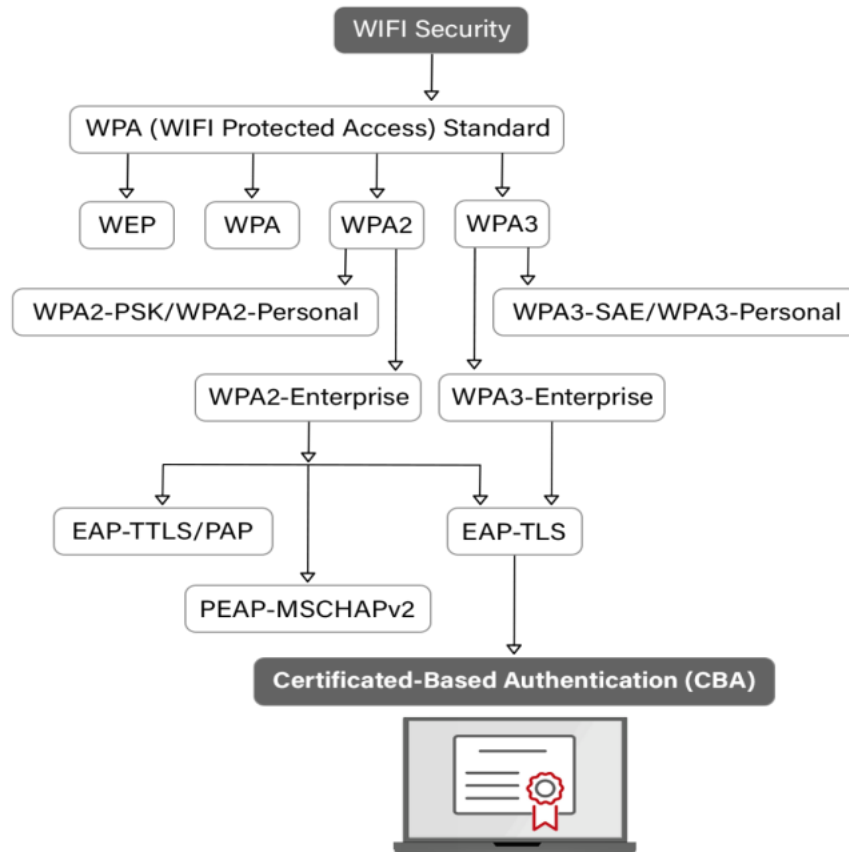
- Κρυπτογράφηση με έλεγχο ταυτότητας: τουλάχιστον 128-bit Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128).
- Παραγωγή και επιβεβαίωση κλειδιού: τουλάχιστον 256-bit Hashed Message Authentication Mode (HMAC) με Secure Hash Algorithm (HMAC-SHA256)
- Στιβαρή προστασία πλαισίου διαχείρισης: τουλάχιστον 128-bit Broadcast/Multicast Integrity Protocol Cipher-based Message Authentication Code (BIP-CMAC-128)

6.2.1.3 WPA3-Enterprise με λειτουργία 192-bit

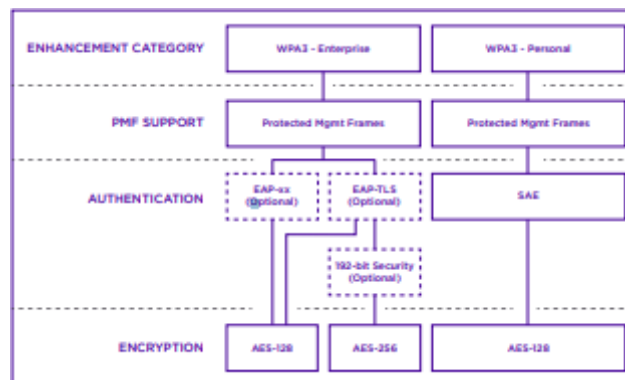
Το WPA3-Enterprise προσφέρει επίσης μια προαιρετική λειτουργία που χρησιμοποιεί πρωτόκολλα ασφαλείας ελάχιστης ισχύος 192 bit και κρυπτογραφικά εργαλεία για την καλύτερη προστασία ευαίσθητων δεδομένων.

- Αυθεντικοποίηση: ECDH (Elliptic Curve Diffie-Hellman) και αλγόριθμος ψηφιακής υπογραφής με ελλειπτική καμπύλη (ECDSA) με χρήση ελλειπτικής καμπύλης 384 bit.
- Αυθεντική κρυπτογράφηση: πρωτόκολλο Galois/Counter Mode 256-bit (GCMP-256).
- Παραγωγή και επιβεβαίωση κλειδιού: 384-bit Hashed Message Authentication Mode (HMAC) με αλγόριθμο ασφαλούς κατακερματισμού (HMAC-SHA384).
- Στιβαρή προστασία πλαισίου διαχείρισης: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256).

Η λειτουργία ασφαλείας 192 bit που προσφέρει το WPA3-Enterprise διασφαλίζει ότι χρησιμοποιείται ο σωστός συνδυασμός κρυπτογραφικών εργαλείων και θέτει μια συνεπή βασική γραμμή ασφαλείας σε ένα δίκτυο WPA3.



Εικόνα 18 wpa3 types



Εικόνα 19 wpa3 types [27]

6.2.2 Διάρφορες με WPA2

Ενώ το WPA2 επέφερε βελτιώσεις σε σχέση με τα προηγούμενα Wired Equivalent Privacy και WPA, το WPA3 είναι ακόμη πιο ασφαλές και ολοκληρωμένο. Σε σύγκριση με το πρότυπο WPA2, το WPA3 προσθέτει τα ακόλουθα αξιοσημείωτα χαρακτηριστικά:

- SAE protocol: Αυτό χρησιμοποιείται για τη δημιουργία μιας ασφαλούς χειραψίας, όπου μια συσκευή δικτύου συνδέεται σε ένα ασύρματο σημείο πρόσβασης και οι δύο

συσκευές επικοινωνούν για να επαληθεύσουν την αυθεντικοποίηση και τη σύνδεση. Ακόμη και αν ο κωδικός πρόσβασης ενός χρήστη είναι αδύναμος, το WPA3 με το dragonfly παρέχει μια ασφαλέστερη χειραψία από το WPA2 που μέσω του PSK μπορούσαμε να πάρουμε πολύτιμα στοιχεία που μπορούσαμε να κάνουμε επιθέσεις ωμής βίας (brute force).

- Εξατομικευμένη κρυπτογράφηση δεδομένων. Σε σύγκριση με το WPA2, το οποίο χρησιμοποιεί κοινόχρηστους κωδικούς πρόσβασης κατά τη σύνδεση σε ένα δημόσιο δίκτυο, το WPA3 εγγράφει μια νέα συσκευή χρησιμοποιώντας το Device Provisioning Protocol. Αυτό επιτρέπει στους χρήστες να επιτρέπουν την είσοδο συσκευών στο δίκτυο χρησιμοποιώντας ετικέτες επικοινωνίας κοντινού πεδίου ή κωδικούς QR (γρήγορης απόκρισης). Επιπλέον, η ασφάλεια WPA3 χρησιμοποιεί κρυπτογράφηση GCMP-256 αντί για κρυπτογράφηση 128 bit. Το Wpa2 χρησιμοποιούσε την λειτουργία WPS η οποία είχε πολλές ευπάθειες και οι κωδικοί του ήταν μικρού μεγέθους.
- Ισχυρότερη προστασία από επιθέσεις brute-force: Το WPA3 προστατεύει από την μαντεψιά του κωδικού πρόσβασης εκτός σύνδεσης, δίνοντας στους χρήστες μόνο μια προσπάθεια μαντεψιάς, κάνοντάς τους να αλληλεπιδρούν άμεσα με μια συσκευή Wi-Fi. Αυτό σημαίνει ότι ο χρήστης πρέπει να είναι φυσικά παρών κάθε φορά που θέλει να μαντέψει τον κωδικό πρόσβασης. Το WPA2 δεν διαθέτει ενσωματωμένη κρυπτογράφηση και προστασία της ιδιωτικής ζωής σε δημόσια ανοικτά δίκτυα, καθιστώντας τις επιθέσεις brute-force μια σημαντική απειλή.
- Μεγαλύτερα κλειδιά συνόδου: Το WPA3 υποστηρίζει μεγαλύτερα μεγέθη κλειδιών συνόδου, έως και ασφάλεια 192 bit σε περιπτώσεις εταιρικής χρήσης.
- Κρυπτογράφηση: Το WPA2 χρησιμοποιεί το Advanced Encryption Standard(AES) για κρυπτογράφηση, ενώ το WPA3 χρησιμοποιεί το πιο ασφαλές GCMP.

Features	WPA2	WPA3
Encryption	AES-CCMP	GCMP-256 / AES-CCMP
Authentication	PSK / 802.1x with EAP	SAE / 802.1x with EAP
Key Length	128-bit	192-bit
Protected Management Frames (PMF)	Optional	Mandatory
Attack resiliency <i>KRACK, Offline Dictionary</i>		✓

Εικόνα 20 Διαφορές wpa version 2 με 3[66]

6.2.3 SAE και Dragonfly handshake

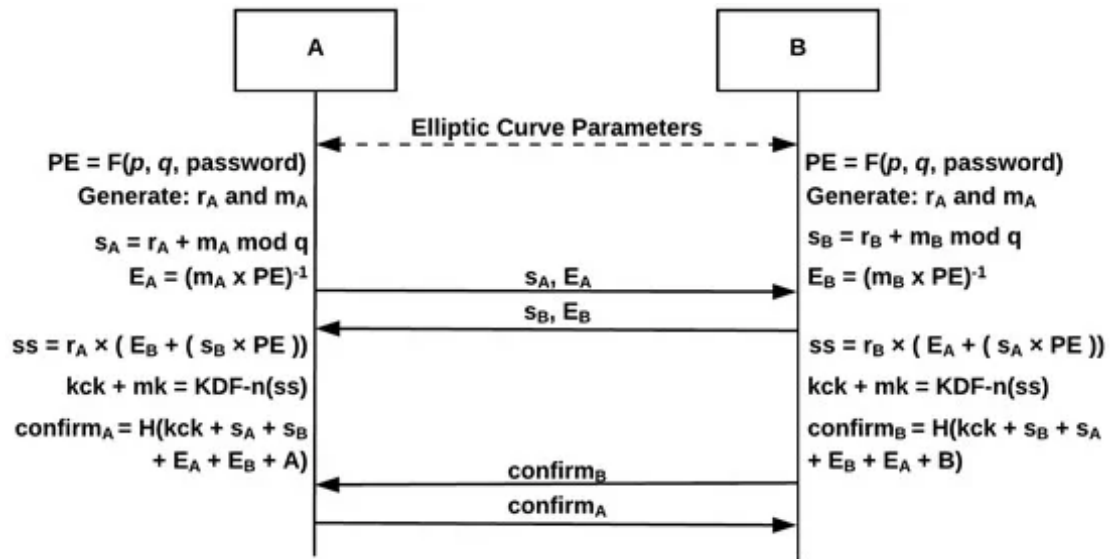
Το WPA3, που κυκλοφόρησε τον Ιούνιο του 2018, είναι το πιο πρόσφατο σχήμα ασφαλείας που έχει σχεδιαστεί για να ενισχύσει την ασφάλεια στα υπάρχοντα δίκτυα Wi-Fi και να λύσει τα προβλήματα που αντιμετώπιζαν οι προηγούμενες εκδόσεις. Το WPA3 χρησιμοποιεί την τεχνική Simultaneous Authentication of Equals (SAE) με βάση τον κωδικό πρόσβασης για την πιστοποίηση ταυτότητας του πελάτη στο AP. Το SAE ήταν ένα πρωτόκολλο που εισήχθη για πρώτη φορά για χρήση σε δίκτυα πλέγματος WLAN (IEEE 802.11s) από τον Dan Harkins το 2008, το οποίο αποδείχθηκε αργότερα ότι ήταν ευάλωτο σε παθητικές και ενεργές επιθέσεις, καθώς και σε off-line επιθέσεις λεξικού, από τις οποίες ισχυριζόταν ότι προστατεύει. Μετά την αναθεώρηση του προτύπου RFC 7764 το 2015, το βελτιωμένο πρωτόκολλο αποδείχθηκε ότι προσφέρει την προστασία που υποσχέθηκε. Η αντίσταση αυτή επιτυγχάνεται με τη χρήση χειραψίας dragonfly για την αξιοποίηση της κρυπτογραφίας διακριτών λογαριθμικών και ελλειπτικών καμπυλών. Το αποτέλεσμα της χειραψίας παράγει ένα PMK, το οποίο στη συνέχεια χρησιμοποιείται στην τυπική τετραπλή χειραψία που χρησιμοποιείται στο σύστημα WPA2.

Το πρωτόκολλο SAE χρησιμοποιεί τον κοινόχρηστο κωδικό πρόσβασης μόνο για τον έλεγχο ταυτότητας και όχι για την εξαγωγή του PMK. Στο πρωτόκολλο dragonfly, ένα στοιχείο κωδικού πρόσβασης PE χρησιμοποιείται αντί του κωδικού πρόσβασης για τον υπολογισμό των κλειδιών. Το PE προσδιορίζεται κατά τη στιγμή της συνόδου, χρησιμοποιώντας ένα συμφωνημένο σύνολο παραμέτρων ελλειπτικής καμπύλης p , που είναι ένας μεγάλος πρώτος αριθμός που χρησιμοποιείται για τον προσδιορισμό του πρώτου πεδίου για την ελλειπτική καμπύλη, και q , που είναι ένας άλλος μεγάλος πρώτος αριθμός στην τάξη μιας ομάδας G , που συμφωνείται από τον πελάτη και το AP με τη χρήση διακριτού λογαριθμικού υπολογισμού και μιας τεχνικής κυνηγιού-και-πίπας με τον κωδικό πρόσβασης ως τιμή εκκίνησης, που περιγράφεται στο. Ένα λεπτομερές διάγραμμα της χειραψίας dragonfly παρέχεται στο Σχήμα 8, όπου παρουσιάζεται μια ομότιμη επικοινωνία μεταξύ δύο μερών A και B. Αφού μοιραστούν οι παράμετροι της ελλειπτικής καμπύλης και το PE έχει προκύψει, τα δύο μέρη θα δημιουργήσουν στη συνέχεια ένα ιδιωτικό r και μια μάσκα m , τα οποία είναι τυχαία επιλεγμένοι μεγάλοι αριθμοί στο εύρος $\{1 \dots q\}$. Στη συνέχεια θα χρησιμοποιήσουν αυτές τις τιμές για να υπολογίσουν ένα κλιμάκιο s και, μαζί με το PE, υπολογίζουν ένα στοιχείο E χρησιμοποιώντας τις δεδομένες εξισώσεις (1) και (2):

$$sA = rA + mA \bmod q$$

(1)

$$E_A = (m_A \times PE)^{-1} \quad (2)$$



Εικόνα 21 wpa3 handshake [35]

Στη συνέχεια, και τα δύο μέρη αποστέλλουν αυτές τις δύο υπολογισμένες τιμές το ένα στο άλλο στα δύο πρώτα μηνύματα. Ο Α θα υπολογίσει στη συνέχεια το κοινόχρηστο μυστικό ss χρησιμοποιώντας τις πληροφορίες που έστειλε ο Β, έτσι ώστε:

$$ss = r_A \times (E_B + (s_B \times PE))$$

Αυτό μπορεί στη συνέχεια να απλοποιηθεί περαιτέρω με την ακύρωση των πράξεων.

$$ss = r_A \times ((m_B \times PE)^{-1} + ((r_B + m_B) \times PE))$$

$$ss = r_A \cdot ((m_B \times PE)^{-1} + (r_B \times PE) + (m_B \times PE))$$

$$ss = r_A \times r_B \times PE = r_B \times r_A \times PE$$

Το ss που υπολογίζεται θα χρησιμοποιηθεί στη συνέχεια για να προκύψει το κλειδί επιβεβαίωσης kck και το κύριο κλειδί mk . Το kck θα τεθεί σε μια συνάρτηση κατακερματισμού, θα συνδεθεί με το κλιμάκιο του αποστολέα, το κλιμάκιο του παραλήπτη, το στοιχείο του αποστολέα, το στοιχείο του παραλήπτη και την ταυτότητα (στην προκειμένη

περίπτωση τη διεύθυνση MAC) του αποστολέα για να επιβεβαιωθεί ότι ο αποστολέας έχει υπολογίσει το σωστό SS και επομένως γνωρίζει τον κωδικό πρόσβασης.

$$\text{confirmA} = H(kck + sA + sB + EA + EB + A)$$

Αυτό το μήνυμα επιβεβαίωσης θα υπολογιστεί και στις δύο πλευρές στα μηνύματα 3 και 4 με αντίστοιχες μεταβλητές για τον αποστολέα. Η σειρά της συνένωσης και η συμπερίληψη της αντίστοιχης ταυτότητας προσθέτει αυθεντικότητα στο μήνυμα για την αποφυγή αναπαραγωγής του μηνύματος του άλλου μέρους. Τέλος, mk θα χρησιμοποιηθεί ως PMK στην τετραπλής κατεύθυνσης χειραψία 802.11i που ακολουθεί.

Η ασφάλεια αυτού του πρωτοκόλλου έγκειται στη δυσχερή φύση της πράξης του γινομένου τελείας στον διακριτό λογαριθμικό υπολογισμό. Γνωρίζοντας το EA και PE, είναι υπολογιστικά δύσκολο να βρεθεί το mA. Με αυτόν τον τρόπο, ακόμη και αν ένας αντίπαλος παραβιάσει τον κωδικό πρόσβασης, δεν μπορεί να τον χρησιμοποιήσει για να εξάγει ο ίδιος το PMK και να αποκρυπτογραφήσει παρελθοντικά μηνύματα. Αυτό παρέχει ένα στοιχείο μυστικότητας προς τα εμπρός στο σύστημα. Δεδομένου ότι οι χρήστες πρέπει να αλληλεπιδρούν με το AP για να εξάγουν κάθε φορά το νέο PMK, οι επιτιθέμενοι μπορούν να προσπαθήσουν να αποκτήσουν τον κοινόχρηστο κωδικό πρόσβασης μόνο δοκιμάζοντας έναν κωδικό πρόσβασης κάθε φορά, λαμβάνοντας σωστό ή λανθασμένο, και στη συνέχεια δοκιμάζοντας ξανά. Αυτό το επίπεδο ισχύος της ασφάλειας επιτρέπει στο χρήστη να έχει έναν λιγότερο περίπλοκο κωδικό πρόσβασης για ευκολία στη χρήση .

6.2.4 handshake attack

Αυτή η συναρπαστική βελτίωση των προτύπων της Wi-Fi Alliance, ενώ παραμένει συμβατό με το WPA2, καθιστά πολλά προαιρετικά στοιχεία (όπως το Protected Management Frames) υποχρεωτικά. Συλλογικά, αυτά βοηθούν στην προστασία από την υποκλοπή και το man-in-the-middle και παρέχουν αντίσταση τόσο κατά των επιθέσεων εκτός σύνδεσης όσο και κατά των επιθέσεων επιθέσεις λεξικού και την ανάκτηση κλειδιών. Επειδή το WPA3 είναι ανθεκτικό στις επιθέσεις λεξικού χωρίς σύνδεση, οι χρήστες μπορούν να επιλέξουν (ή οι διαχειριστές μπορούν να ορίσουν) κωδικούς πρόσβασης που είναι απλούστεροι, ευκολότερα να θυμούνται και ευκολότερα να εισάγονται, διατηρώντας παράλληλα υψηλή ασφάλεια. Οπότε σε οποιαδήποτε offline επίθεση που χρειάζεται brute force το wpa3 είναι άτρωτο καθώς μειώνει τον κίνδυνο παραβίασης με τη δημιουργία ενός ξεχωριστού νέου PMK μεταξύ κάθε πελάτη

και AP γι' αυτό τόσο το 4-way handshake attack όσο και το pmkid attack δεν μπορούν να βρουν τρωτό σημείο καθώς έχουν μόνο μια προσπάθεια για να μαντέψουν τον κωδικό.

Το AP δεν διαθέτει στατικό PMK που προέρχεται από το PSK. Αντ' αυτού, το PMK προέρχεται από τη χειραψία dragonfly, η οποία απαιτεί αλληλεπίδραση με τον πελάτη. Επομένως, το PMKID δεν θα είναι διαθέσιμο μέχρι να γίνει έγκυρη εκτέλεση της χειραψίας dragonfly. Αυτό δεν είναι εφικτό, όπως φαίνεται στην απόδειξη της επίθεσης λεξικού σύλληψης χειραψίας. Επομένως, η εκτέλεση αυτής της off-line επίθεσης λεξικού είναι ανέφικτη.

Βιβλιογραφία

- [1] Wireless Penetration Testing: PMKID Attack (June 24, 2021) By Raj Chandel Retrieved from <https://www.hackingarticles.in/wireless-penetration-testing-pmkid-attack/>
- [2] 4-WAY HANDSHAKE (24th January 2019). Retrieved from <https://www.wifi-professionals.com/2019/01/4-way-handshake>
- [3] The 4-way handshake WPA/WPA2 encryption protocol By Alon Ronder Alon Ronder (Jan 16, 2020). Retrieved from <https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64>
- [4] Wi-Fi Security: WEP vs WPA or WPA2 Retrieved from <https://www.avast.com/c-wep-vs-wpa-or-wpa2>
- [5] WPA2 .Retrieved from <https://www.nfon.com/en/get-started/cloud-telephony/lexicon/knowledge-base-detail/wpa2>
- [6] Wireless security: WEP, WPA, WPA2 and WPA3 differences by Alissa Irei. Retrieved from <https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2>
- [7] Wi-Fi Protected Access (WPA) By Alexander S. Gillis . Retrieved from <https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access>
- [8] An Overview of Wireless Protected Access 2 (WPA2) By Bradley Mitchell Updated on (July 2, 2021). Retrieved from <https://www.lifewire.com/what-is-wpa2-818352>
- [9] Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode By John L. MacMichael. Retrieved from <https://dl.acm.org/doi/fullHtml/10.5555/1084783.1084785>
- [10] A Formal Analysis of IEEE 802.11's WPA2: Countering the Kracks Caused by Cracking the Counters Cas Cremers, Benjamin Kiesl, and Niklas Medinger, CISPA Helmholtz Center for Information Security. Retrieved from <https://www.usenix.org/system/files/sec20-cremers.pdf>
- [11] Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2) By Paul Arana. Retrieved from https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf
- [12] A Practical Attack on the Fixed RC4 in the WEP Mode By Itsik Mantin. Retrieved from <https://www.iacr.org/archive/asiacrypt2005/390/390.pdf>
- [13] What Is RC4, and why is it a vulnerability (Apr 2, 2021) By Borislav Kiprin. Retrieved from <https://crashtest-security.com/disable-ssl-rc4/>
- [14] What is RC4 Encryption? . Retrieved from <https://www.geeksforgeeks.org/what-is-rc4-encryption/>
- [15] Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys By Mathy Vanhoef and Frank Piessens, Katholieke Universiteit Leuven. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_vanhoef.pdf
- [16] WEP, WPA, WPA2 and WPA3: Differences and explanation. Retrieved from <https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa>

- [17] Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven, (2017) . Retrieved from <https://www.krackattacks.com/>
- [18] Wireless Security Protocols. Retrieved from <https://ipcisco.com/lesson/wireless-security-protocols/>
- [19] Wired Equivalent Privacy. Retrieved from https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
- [20] Wired Equivalent Privacy (WEP): Definition & Risks. Retrieved from <https://www.okta.com/identity-101/wep/>
- [21] WEP (Wired Equivalent Privacy) . Retrieved from <https://www.javatpoint.com/wep-wired-equivalent-privacy>
- [22] Wired Equivalent Privacy (WEP) . Retrieved from <https://www.tutorialspoint.com/wired-equivalent-privacy-wep>
- [23] WEP (Wired Equivalent Privacy) Avoid using this outdated security standard By Bradley Mitchell Updated on (September 11, 2020). Retrieved from <https://www.lifewire.com/definition-of-wired-equivalent-privacy-816575>
- [24] Difference between WEP and WPA. Retrieved from <https://www.geeksforgeeks.org/difference-between-wep-and-wpa/>
- [25] WEP, WPA, WPA2 and WPA3: Differences and explanation. Retrieved from <https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa>
- [26] New attack on WPA/WPA2 using PMKID. Retrieved from <https://hashcat.net/forum/thread-7717.html>
- [27] WPA3: The Next Generation of Wi-Fi Security. Retrieved from <https://relnet.hu/wp-content/uploads/2019/12/WPA3.pdf>
- [28] WPA3 Stronger Security for Your Network. Retrieved from <https://www.tp-link.com/gr/wpa3/>
- [29] How to Hack WiFi Passwords in 2022 (PMKID/Kr00k Attack) By Shaheer (January 2, 2022) . Retrieved from <https://www.secureyou.com/how-to-hack-wifi-password-pmkid-attack-method/>
- [30] Hacking WiFi without users using PMKID attack Updated on (May 20, 2021) by Kalitut. Retrieved from <https://kalitut.com/pmkid-attack/>
- [31] PMKID attack on WPA/WPA2 WiFi networks. Retrieved from <https://www.fortiguard.com/psirt/FG-IR-18-199>
- [32] Wi-Fi Hacking, Part 11: The PMKID Attack Updated: (Feb 17 2023). Retrieved from <https://www.hackers-arise.com/post/wi-fi-hacking-part-11-the-pmkid-attack>
- [33] How A Dragonfly Aims To Fix Delicate Wi-Fi's Wings. Retrieved from <https://medium.com/asecuritysite-when-bob-met-alice/how-a-dragonfly-aims-to-fix-delicate-wi-fis-wings-f26d82798010>

- [34] WPA 3 - Improvements over WPA 2 or broken again? Maximilian Appel, Dr.-Ing. Stephan Guenther. Retrieved from https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2020-11-1/NET-2020-11-1_02.pdf
- [35] A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3 by Christopher P. Kohlios , andThaier Hayajneh. Retrieved from <https://www.mdpi.com/2079-9292/7/11/284#B33-electronics-07-00284>
- [36] WPA3 Dragonfly Handshake. Retrieved from https://sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake#What_is_new_in_WPA3
- [37] Galois/Counter Mode. Retrieved from https://en.wikipedia.org/wiki/Galois/Counter_Mode
- [38] WPA3-Simultaneous Authentication of Equals(SAE) By Bhanu Prasad (Mar 6, 2021). Retrieved from <https://www.wirelessnetworksbies.com/post/wpa3-simultaneous-authentication-of-equals-sae>
- [39] Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd Publisher: IEEE. Retrieved from <https://ieeexplore.ieee.org/abstract/document/9152782>
- [40] what is wifi handshake and how to capture it in Kali Linux Last Updated on(May 24, 2021) by Walid Salame. Retrieved from <https://kalitut.com/capture-wifi-handshake/>
- [41] Cracking WPA2 Passwords Using the New PMKID Hashcat Attack BY KODY. Retrieved from <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-passwords-using-new-pmkid-hashcat-attack-0189379/>
- [42] PMKID attack. Retrieved from <https://amandinegh.gitbook.io/cyberadventure/wireless/attacking-wireless-network/pmkid-attack>
- [43] A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3 (October 2018) By Thaier Hayajneh ,Christopher Kohlios. Retrieved from https://www.researchgate.net/figure/CCMP-encryption-diagram_fig2_328632250
- [44] A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3 (October 2018) By Thaier Hayajneh ,Christopher Kohlios. Retrieved from https://www.researchgate.net/figure/Attacks-against-Wi-Fi-networks-are-listed-and-whether-or-not-WPA3-addresses-these_tbl1_328632250
- [45] DRAGONBLOOD Analysing WPA3's Dragonfly Handshake By Mathy Vanhoef (NYUAD) and Eyal Ronen (Tel Aviv University & KU Leuven) . Retrieved from <https://wpa3.mathyvanhoef.com/>
- [46] Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) Rahul Awati By Rahul Awati. Retrieved from <https://www.techtarget.com/searchsecurity/definition/CCMP-Counter-Mode-with-Cipher-Block-Chaining-Message-Authentication-Code-Protocol>
- [47] CCMP (cryptography) . Retrieved from [https://en.wikipedia.org/wiki/CCMP_\(cryptography\)](https://en.wikipedia.org/wiki/CCMP_(cryptography))
- [48] WPA2 CCMP: importance and security of the network-Standards (Jul 10, 2023) . Retrieved from <https://technical-tips.com/blog/internet/wpa2-ccmp-importance-and-security-27991>

- [49] Qué es WPA PSK TKIP CCMP – Información de seguridad WiFi (14 Dic 2014) Tarlogic Research. Retrieved from <https://www.acrylicwifi.com/blog/que-es-wpa-psk-tkip-ccmp/>
- [50] <https://learningnetwork.cisco.com/s/question/0D53i00000Ksnr2CAB/wep-wpa-wpa2-tkip-aes-ccmp-eap>
- [51] Understanding WiFi Security – WEP, WPA, WPA2, & WPA3. Retrieved from <https://study-ccna.com/wifi-security/>
- [52] Wi-Fi Protected Access. Retrieved from https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- [53] WEP vs. WPA vs. WPA2 vs. WPA3: Wi-Fi Security Types Explained. Retrieved from <https://www.makeuseof.com/tag/wep-wpa-wpa2-wpa3-explained/>
- [54] WPA2 vs. WPA3. Retrieved from https://www.diffen.com/difference/WPA2_vs_WPA3
- [55] AES-CCMP. Retrieved from <https://www.pcmag.com/encyclopedia/term/aes-ccmp>
- [56] Wireless security: IEEE 802.11 and CCMP/AES. Retrieved from <https://www.controleng.com/articles/wireless-security-ieee-802-11-and-ccmp-aes/>
- [57] https://www.arubanetworks.com/techdocs/ArubaOS_85_Web_Help/Content/arubaos-solutions/802-1x/wpa3-suppl.htm
- [58] What is CCMP? (March 5, 2022) by Information Security Asia. Retrieved from <https://informationsecurityasia.com/what-is-ccmp/>
- [59] CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) . Retrieved from [https://www.cybertraining365.com/cybertraining/Topics/CCMP_\(Counter_Mode_with_Cipher_Block_Chaining_Message_Authentication_Code_Protocol\)](https://www.cybertraining365.com/cybertraining/Topics/CCMP_(Counter_Mode_with_Cipher_Block_Chaining_Message_Authentication_Code_Protocol))
- [60] CCMP – Cipher Block Chaining. Retrieved from <https://vocal.com/secure-communication/ccmp/>
- [61] What is WPA3? . Retrieved from <https://idblender.com/support/wifi-protected-access-3>
- [62] WPA3: The Cutting-Edge of WiFi Security. Retrieved from <https://www.netspotapp.com/blog/wifi-security/what-is-wpa3.html>
- [63] Encrypted Data Communication: An Overview of the WEP Standard. Retrieved from <https://nullsec.us/wep-overview/>
- [64] Qué es Wifi WPA3? By Yendry Lopez Gomez. Retrieved from <https://lovtechnology.com/que-es-wifi-wpa3/>
- [65] Basic security measures for IEEE 802.11 wireless networks August 2008 By Oscar P. Sarmiento ,Fabio G. Guerrero , David Rey Argote. Retrieved from https://www.researchgate.net/figure/WPA-2-encryption-and-integrity-check_fig5_262458771
- [66] Seamless Next-generation Wi-Fi Security Through Multivendor End-to-end WPA3 Verification. Retrieved from <https://www.intel.com/content/dam/support/us/en/documents/wireless/intel-whitepaper-wifi-security-through-wpa3-verification.pdf>

