ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

EAP-TPM
Αυθεντικοποίηση Χρηστών σε Ασύρματα Δίκτυα Πρόσβασης

Αφροδίτη Η. Ιβανίδου

Επιβλέποντες: **Ευστάθιος Χατζηευθυμιάδης,** Καθηγητής
Ανέστης Παπακοτούλας, Υποψήφιος Διδάκτωρ

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2021

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

EAP-TPM
Αυθεντικοποίηση Χρηστών σε Ασύρματα Δίκτυα Πρόσβασης

Αφροδίτη Η. Ιβανίδου

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Ευστάθιος Χατζηευθυμιάδης,** Καθηγητής
Ανέστης Παπακοτούλας, Υποψήφιος Διδάκτωρ

Οκτώβριος 2021

ΠΕΡΙΛΗΨΗ

Στην σημερινή εποχή πληθώρα συσκευών είναι συνδεδεμένες σε ασύρματα δίκτυα τόσο ιδιωτικά όσο και δημόσια. Η αυθεντικοποίηση τους στο δίκτυο αποτελεί μία διαδικασία στην οποία θα πρέπει να επεμβαίνει ο χρήστης ώστε να εισάγει τα διαπιστευτήρια του. Σκοπός της παρούσας εργασίας είναι η παρουσίαση μιας εναλλακτικής μεθόδου αυθεντικοποίησης στα ασύρματα δίκτυα μέσω του Trusted Platform Module (TPM). Βασική ιδέα ήταν η δημιουργία ενός μηχανισμού αυθεντικοποίησης παρόμοιου με αυτόν των δικτύων τηλεφωνίας. Σε ένα τηλεφωνικό δίκτυο και κατ'επέκταση σε ένα 5G δίκτυο, η αυθεντικοποίηση των χρηστών γίνεται μέσω διαπιστευτηρίων που είναι αποθηκευμένα στην κάρτα SIM των συσκευών, χωρίς να απαιτείται ο χρήστης να παρέχει επιπλέον στοιχεία για να συνδεθεί στο δίκτυο. Το ίδιο λοιπόν θα μπορούσε να εφαρμοστεί και σε περιπτώσεις σύνδεσης χρηστών σε ένα WiFi δίκτυο μέσω της χρήσης του TPM, το οποίο βρίσκεται πλέον ενσωματωμένο στις περισσότερες φορητές συσκευές (laptops, κινητα) και μπορεί να δημιουργεί αλλά και να αποθηκεύει πιστοποιητικά ασφαλείας. Βασιζόμενοι σε προηγούμενες έρευνες για την υλοποίηση μιας παραλλαγής του πρωτοκόλλου EAP-TLS, που ονομάστηκε EAP-TPM, προσπαθήσαμε να μελετήσουμε την υλοποίηση αυτού τον τρόπο αυθεντικοποίησης. Δημιουργήσαμε λοιπόν ένα δοκιμαστικό περιβάλλον αποτελούμενο από ένα ασύρματο σημείο πρόσβασης, έναν FreeRADIUS server και έναν client, ο οποίος έχει ενσωματωμένο TPM, και μελετήσαμε τον τρόπο δημιουργίας πιστοποιητικών ασφαλείας, τα οποία θα αποθηκεύονται στο TPM. Στην συνέχεια μελετήσαμε την παραμετροποίηση του TPM για να μπορεί να υποστηρίξει αυθεντικοποίηση μέσω του πρωτοκόλλου EAP-TLS, ώστε ο client να μπορεί να αυθεντικοποιείται μέσω των αποθηκευμένων σε αυτό πιστοποιητικών. Τέλος, παρουσιάζονται η οικονομική αξία των ασύρματων δικτύων πρόσβασης, όπως προκύπτει από έρευνες, τα πλεονεκτήματα που απορρέουν από την χρήση τους, το κόστος εγκατάστασης τους αλλα και τα βασικότερα κριτήρια επιλογής αυτών των δικτύων.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Αυθεντικοποίηση χρηστών και ασφάλεια συστημάτων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: TPM, EAP-TLS, Πρωτόκολλα Αυθεντικοποίησης, Ασφάλεια, WiFi

ABSTRACT

Nowadays, many devices are connected to wireless networks, both private and public. Their authentication on the network is a process in which the user must intervene in order to enter his credentials. The purpose of this paper is to present an alternative authentication method for wireless networks through the Trusted Platform Module (TPM). The basic idea was to create an authentication mechanism similar to that of telephone networks. In a telephone network and consequently in a 5G network, user authentication is done through credentials stored on the SIM card of the devices, without requiring the user to provide additional information to connect to the network. The same could be applied in cases of users connecting to a wireless network through the use of TPM, which is now integrated in most mobile devices (laptops, mobile phones) and can create and store security certificates. Based on previous research to implement a variant of the EAP-TLS protocol, called EAP-TPM, we have tried to implement this authentication method. So we created a test environment consisting of a wireless access point, a FreeRADIUS server and a client, which has a built-in TPM, and we studied how to create security certificates, which will be stored in the TPM. Then we studied the TPM configuration to be able to support authentication via the EAP-TLS protocol, so that the client can authenticate via the certificates stored in it. Finally, the economic value of wireless access networks is presented, as shown by research, the advantages resulting from their use, their installation costs and the most basic selection criteria of these networks.

SUBJECT AREA: Users Authentication and System's Security

KEYWORDS: TPM, EAP-TLS, Authentication Protocols, Security, WiFi

ΕΥΧΑΡΙΣΤΙΕΣ

Αρχικά θα ήθελα να εκφράσω τις ευχαριστίες μου στους επιβλέποντες της διπλωματικής μου εργασίας, τον Καθηγητή του Τμήματος Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών Ευστάθιο Χατζηευθυμιάδη και τον Υποψήφιο Διδάκτορα Ανέστη Παπακοτούλα, οι οποίοι με καθοδήγησαν στην έρευνα του θέματος της εργασίας μου και ήταν πάντα δίπλα μου όταν χρειάστηκα την βοήθεια τους. Επιπλέον θα ήθελα να ευχαριστήσω τους γονείς μου και όλους όσους με υποστήριξαν καθ'όλο το διάστημα των σπουδών μου και της εκπόνησης της διπλωματικής μου εργασίας. Δίχως την στήριξη τους τίποτα από όλα αυτά δεν θα ήταν εφικτό.

Αφροδίτη Η. Ιβανίδου

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ 2

ABSTRACT 3

ΕΥΧΑΡΙΣΤΙΕΣ 4

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ 9

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ 10

1. ΕΙΣΑΓΩΓΗ 1

1.1 Κίνητρα και στόχοι 1

1.2 Research questions 2

1.3 Δομή της εργασίας 3

2. Η ΑΣΦΑΛΕΙΑ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ 5

2.1 Εισαγωγή 5

2.2 Η αρχιτεκτονική του προτύπου IEEE 802 5

2.3 Το πρότυπο 802.11 6

2.4 Επιθέσεις στα ασύρματα δίκτυα 7

2.5 802.1x Port-Based Authentication 9

3. ΠΡΩΤΟΚΟΛΛΑ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ 11

3.1 Αυθεντικοποίηση 11

3.2 Πρωτόκολλο EAP 12

3.2.1 Τα μηνύματα EAP 13

3.2.2 Διαχείριση κλειδιών 15

3.2.3 Μέθοδοι EAP 17

3.2.3.1 EAP-MD5 18

3.2.3.2 EAP-TLS 18

3.2.3.3 EAP-TTLS 19

3.2.3.4 LEAP 20

3.2.3.5 EAP-PEAP 20

3.2.3.6 EAP-POTP 20

3.3 Πρωτόκολλο RADIUS 22
3.3.1 Μηνύματα RADIUS 22
3.3.2 Αλληλεπίδραση πρωτοκόλλων RADIUS και EAP 23
3.3.3 Η ασφάλεια και η αξιόπιστη μεταφορά μηνυμάτων στο RADIUS 24
4. TRUSTED PLATFORM MODULE (TPM) 25
4.1 Η ιστορία του TPM 25
4.2 Τα χαρακτηριστικά του TPM 27
4.2.1 I/O Buffer 28
4.2.2 Υποσύστημα κρυπτογραφίας 29
4.2.3 Υποσύστημα εξουσιοδότησης 31
4.2.4 Random Access Memory (RAM) 31
4.2.5 Non-Volatile (NV) Memory 32
4.2.6 Power Detection 32
4.2.7 Execution Engine 32
4.3 TPM Services 33
4.3.1 Roots of Trust 33
4.3.2 Boot Process 33
4.3.3 Secure Storage 34
4.3.4 Attestation 35
5. RELATED WORK 36
5.1 EAP-TPM 36
5.1.1 Η αρχιτεκτονική του συστήματος 36
5.1.2 Υλοποίηση 37
5.1.3 Αυθεντικοποίηση 40
5.1.4 Δοκιμή σε Πραγματικό Περιβάλλον 43
5.2 EAP-TPM στην Ασφάλεια Ασύρματων Δικτύων Πόλεων 44
5.2.1 Απειλές 44
5.2.2 EAP-TLS with TPM Attestation Based Device and User Authentication 44
5.2.3 EAP-TLS with TPM Sealed Storage Based Device and User Authentication 45

5.3 Συμπεράσματα 46

6. FREERADIUS 48

6.1 Εισαγωγή 48

6.2 Εγκατάσταση FreeRADIUS 49

6.3 Γενική επισκόπηση λειτουργίας του FreeRADIUS server 52

6.3.1 Clients 52

6.3.2 Χρήστες 53

6.3.3 Αρχεία ρυθμίσεων 54

6.3.4 Βιβλιοθήκες και λεξικά 54

6.3.5 Ενότητα Listen 55

6.3.6 Αρχεία διαμόρφωσης 55

6.3.7 Αρχεία καταγραφής 61

6.3.8 Διαδικασία Αυθεντικοποίησης 61

7. ΥΛΟΠΟΙΗΣΗ 63

7.1 Αρχιτεκτονική 63

7.2 Παραμετροποίηση του FreeRADIUS 63

7.3 Secondary Freeradius 65

7.4 Δημιουργία Πιστοποιητικών 67

7.5 Mikrotik 70

7.6 UniFi Access Point 70

7.7 Προσθήκη ιδιωτικού κλειδιού & πιστοποιητικού CA στον supplicant 72

7.7.1 Windows 10 72

7.7.2 Android 74

7.8 Παραμετροποίηση του TPM 75

8. ΥΙΟΘΕΤΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ WIFI 79

8.1 Η οικονομική αξία του WiFi 79

8.1.1 Το WiFi σε Επιχειρηματικά Περιβάλλοντα 80

8.1.2 Μελλοντικές προβλέψεις 81

8.2 Πλεονεκτήματα ενός WiFi Δικτύου 81

8.3 Εγκατάσταση ενός WiFi Δικτύου 83

8.3.1 Κριτήρια Επιλογής 83

8.3.2 Κόστος Εγκατάστασης 85

9. ΣΥΜΠΕΡΑΣΜΑΤΑ 87

10. ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ 88

ΑΚΡΩΝΥΜΙΑ 90

ΒΙΒΛΙΟΓΡΑΦΙΑ 91

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Η αρχιτεκτονική του προτύπου IEEE 802.11 5
Εικόνα 2: MPDU Format 6
Εικόνα 3: Το μοντέλο αυθεντικοποίησης των τριών μερών με την χρήση ενός AAA Server 10
Εικόνα 4: Ανταλλαγή μηνυμάτων EAP 14
Εικόνα 5: Αυθεντικοποίηση EAP-XXX 17
Εικόνα 6: Το EAP-TLS στην αυθεντικοποίηση τριών μερών 18
Εικόνα 7: Ενσωμάτωση των μηνυμάτων EAP εντός των μηνυμάτων RADIUS 24
Εικόνα 8: Η Αρχιτεκτονική του TPM 28
Εικόνα 9: Η αρχιτεκτονική του προτεινόμενου συστήματος 37
Εικόνα 10: Αυθεντικοποίηση με διαμόρφωση 41
Εικόνα 11: Αυθεντικοποίηση με μηδενική διαμόρφωση 41
Εικόνα 12: Ο απαιτούμενος χρόνος για την δημιουργία ενός νέου πιστοποιητικού ταυτότητας 42
Εικόνα 13: Η διαδικασία δημιουργίας ενός νέου πιστοποιητικού 43
Εικόνα 14: Τοπολογία δικτύου δοκιμαστικού περιβάλλοντος 63
Εικόνα 15: UniFi AP - Καρτέλα Settings (1/4) 71
Εικόνα 16: UniFi AP - Καρτέλα Settings (2/4) 71
Εικόνα 17: UniFi AP - Καρτέλα Settings (3/4) 72
Εικόνα 18: UniFi AP - Καρτέλα Settings (4/4) 72
Εικόνα 19: Windows 10 - Καρτέλα Network and Sharing Center 73
Εικόνα 20: Windows 10 - Καρτέλα Set Up a Network 73
Εικόνα 21: Windows 10 - Καρτέλα Wireless Network Properties 74
Εικόνα 22: Το WiFi σε αριθμούς 79
Εικόνα 23: Η Οικονομική αξία του WiFi 81
Εικόνα 24: Επίδραση της ασύρματης πρόσβασης στην παραγωγικότητα των χρηστών 83
Εικόνα 25: Παράδειγμα ασύρματου δικτύου πρόσβασης 85

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1. Δομή της εργασίας 4
Πίνακας 2: Σύγκριση WiFi και Ethernet 82
Πίνακας 3: Σύγκριση κόστους εγκατάστασης WLAN και LAN 86

1. ΕΙΣΑΓΩΓΗ

Η παρούσα έρευνα έχει ως σκοπό την μελέτη της αυθεντικοποίησης χρηστών σε ασύρματα δίκτυα πρόσβασης με την χρήση του μηχανισμού TPM. Για την επικοινωνία χρήστη-εξυπηρετητή μελετάται η χρήση του πρωτοκόλλου EAP-TLS, τροποποιημένου ως προς τον τρόπο χρήσης των πιστοποιητικών μέσω του TPM. Στη συνέχεια παρουσιάζεται η ολοένα αυξανόμενη χρήση των ασύρματων δικτύων πρόσβασης, η οικονομική τους αξία, τα πλεονεκτήματα τους έναντι των παραδοσιακών ενσύρματων δικτύων και ο ρόλος που παίζει η επίτευξη ασφάλειας σε αυτά τα δίκτυα.

1.1 Κίνητρα και στόχοι

Η εκτεταμένη χρήση των ασύρματων δικτύων πρόσβασης τόσο από συσκευές χρηστών όσο και από συσκευές που χρησιμοποιούνται στα πλαίσια του IoT, έχει δημιουργήσει την ανάγκη για γρήγορους και αποτελεσματικούς τρόπους αυθεντικοποίησης. Μέχρι σήμερα η αυθεντικοποίηση γίνεται μέσω πρωτοκόλλων που απαιτούν την παρέμβαση των χρηστών και την εισαγωγή διαπιστευτηρίων.

Το 2007 προτάθηκε για πρώτη φορά σε μελέτες η χρήση ενός πρωτοκόλλου το οποίο βασίζεται στον τρόπο αυθεντικοποίησης του EAP-TLS και ονομάστηκε EAP-TPM. Η ιδέα για την χρήση αυτής της μεθόδου αυθεντικοποίησης προήλθε από την λειτουργία των δικτύων GSM, όπου ο χρήστης μέσω μιας κάρτας SIM αυθεντικοποιείται αυτόματα στο δίκτυο χωρίς να απαιτείται κάποια ρύθμιση από μέρους του. Ως μέσο υλοποίησης για την παραπάνω ιδέα χρησιμοποιήθηκε το TPM, το οποίο αποτελεί ένα είδος ενσωματωμένου διακριτικού υλικού που έχει την δυνατότητα να εκδίδει και να αποθηκεύει τα πιστοποιητικά του χρήστη ώστε να τον αυθεντικοποιεί αυτόματα σε ένα ασύρματο δίκτυο.

Η ιδέα αυτού του τρόπου αυθεντικοποίησης μπορεί να χρησιμοποιηθεί σε περιβάλλοντα όπου χρησιμοποιούνται ασύρματα δίκτυα πρόσβασης, όπως σε έξυπνες πόλεις, σε συσκευές IoT και σε επιχειρήσεις. Στην τελευταία περίπτωση προκύπτουν σημαντικά οικονομικά οφέλη καθώς η εγκατάσταση και η συντήρηση ενός ασύρματου δικτύου πρόσβασης έχει μικρότερο κόστος σε σχέση με τα ευρέως χρησιμοποιούμενα ενσύρματα δίκτυα. Πέραν ωστόσο των παραπάνω πλεονεκτημάτων, όπως θα δούμε και στα επόμενα κεφάλαια, προκύπτουν σημαντικά οφέλη και για τους χρήστες, οι οποίοι θα μπορούν να αυθεντικοποιούνται σε ένα δίκτυο χωρίς να χρειάζεται να εισάγουν κάθε φορά τα διαπιστευτήρια τους. Αυτό σε συνδυασμό με την ολοένα μεγαλύτερη υιοθέτηση των ασύρματων δικτύων δημιουργεί μία συνεχώς αυξανόμενη οικονομική αξία για τα δίκτυα αυτά.

Σκοπός της παρούσας εργασίας είναι να παρουσιαστούν τα πρωτόκολλα που χρησιμοποιούνται για την αυθεντικοποίηση σε ασύρματα δίκτυα πρόσβασης και εν συνεχεία να μελετηθεί ο συνδυασμός αυτών των πρωτοκόλλων και συγκεκριμένα του EAP-TLS, με τον μηχανισμό αυθεντικοποίησης TPM. Με γνώμονα την επίτευξη ασφάλειας στα ασύρματα δίκτυα παρουσιάζεται η οικονομική τους αξία και τα πλεονεκτήματα που προκύπτουν από την υιοθέτηση αυτών των δικτύων. Οι θεματικές ενότητες που παρουσιάζονται είναι οι εξής:

1. Ανάλυση της αρχιτεκτονικής του προτύπου 802.11.
2. Παρουσίαση των πρωτοκόλλων αυθεντικοποίησης στα ασύρματα δίκτυα πρόσβασης.
3. Ανάλυση της λειτουργίας του πρωτοκόλλου EAP-TLS.
4. Παρουσίαση της λειτουργίας του TPM.
5. Αναφορά σε υλοποιήσεις του προτεινόμενου πρωτοκόλλου EAP-TPM.
6. Μελέτη πρακτικής εφαρμογής του EAP-TPM.
7. Πλεονεκτήματα της προτεινόμενης μεθόδου.
8. Οικονομική αξία ασύρματων δικτύων πρόσβασης.
9. Πλεονεκτήματα ασύρματων δικτύων πρόσβασης.
10. Κριτήρια επιλογής και κόστος εγκατάστασης ασύρματων δικτύων πρόσβασης.

1.2 Research questions

Για να υλοποιηθεί ο στόχος που αναφέρεται παραπάνω χρειάστηκε να απαντηθούν ορισμένα ερευνητικά ερωτήματα, τα σημαντικότερα των οποίων αναγράφονται παρακάτω:

"Πως υλοποιείται η αυθεντικοποίηση χρηστών σε ένα ασύρματο δίκτυο;"

Στα ασύρματα δίκτυα πρόσβασης υπάρχουν διάφοροι τρόποι αυθεντικοποίησης. Το πρότυπο 802.11 αρχικά υποστήριζε μόνο αυθεντικοποίηση με ανοιχτό έλεγχο ταυτότητας και μέσω του πρωτοκόλλου WEP. Στη συνέχεια, με σκοπό την επίτευξη μεγαλύτερης ασφάλειας χρησιμοποιήθηκε το πρωτόκολλο EAP. Σε αυτό το πρωτόκολλο μπορούν να προστεθούν πολλαπλές μέθοδοι ελέγχου ταυτότητας, μία εκ των οποίων είναι και το TLS.

"Ποια είναι τα μειονεκτήματα των μεθόδων που ευρέως χρησιμοποιούνται σήμερα;"

Το ευρέως χρησιμοποιούμενο EAP-TLS αποτελεί ένα πρωτόκολλο αυθεντικοποίησης τριών μερών με την συμβολή ενός ενδιάμεσου authenticator. Η διαδικασία γίνεται μέσω ψηφιακών πιστοποιητικών. Ενώ η διαδικασία αυτή είναι διαχειρίσιμη από την πλευρά του server, τις περισσότερες φορές είναι περίπλοκη και δαπανηρή για τους χρήστες. Επιπλέον ένα ακόμα μειονέκτημα είναι ο κίνδυνος που υπάρχει να αποκαλυφθεί η ταυτότητα των χρηστών και για αυτό θα πρέπει να προβλεφθεί κατάλληλη υποδομή που θα αποδεικνύει τους ιδιοκτήτες των κλειδιών.

"Πως η χρήση ενός μηχανισμού όπως το TPM μπορεί να βελτιστοποιήσει τους υπάρχοντες τρόπους αυθεντικοποίησης;"

Η χρήση του TPM στην διαδικασία της αυθεντικοποίησης ξεπερνάει τα μειονεκτήματα των πιστοποιητικών από την μερια του χρήστη καθώς η διαδικασία περιλαμβάνει την αυτοματοποιημένη παραγωγή και διανομή των πιστοποιητικών και έναν ασφαλή και αξιόπιστο τρόπο αποθήκευσης του ιδιωτικού κλειδιού, που βασίζεται σε εξαρτήματα υλικού.

"Πως διασφαλίζονται τα διαπιστευτήρια του χρήστη με την χρήση του TPM;"

Όπως θα δούμε και στο κεφάλαιο 4 η ιδέα πίσω από το TPM βασίζεται στη μετακίνηση της ασφάλειας στο υλικό. Σε αντίθεση με τα υπάρχοντα συστήματα ασφαλείας το TPM ταυτοποιεί μοναδικά το υλικό και δεν επιτρέπει σε ευαίσθητα δεδομένα να φύγουν από αυτό. Ακόμα κι αν κάποιος κατάφερε να αποκτήσει απεριόριστη πρόσβαση στον υπολογιστή, δεν θα είχε πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο TPM.

"Για ποιό λόγο είναι προτιμότερη η χρήση του TPM έναντι του λογισμικού OpenSSL για την παραγωγή κλειδιών κατά την διαδικασία αυθεντικοποίησης;"

Η διαφορά του TPM έναντι του λογισμικού OpenSSL δεν φορά τόσο την ασφάλεια της δημιουργίας κλειδιών, όσο την ασφάλεια της αποθήκευσης κλειδιών. Το TPM είναι σχεδιασμένο έτσι ώστε το κλειδί να δημιουργείται μέσα σε αυτό και ως εκ τούτου δεν μπορεί να αντιγραφεί σε κάποιο άλλο μέσο. Αντιθέτως στην περίπτωση της χρήσης λογισμικού το κλειδί δημιουργείται σε ένα απλό αρχείο το οποίο μπορεί εύκολα να αντιγραφεί.

"Είναι προτιμότερη η εγκατάσταση ενός ασύρματου ή ενός ενσύρματου δικτύου;"

Ο τύπος του δικτύου που θα χρησιμοποιήσει ένας οργανισμός εξαρτάται από πολλούς παράγοντες μερικοί εκ των οποίων είναι το κόστος εγκατάστασης και η παρεχόμενη ασφάλεια. Τα ασύρματα δίκτυα πρόσβασης φαίνεται να κερδίζουν όλο και περισσότερο έδαφος σε επιχειρήσεις και δημόσιους οργανισμούς.

1.3 Δομή της εργασίας

Στον παρακάτω πίνακα παρουσιάζεται μία σύνοψη της δομής της εργασίας, η οποία ξεκινάει με μία σύντομη εισαγωγή στα χαρακτηριστικά των ασύρματων δικτύων πρόσβασης και των προτύπων που έχουν δημιουργηθεί πάνω σε αυτά. Στη συνέχεια παρουσιάζονται τα πρωτόκολλα αυθεντικοποίησης που χρησιμοποιούνται στα εν λόγω δίκτυα.

Στο κύριο μέρος της εργασίας παρουσιάζονται τα χαρακτηριστικά του TPM και τα πλεονεκτήματα από την χρήση του κατά την αυθεντικοποίηση με το πρωτόκολλο EAP-TLS. Την θέση αυτή έρχονται να υποστηρίξουν υλοποιήσεις του προτεινόμενου τρόπου αυθεντικοποίησης στα πλαίσια παλαιότερων ερευνών.

Εν συνεχεία παρουσιάζεται η πρακτική υλοποίηση του πρωτοκόλλου EAP-TLS σε δοκιμαστικό περιβάλλον καθώς και ο κώδικας παραμετροποίησης του TPM. Προκειμένου να γίνουν αντιληπτά όσα παρουσιάζονται στα κεφάλαια 6-7 θα πρέπει να γίνουν κατανοητές οι έννοιες των κεφαλαίων 2-3-4.

Πίνακας 1: Δομή της εργασίας

Κεφάλαια	Υποενότητες	Περίληψη
1.Εισαγωγή	1.1 Κίνητρα και στόχοι 1.2 Ερευνητικά ερωτήματα	Εισαγωγή στην εργασία, παράθεση κινήτρων και στόχων και ανάλυση της δομής της.
2.Η ασφάλεια στα ασύρματα δίκτυα	2.1 Εισαγωγή 2.2 Η αρχιτεκτονική του προτύπου IEEE 802 2.3 Το πρότυπο 802.11 2.4 Επιθέσεις στα ασύρματα δίκτυα 2.5 802.1x Port-Based Authentication	Εισαγωγή στα ασύρματα δίκτυα πρόσβασης και παρουσία του προτύπου 802.11.
3.Πρωτόκολλα αυθεντικοποίησης	3.1 Αυθεντικοποίηση 3.2 Πρωτόκολλο EAP 3.3 Πρωτόκολλο RADIUS	Τρόποι αυθεντικοποίησης στα ασύρματα δίκτυα και αναλυτική παρουσίαση των πρωτοκόλλου EAP και RADIUS.
4.Trusted Platform Module (TPM)	4.1 Η ιστορία του TPM 4.2 Τα χαρακτηριστικά του TPM 4.3 TPM Services	Παρουσίαση των χαρακτηριστικών και των λειτουργιών του TPM.
5.Related Work	5.1 EAP-TPM 5.2 EAP-TPM στην Ασφάλεια Ασύρματων Δικτύων Πόλεων 5.3 Συμπεράσματα	Παρουσίαση προηγούμενων ερευνών πάνω στην υλοποίηση του πρωτοκόλλου EAP-TPM και συμπεράσματα επί αυτών.
6. FreeRADIUS	6.1 Εισαγωγή 6.2 Εγκατάσταση FreeRADIUS 6.3 Γενική επισκόπηση λειτουργίας του FreeRADIUS server	Τρόπος εγκατάστασης ενός FreeRADIUS Server και γενική επισκόπηση της λειτουργίας του.
7. Υλοποίηση	7.1 Αρχιτεκτονική 7.2 Παραμετροποίηση του FreeRADIUS 7.3 Secondary Freeradius 7.4 Δημιουργία Πιστοποιητικών 7.5 Mikrotik 7.6 UniFi Access Point 7.7 Προσθήκη ιδιωτικού κλειδιού & πιστοποιητικού CA στον supplicant 7.8 Παραμετροποίηση του TPM	Πρακτική υλοποίηση του πρωτοκόλλου EAP-TLS και περιγραφή παραμετροποίησης του TPM ώστε να συμμετέχει στην διαδικασία της αυθεντικοποίησης.
8.Υιοθέτηση ενός Wifi Δικτύου	8.1 Η οικονομική αξία του WiFi 8.2 Πλεονεκτήματα ενός WiFi Δικτύου 8.3 Εγκατάσταση ενός WiFi Δικτύου	Παρουσίαση της οικονομικής αξίας των ασύρματων δικτύων, των πλεονεκτημάτων τους και του κόστους εγκατάστασης τους.
9.Συμπεράσματα	Συμπεράσματα και μελλοντικές επεκτάσεις	Συμπεράσματα και μελλοντικές επεκτάσεις

2. Η ΑΣΦΑΛΕΙΑ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

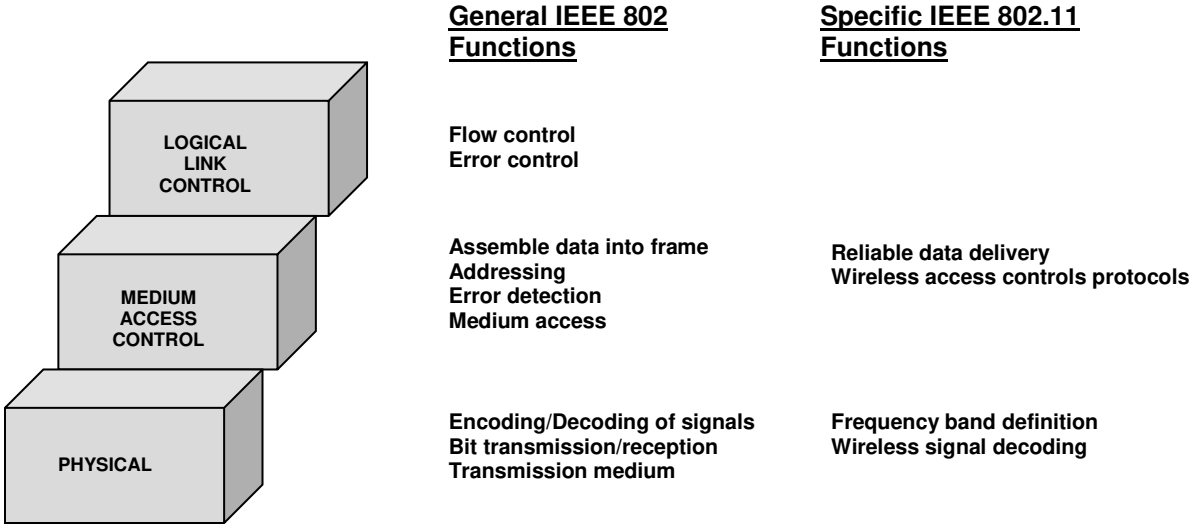
Σε αυτό το κεφάλαιο παρουσιάζονται συνοπτικά τα πρότυπα ασφάλειας στα ασύρματα δίκτυα, η αρχιτεκτονική τους και οι πιο διαδεδομένες επιθέσεις που λαμβάνουν χώρα σε αυτά.

2.1 Εισαγωγή

Η ραγδαία τεχνολογική ανάπτυξη και η πληθώρα φορητών συσκευών που χρησιμοποιούμε σε κάθε πτυχή της καθημερινότητας μας έχουν συμβάλει στην ταχύτατη ανάπτυξη των ασύρματων δικτύων επικοινωνιών. Η ασύρματη πρόσβαση χρησιμοποιείται εκτενώς τόσο στην προσωπική μας ζωή όσο και στο εργασιακό μας περιβάλλον. Κύριο χαρακτηριστικό των ασύρματων δικτύων είναι η κινητικότητα που προσφέρουν στους χρήστες τους, οι οποίοι μπορούν να έχουν πρόσβαση από οποιοδήποτε σημείο με οποιαδήποτε φορητή συσκευή χωρίς περιορισμούς. Ένα ακόμα κριτήριο επιλογής αυτών των δικτύων είναι αφενός το χαμηλό κόστος εγκατάστασης τους, καθώς απαιτούν λιγότερο εξοπλισμό και αφετέρου η δυνατότητα χρήσης τους απο μεγάλο αριθμό χρηστών χωρίς τον περιορισμό των καλωδίων.

Με σκοπό τη δημιουργία ενός πρωτοκόλλου που θα διέπει την μετάδοση δεδομένων στα ασύρματα δίκτυα η επιτροπή IEEE συγκρότησε μία νέα ομάδα εργασίας την IEEE 802.11. Το πρότυπο 802.11 είναι μέλος της οικογένειας προτύπων 802, τα οποία αποτελούν μια σειρά προδιαγραφών για τοπικά δίκτυα (LAN-Local Area Networks). Τα ανωτέρω πρότυπα επικεντρώνονται στα δύο χαμηλότερα επίπεδα του OSI, το φυσικό επίπεδο και το επίπεδο ζεύξης δεδομένων. Όλα τα 802 δίκτυα έχουν ένα φυσικό κομμάτι (physical layer) και ένα κομμάτι ελέγχου πρόσβασης στο μέσο μετάδοσης (medium access control) [1].

2.2 Η αρχιτεκτονική του προτύπου IEEE 802

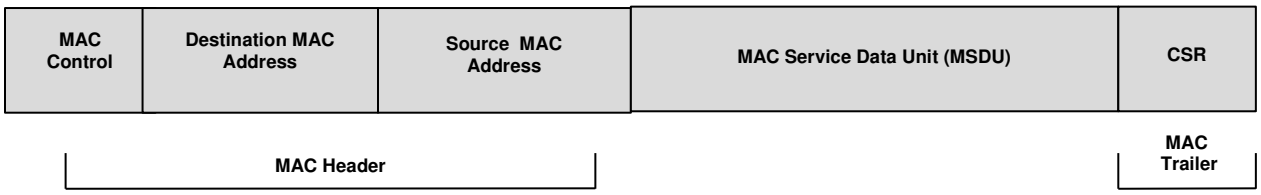


Εικόνα 1: Η αρχιτεκτονική του προτύπου IEEE 802.11

Το φυσικό κομμάτι αποτελεί το χαμηλότερο κομμάτι του πρωτοκόλλου IEEE 802 και συμπεριλαμβάνει λειτουργίες όπως η κωδικοποίηση και αποκωδικοποίηση των σημάτων και η μεταφορά και υποδοχή των bits. Επιπλέον στο φυσικό επίπεδο περιλαμβάνεται ο προσδιορισμός του μέσου μεταφοράς. Στην περίπτωση του πρωτοκόλλου IEEE 802.11 στο φυσικό επίπεδο καθορίζονται και οι ζώνες συχνοτήτων και τα χαρακτηριστικά των κεραιών.

Στα τοπικά δίκτυα ένας συνδυασμος συσκευών μοιράζονται τη χωρητικότητα του δικτύου και ως εκ τούτου χρειάζεται ένας μηχανισμός στο μέσο μεταφοράς που θα ελέγχει την αποδοτική χρήση της χωρητικότητας του. Αυτή τη λειτουργία την αναλαμβάνει το επίπεδο ελέγχου πρόσβασης στο μέσο, το οποίο λαμβάνει δεδομένα από ένα πρωτόκολλο υψηλότερου επιπέδου, του επιπέδου ελέγχου λογικής ζεύξης (logical link control). Τα δεδομένα που λαμβάνει είναι της μορφής ενός συνόλου δεδομένων που ονομάζεται MAC service data unit (MSDU). Σε γενικές γραμμές οι λειτουργίες που αναλαμβάνει το επίπεδο ελέγχου πρόσβασης στο μέσο είναι οι εξής [2]:

- Κατά την μετάδοση συνθέτει ένα πακέτο δεδομένων που ονομάζεται MAC protocol data unit (MPDU) και περιλαμβάνει πεδία διευθύνσεων και αναγνώρισης λαθών.
- Κατά την λήψη των δεδομένων αποσυνθέτει το πακέτο και πραγματοποιεί αναγνώριση των διευθύνσεων και ανίχνευση λαθών.
- Τέλος διαχειρίζεται την πρόσβαση στο μέσο μετάδοσης του τοπικού δικτύου.



Εικόνα 2: MPDU Format

Στα περισσότερα πρωτόκολλα ελέγχου ζεύξης δεδομένων, το πρωτόκολλο είναι υπεύθυνο όχι μόνο για την ανίχνευση λαθών αλλά και για την επίλυση τους μεταφέροντας ξανά τα κατεστραμμένα πακέτα. Στην αρχιτεκτονική του πρωτοκόλλου LAN, αυτές οι δύο λειτουργίες χωρίζονται μεταξύ των επιπέδων MAC και LLC. Το επίπεδο MAC είναι υπεύθυνο για την ανίχνευση λαθών και την απόρριψη των πλαισίων που τα περιέχουν. Το επίπεδο LLC καταγράφει ποια πλαίσια έχουν ληφθεί επιτυχώς και στέλνει εκ νέου αυτά των οποίων η λήψη έχει αποτύχει.

2.3 Το πρότυπο 802.11

Όπως αναφέρθηκε και προηγουμένως το πρωτόκολλο 802.11 αναφέρεται στο επίπεδο της ζεύξης δεδομένων. Το 802.11 περιλαμβάνει και αυτό το επίπεδο MAC και δύο φυσικά επίπεδα: το frequency-hopping spread-spectrum (FHSS) που αναφέρεται στο φυσικό

επίπεδο και το direct-sequence spread-spectrum (DSSS) που αναφέρεται στο επίπεδο ζεύξης δεδομένων. Στις επόμενες εκδόσεις του πρωτοκόλλου έχουν προστεθεί και πρόσθετα φυσικά επίπεδα. Η χρήση των ραδιοκυμμάτων ως μέσο μετάδοσης απαιτεί ένα σύνθετο φυσικό επίπεδο. Στο 802.11 το φυσικό επίπεδο αποτελείται από δύο μέρη: το ένα ονομάζεται Physical Layer Convergence Procedure (PLCP) και χαρτογραφεί τα MAC πακέτα μέσα στο μέσο και το άλλο Physical Medium Dependent (PMD) system και μεταφέρει αυτά τα πακέτα. Το PLCP προσθέτει έναν αριθμό πεδίων στο πλαίσιο καθώς αυτό μεταδίδεται στο μέσο μετάδοσης, δηλαδή τον αέρα.

Τα ασύρματα δίκτυα του προτύπου 802.11 αποτελούνται από 4 βασικά φυσικά μέρη [1]:

- **Σύστημα διανομής (Distribution system)**
  Όταν πολλά σημεία πρόσβασης διασυνδέονται για να δημιουργήσουν μία μεγάλη περιοχή κάλυψης, θα πρέπει να επικοινωνούν μεταξύ τους για να καταγράφονται οι κινήσεις των κινητών σταθμών. Το συστημα διανομής είναι ένα φυσικό μέρος του δικτύου το οποίο χρησιμοποιείται για την αποστολή των πακέτων στον προορισμό τους. Στο πρότυπο 802.11 δεν προσδιορίζεται συγκεκριμένη τεχνολογία για το σύστημα διανομής. Στα περισσότερα εμπορικά προϊόντα, το σύστημα διανομης είναι ένας συνδυασμός από ένα μηχάνημα γεφύρωσης και ένα μέσο επικοινωνίας, το οποίο χρησιμοποιείται για την αναμετάδοση των πακέτων μεταξύ των σημείων πρόσβασης. Το συγκεκριμένο κομμάτι του δικτύου ονομάζεται δίκτυο κορμού και τις περισσότερες φορές χρησιμοποιείται σε αυτό η τεχνολογία Ethernet.

- **Σημεία πρόσβασης (Access points)**
  Τα πακέτα στο ασύρματο δίκτυο πρέπει να μετατρέπονται σε ένα άλλο είδος πακέτου για να μεταφερθούν στον υπόλοιπο κόσμο. Οι συσκευές που ονομάζονται σημεία πρόσβασης μετατρέπουν το ραδιοκύμματα σε κατάλληλη μορφή ώστε να μεταφερθούν στο ενσύρματο μέσο επικοινωνίας.

- **Ασύρματο μέσο επικοινωνίας (Wireless medium)**
  Για να μεταφερθούν τα πακέτα από σταθμό σε σταθμό χρησιμοποιείται ένα ασύρματο μέσο επικοινωνίας. Η αρχιτεκτονική επιτρέπει πολλά φυσικά επίπεδα να αναπτυχθούν για να υποστηρίξουν το επίπεδο MAC. Αρχικά προτυποποιήθηκαν δύο επίπεδα ραδιοσυχνοτήτων και ένα υπερύθρων, ωστόσο τα στρώματα ραδιοσυχνοτήτων θεωρούνται πιο δημοφιλή.

- **Σταθμοί (Stations)**
  Τα δίκτυα έχουν σχεδιαστεί για να μεταφέρουν δεδομένα μεταξύ των σταθμών. Οι σταθμοί είναι συσκευές που διαθέτουν δυνατότητα ασύρματης λειτουργίας.

2.4 Επιθέσεις στα ασύρματα δίκτυα

Σε ένα ενσύρματο δίκτυο το μέσο διασύνδεσης είναι το καλώδιο. Προκειμένου να συνδεθεί λοιπόν κάποιος χρήστης σε ένα τοπικό δίκτυο και να μεταδώσει πληροφορίες θα πρέπει

να υπάρχει φυσική σύνδεση. Σε αυτή την περίπτωση παρεμβάλλεται μια διαδικασία αυθεντικοποίησης των χρηστών. Απο την άλλη μεριά, στα ασύρματα δίκτυα μπορεί να συνδεθεί οποιοσδήποτε διαθέτει μια ασύρματη συσκευή και να μεταδώσει πληροφορίες στο δίκτυο. Παρομοίως και από τη μεριά του λήπτη των πληροφοριών σε ένα ενσύρματο δίκτυο θα πρέπει να υπάρχει συσκευή που να είναι φυσικά συνδεδεμένη στο δίκτυο, εξασφαλίζοντας με αυτό τον τρόπο την ιδιωτικότητα. Στην περίπτωση του ασύρματου δικτύου μπορεί οποιαδήποτε συσκευή να λειτουργήσει ως λήπτης. Τα μέρη λοιπόν ενός ασύρματου δικτύου είναι δυνατόν να αποτελέσουν στόχους επιθέσεων. Αυτό έχει ως αποτέλεσμα να καταστρατηγούνται ένας ή περισσότεροι στόχοι της ασφάλειας, που είναι η εμπιστευτικότητα η ακεραιότητα και η διαθεσιμότητα. Για αυτό το λόγο στα ασύρματα δίκτυα υπάρχει η ανάγκη για εύρεση αποδοτικών μηχανισμών ασφάλειας.

Μερικές από τις επιθέσεις που συχνά συναντώνται στα ασύρματα δίκτυα είναι οι εξής [2]:

- **Accidental association**
  Αυτή η επίθεση αναφέρεται σε περιπτώσεις όπου δημιουργούνται επικαλυπτόμενες περιοχές διάδοσης. Σε αυτή την περίπτωση είναι δυνατόν ένας χρήστης που επιθυμεί να συνδεθεί σε ένα τοπικό δίκτυο να συνδεθεί ακούσια σε ένα σημείο ασύρματης πρόσβασης ενός γειτονικού δικτύου. Αν και η συγκεκριμένη παραβίαση ασφαλείας είναι τυχαία, παρ 'όλα μπορεί να εκθέσει τους πόρους ενός τοπικού δικτύου σε ένα τυχαίο χρήστη.

- **Malicious association**
  Σε αυτήν την περίπτωση, μία ασύρματη συσκευή προσπαθεί να προσποιηθεί ένα νόμιμο σημείο πρόσβασης, επιτρέποντας στον επιτιθέμενο να υποκλέπτει στοιχεία από τους νόμιμους χρήστες και στη συνέχεια να διεισδύει στο δίκτυο μέσω ενός νόμιμου σημείου ασύρματης πρόσβασης.

- **Ad hoc networks**
  Αυτή η περίπτωση αναφέρεται σε peer-to-peer, δηλαδή δίκτυα μεταξύ ασύρματων τερματικών συσκευών χωρίς να παρεμβάλλεται κάποιο σημείο πρόσβασης μεταξύ τους. Τα δίκτυα αυτά μπορούν να αποτελέσουν απειλή λόγω έλλειψης κεντρικού σημείου ελέγχου.

- **Identity theft (MAC spoofing)**
  Σε αυτή την περίπτωση ο επιτιθέμενος ακούει την κίνηση του δικτύου και καταφέρνει κλέβοντας την mac-address μιας συσκευής του δικτύου να προσποιηθεί ότι είναι εξουσιοδοτημένος χρήστης.

- **Man-in-the middle attacks**
  Τα ασύρματα δίκτυα είναι ιδιαίτερα ευάλωτα σε αυτό τον τύπο επιθέσεων. Στη συγκεκριμένη επίθεση ο κακόβουλος χρήστης παρεμβάλλεται μεταξύ της τερματικής ασύρματης συσκευής και του ασύρματου σημείου πρόσβασης καταφέρνοντας όλη η επικοινωνία να περάσει μέσα από τη δική του συσκευή.

- **Denial of service (DoS)**
  Μία επίθεση DoS συμβαίνει όταν ένας εισβολέας στέλνει συνεχώς ένα σημείο ασύρματης πρόσβασης ή κάποια άλλη προσβάσιμη ασύρματη συσκευή μηνύματα σχεδιασμένα να καταναλώνουν πόρους συστήματος. Με αυτό τον τρόπο το σύστημα καταρρέει και δεν μπορεί να διεκπεραιώσει αιτήματα νόμιμων χρηστών.

Οι επιθέσεις στα ασύρματα δίκτυα μπορούν να κατηγοριοποιηθούν ανάλογα με το μέρος του δικτύου στο οποίο στοχεύουν κάθε φορά, δηλαδή σε επιθέσεις στο κανάλι επικοινωνίας, σε επιθέσεις στα ασύρματα σημεία πρόσβασης και τέλος σε επιθέσεις σε τερματικές και δικτυακές συσκευές. Στην παρούσα εργασία θα αναλυθούν τρόποι προστασίας από μη εξουσιοδοτημένη πρόσβαση στα ασύρματα σημεία πρόσβασης ενός δικτύου.

2.5 802.1x Port-Based Authentication

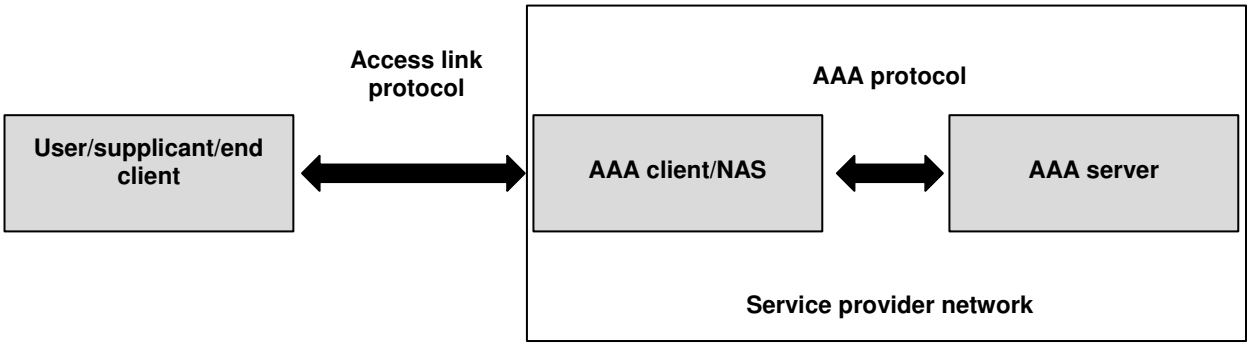
Σήμερα λοιπόν που η ασφάλεια των ασύρματων δικτύων αποτελεί μία πολύπλοκη διαδικασία, η είσοδος σε ένα ασύρματο τοπικό δίκτυο χρηστών που βρίσκονται έξω από το τείχος προστασίας (firewall) ενέχει πολλούς κινδύνους ασφαλείας. Τις περισσότερες φορές χρησιμοποιείται η τεχνολογία VPN (Virtual Private Network). Το VPN είναι μία κρυπτογραφημένη σύνδεση στο εσωτερικό δίκτυο, που εκτελείται μέσω ενός δημοσίου δικτύου. Προκειμένου να εφαρμοστεί αυτή η τεχνολογία απαιτείται εγκατάσταση συγκεκριμένου λογισμικού στην πλευρά του χρήστη και η ύπαρξη ενός VPN Server μέσα στο δίκτυο. Το VPN λειτουργεί στο επίπεδο 3 του μοντέλου OSI, κάτι που σημαίνει πως ο χρήσης προκειμένου να περάσει στο στάδιο της αυθεντικοποίησης χρειάζεται διεύθυνση IP και σύνδεση σε επίπεδο IP με το δίκτυο. Από την άλλη πλευρά το πρότυπο 802.1x καθορίζει ένα μηχανισμό port-based πρόσβασης στο δίκτυο. Σε ένα δίκτυο που χρησιμοποιεί τον μηχανισμό αυθεντικοποίησης 802.1x μπορεί να ξεκινήσει η διαδικασία ελέγχου ταυτότητας χωρίς να έχει προηγουμένως δημιουργηθεί σύνδεση IP.

Ένα από τα πλεονεκτήματα λοιπόν ενός συστήματος αυθεντικοποίησης 802.1x είναι ότι η πληροφορία για το ασύρματο δίκτυο δεν χρειάζεται να παρέχεται έξω από το firewall. Αυτό συμβαίνει επειδή τα σημεία πρόσβασης δεν ανταλλάσουν άλλα πακέτα πέρα από αυτά που αφορούν τη διαδικασία αυθεντικοποίησης. Με αυτό τον τρόπο ακόμα και εάν ένας επιτιθέμενος υποκλέψει την κίνηση του ασύρματου δικτύου δεν θα μπορεί να αποκτήσει διεύθυνση IP και να αποκτήσει πρόσβαση στο ενσύρματο δίκτυο. Βεβαία υπάρχουν πολλές προϋποθέσεις που θα πρέπει να συντρέχουν σε αυτή την περίπτωση, ώστε να επιτευχθεί η προσδοκώμενη ασφάλεια, οι οποίες θα αναλυθούν παρακάτω.

Στην περίπτωση της port-based αυθεντικοποίησης ο όρος “port” (θύρα) αναφέρεται στο επίπεδο 2 του μοντέλου OSI. Σε ένα ενσύρματο δίκτυο με τον όρο θύρα εννοούμε τις θύρες ενός EthernetSwitch. Οι συσκευές συνδέονται στο δίκτυο μέσω καλωδίου που ανήκει στο επίπεδο 1 του μοντέλου OSI και με την port-base μέθοδο αυθεντικοποίησης γίνεται έλεγχος των συσκευών που συνδέονται στις θύρες του Switch. Στην περίπτωση ενός ασύρματου δικτύου οι θύρες συσχετίζονται με σημεία πρόσβασης. Οι ασύρματες συσκευές σαρώνουν τα σημεία πρόσβασης και η διαδικασία σύνδεσης περιλαμβάνει

ανταλλαγή πακέτων μεταξύ του χρήστη και του σημείου πρόσβασης. Όταν χρησιμοποιείται το 802.1x η πρόσβαση στο δίκτυο δεν είναι εφικτή μέχρι να αυθεντικοποιηθεί ο χρήστης, δηλαδή επιτυγχάνεται σύνδεση μόνο με το σημείο πρόσβασης χωρίς να μπορεί να μεταβιβάσει δεδομένα σε άλλα τμήματα του δικτύου. Η διαδικασία της αυθεντικοποίησης καθορίζεται από το πρωτόκολλο Extensible Authentication Protocol (EAP) [3].

Ένα σύστημα αυθεντικοποίησης 802.1x αποτελείται από τα εξής στοιχεία: τον supplicant, τον authenticator και τον authentication server. Σε ένα ασύρματο δίκτυο ο supplicant είναι συνήθως ένας κινητός κόμβος, το σημείο πρόσβασης είναι ο authenticator και ένας Authentication, Authorization, and Accounting (AAA) server, όπως ο RADIUS είναι ο authentication server. Η θύρα (port) απεικονίζει τη σχέση μεταξύ του authenticator και του supplicant, οι οποίοι έχουν ένα Port Access Entity (PAE), που χρησιμοποιεί τους αλγορίθμους και τα πρωτόκολλα που σχετίζονται με τον μηχανισμό αυθεντικοποίησης.



Εικόνα 3: Το μοντέλο αυθεντικοποίησης των τριών μερών με την χρήση ενός AAA Server

Βασισμένο στο πρωτόκολλο EAP, το πρότυπο 802.1x μπορεί να χρησιμοποιήσει διάφορους μηχανισμούς αυθεντικοποίησης, όπως τους MD, TLS, TTLS και PEAP. Στο 802.1x καθορίζεται και το EAP πάνω από ένα LAN (EAPOL) με σκοπό την ενθυλάκωση των EAP μηνυμάτων μεταξύ του supplicant και του authenticator. Το PAE του authenticator μεταδίδει τα μηνύματα μεταξύ του supplicant και του authenticator. Το 802.1x χρησιμοποιείται για να επιβάλει τη χρήση συγκεκριμένου μηχανισμού αυθεντικοποίησης και για να κατευθύνει τα μηνύματα ελέγχου ταυτότητας στην κατάλληλη διαδρομή, ενώ οι μηχανισμοί αυθεντικοποίησης ορίζουν τις πραγματικές ανταλλαγές επαλήθευσης ταυτότητας που λαμβάνουν χώρα [4].

3. ΠΡΩΤΟΚΟΛΛΑ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Σε αυτό το κεφάλαιο θα αναλυθούν πρωτόκολλα αυθεντικοποίησης και θα περιγραφεί ο τρόπος ανταλλαγής μηνυμάτων ανάμεσα στον χρήστη που θελει να αυθεντικοποιηθεί και τον εξυπηρετητή.

3.1 Αυθεντικοποίηση

Η αυθεντικοποίηση σε επίπεδο χρηστών ή συσκευών εξασφαλίζει ότι τα μέρη μιας επικοινωνίας είναι αξιόπιστα. Η αυθεντικοποίηση ωστόσο του χρήστη είναι μονομερής, όπου το ένα μέρος της επικοινωνίας αποδεικνύει στο άλλο μέρος ότι είναι αξιόπιστο. Αυτό συμβαίνει γιατί στην πλειοψηφία των περιπτώσεων ο πελάτης εμπιστεύεται το δίκτυο στο οποίο συνδέεται. Η αμοιβαία αυθεντικοποίηση μεταξύ ενός χρήστη και ενός εξυπηρετητή είναι μία ειδική περίπτωση, όπου τα δύο μέρη είναι ομότιμα. Σε αυτή την περίπτωση κάθε κόμβος αυθεντικοποιείται απο τον άλλο είτε διαδοχικά είτε παράλληλα.

Στα μεγάλα δίκτυα η αυθεντικοποίηση γίνεται με το μοντέλο των τριών μερών. Σε αυτή την περίπτωση ανάμεσα στον χρήστη και στον authentication server παρεμβάλλεται ένας network authentication server (NAS), ο οποίος ελέγχει την επικοινωνία μέσα και έξω από το ιδιωτικό δίκτυο. Επιπλέον λειτουργεί ως νέο σημείο διαχωρισμού των πρωτοκόλλων, καθώς η επικοινωνία του NAS με τον authentication server γίνεται πάνω από το αξιόπιστο ιδιωτικό δίκτυο ενώ η επικοινωνία του με τη μεριά του χρήστη γίνεται πάνω από ένα μη έμπιστο ασύρματο κανάλι επικοινωνίας. Προκειμένου να υπάρξει διαλειτουργικότητα μεταξύ του δικτυακού εξοπλισμού, τα πρωτόκολλα που χρησιμοποιούνται έχουν προτυποποιηθεί. Τα πρωτόκολλα για την επικοινωνία του χρήστη και του NAS εξαρτώνται από τον τύπο της τεχνολογίας πρόσβασης που χρησιμοποιεί ο πάροχος του δικτύου, και τις περισσότερες φορές είναι πρωτόκολλα χαμηλότερων επιπέδων. Ωστόσο ο NAS στην επικοινωνία με τον authentication server χρησιμοποιεί UDP/IP ή TCP/IP πρωτόκολλα προκειμένου να μεταφερθούν τα μηνύματα αυθεντικοποίησης για λογαριασμό του χρήστη. Για αυτό το λόγο, το πρωτόκολλο μεταξύ του NAS και του authentication server είναι ένα AAA πρωτόκολλο.

Ανάμεσα στον χρήστη και στον authentication server δεν υπάρχει άμεση επικοινωνία. Για την ανταλλαγή μηνυμάτων μεταξύ τους παρεμβάλλεται ο NAS. Το πρωτόκολλο που χρησιμοποιείται λοιπόν για την επικοινωνία μεταξύ του χρήστη και του authentication server είναι το RADIUS, το οποίο έχει σχεδιαστεί για να επιτρέπει στον NAS να μεταβιβάζει τα αιτήματα ενός χρήστη μαζί με τα διαπιστευτήρια του στον authentication server και στη συνέχεια για να απαντάει στο χρήστη με την απάντηση του server. Τα μηνύματα Access-Request και Access-Challenge του πρωτοκόλλου RADIUS δείχνουν ότι είναι σχεδιασμένο για μεθόδους αυθεντικοποίησης βασισμένες σε κωδικό, ώστε ο NAS να μεταβιβάζει τα μηνύματα του χρήστη στον authentication server και να παρουσιάζει στο χρήστη πιθανές προκλήσεις που δημιουργούνται από το δίκτυο. Ανάμεσα στο NAS και στον authentication server υπάρχει συνήθως ένας κόμβος. Στην περίπτωση που χρησιμοποιούνται και ενδιάμεσοι κόμβοι (proxies) η επικοινωνία τους δεν λαμβάνει πλέον

μέρος σε ένα ιδιωτικό δίκτυο και για αυτό θα πρέπει σε αυτές τις περιπτώσεις να υπάρχουν ειδικοί μηχανισμοί ασφάλειας.

Η επικοινωνία μεταξύ του χρήστη και του NAS είναι μέρος του δικτύου πρόσβασης. Η σύνδεση τους γίνεται μέσω ενός φυσικού καναλιού επικοινωνίας με τη χρήση ενός πρωτοκόλλου πρόσβασης. Το φυσικό κανάλι αναλαμβάνει την κωδικοποίηση και την διαμόρφωση των bits της πληροφορίας σε ηλεκτρικά σήματα. Οι νέες τεχνολογίες ασύρματης πρόσβασης, όπως τα ασύρματα τοπικά δίκτυα του προτύπου 802.11 έχουν τους δικούς τους μηχανισμούς δημιουργίας πακέτων και δεν χρειάζονται πρόσθετα πρωτόκολλα, όπως το πρωτόκολλο Point to Point (PPP) για να μεταβιβάσουν μηνύματα του επιπέδου 2. Ωστόσο, η επικοινωνία στο επίπεδο IP πραγματοποιείται μετά από την αρχική αυθεντικοποίηση. Για αυτό το λόγο η ανταλλαγή μηνυμάτων αυθεντικοποίησης μεταξύ του χρήστη και του NAS πρέπει να γίνει απευθείας με ένα πρωτόκολλο 2ου επιπέδου.

3.2 Πρωτόκολλο EAP

Για πολλά χρόνια οι χρήστες που επιθυμούσαν να συνδεθούν απομακρυσμένα μέσω μιας ενσύρματης σύνδεσης χρησιμοποιούσαν υπηρεσίες που βασίζονταν στο PPP, το οποίο ήταν σχεδιασμένο να παρέχει πολλές λειτουργικότητες του επιπέδου ζεύξης δεδομένων (link layer). Ο κύριος ρόλος του PPP ήταν να δημιουργεί πακέτα δευτέρου επιπέδου ενθυλακώνοντας δεδομένα μεταξύ της κεφαλίδας PPP και του CRC. Το PPP περιλαμβάνει 3 φάσεις προκειμένου να επιτευχθεί σύνδεση: την φάση Link Control Protocol (LCP), την φάση αυθεντικοποίησης και τη φάση Network Control Protocol (NCP). Οι μηχανισμοί αυθεντικοποίησης που υποστηρίζει το PPP ήταν το Password Authentication Protocol (PAP) και το Challenge Handshake Protocol (CHAP). Το PPP ωστόσο τρέχει πάνω από μία σύνδεση μεταξύ του χρήστη και του τελικού κόμβου. Όταν εφαρμόστηκε το μοντέλο της αυθεντικοποίησης των τριών μερών, για την μεταβίβαση των δεδομένων σε έναν authentication server θα έπρεπε να χρησιμοποιηθεί ένα άλλο πρωτόκολλο για την ασφαλή μεταφορά των δεδομένων. Οι μέθοδοι αυθεντικοποίησης PAP και CHAP δεν περιείχαν κρυπτογράφηση καθώς είχαν δημιουργηθεί για να χρησιμοποιούνται σε τηλεφωνικές γραμμές. Ένα ακόμα μειονέκτημα του PPP ήταν ότι, όταν χρησιμοποιούνται για συνδέσεις στο επίπεδο link layer, το πρωτόκολλο και ο μηχανισμός από τον οποίο ο χρήστης έπρεπε να αυθεντικοποιηθεί στο δίκτυο διαπραγματευόταν κατά την φάση LCP. Η πραγματική αυθεντικοποίηση ωστόσο πραγματοποιούνταν στη φάση της αυθεντικοποίησης. Αυτό σημαίνει ότι το σημείο της διαδικασίας στην οποία εμπλεκόταν ο χρήστης θα έπρεπε να κατανοήσει τις διαπραγματεύσεις σχετικά με τον μηχανισμό αυθεντικοποίησης.

Λόγω των προβλημάτων του PPP που αναφέρθηκαν παραπάνω, σε σχέση με τους νέους μηχανισμούς αυθεντικοποίησης, ο IETF αποφάσισε να επεκτείνει το PPP. Για αυτό το λόγο σχεδιάστηκε το EAP βάσει του προτύπου RFC2284 ως μία επέκταση του PPP, ώστε να μπορεί να υποστηρίξει τους νέους μηχανισμούς αυθεντικοποίησης. Η διαφορά του πρωτοκόλλου EAP έναντι του PPP ήταν ότι ενώ στο PPP τα δύο μέρη της διαπραγμάτευσης διαπραγματεύονταν την χρήση της μεθόδου PAP ή CHAP ως μέθοδο

αυθεντικοποίησης στη φάση LCP, ενώ στο EAP η διαπραγμάτευση της μεθόδου αυθεντικοποίησης γίνεται στη φάση της αυθεντικοποίησης, δηλαδή ένα στάδιο μετά.

Από την δημιουργία του το EAP έχει βρεί εφαρμογή σε πολλά περιβάλλοντα και εφαρμογές, ειδικά σε περιβάλλοντα πρόσβασης. Το EAP θεωρείται ένα πρωτόκολλο αυθεντικοποίησης, το οποίο έχει τη δυνατότητα να μεταφέρει μηνύματα αυθεντικοποίησης πάνω από πρωτόκολλα, όπως το PPP και πρωτόκολλα της οικογένειας IEEE 802, ή ακόμα και AAA πρωτόκολλα, τα οποία χρησιμοποιούνται μεταξύ του NAS και του authentication server.

3.2.1 Τα μηνύματα EAP

Το EAP δεν εκτελεί τον ίδιο τον έλεγχο ταυτότητας. Είναι ένα πλαίσιο που μεταφέρει μηνύματα πολύ διαφορετικών μεθόδων επαλήθευσης ταυτότητας. Αυτό σημαίνει ότι επικοινωνούν μεταξύ τους μόνο ο κόμβος με τον server, με τον NAS μεταξύ τους να μεταφράζει τα μηνύματα ανάμεσα στα πρωτόκολλα από διαφορετικές τεχνολογίες διασύνδεσης, διαβιβάζοντας τα χωρίς να ξέρει το ακριβές περιεχόμενο του μηνύματος. Τα μηνύματα του EAP είναι τα εξής:

- EAP request
- EAP response
- EAP success
- EAP failure

Τα πρώτα δύο είδη μηνυμάτων χρησιμοποιούνται για να μεταφέρουν οποιαδήποτε πληροφορία της επιλεγόμενης μεθόδου EAP, ενώ τα δύο τελευταία για τον τερματισμό μιας επικοινωνίας. Τα EAP request μηνύματα στέλνονται απο τον authentication server στον χρήστη ζητώντας την ταυτότητα του, ενώ τα EAP response μηνύματα στέλνονται ως απάντηση από τον χρήστη στον server. Ο NAS βρίσκεται ενδιάμεσα και δεν καταλαβαίνει τα request και response μηνύματα, απλά τα προωθεί. Τα μηνύματα τα οποία καταλαβαίνει ο NAS είναι τα success και failure.

Τα request και response μηνύματα έχουν ένα πεδίο στο οποίο καθορίζεται ο τύπος της πληροφορίας που διακινείται. Για παράδειγμα το “1” είναι για ταυτότητα και το “3” για Negative Acknowledgement (NAK). Ωστόσο οι περισσότεροι αριθμοί χρησιμοποιούνται για να προσδιορίσουν την μέθοδο της EAP αυθεντικοποίησης, όπως για παράδειγμα το “13” χρησιμοποιείται για τη μέθοδο EAP-TLS. Αυτή η αριθμοδότηση έχει καθοριστεί από την Internet Assigned Numbers Authority (IANA) [5].

Το πρωτόκολλο EAP έχει γίνει δημοφιλές για πολλούς λόγους. Ένας λόγος είναι η ευελιξία του, η οποία συνδυάζεται με την εισαγωγή του πεδίου του τύπου στα request και response μηνύματα. Με αυτό τον τρόπο οι νέοι αλγόριθμοι αυθεντικοποίησης μπορούν εύκολα να εφαρμοστούν χωρίς να αλλάξει τίποτα στον authenticator ή στο πρωτόκολλο EAP. Από την άλλη πλευρά, το πρωτόκολλο EAP είναι πολύ εύκολο να εφαρμοστεί από τις συσκευές που λειτουργούν ως NAS, επειδή υποστηρίζει μόνο τέσσερις τύπους

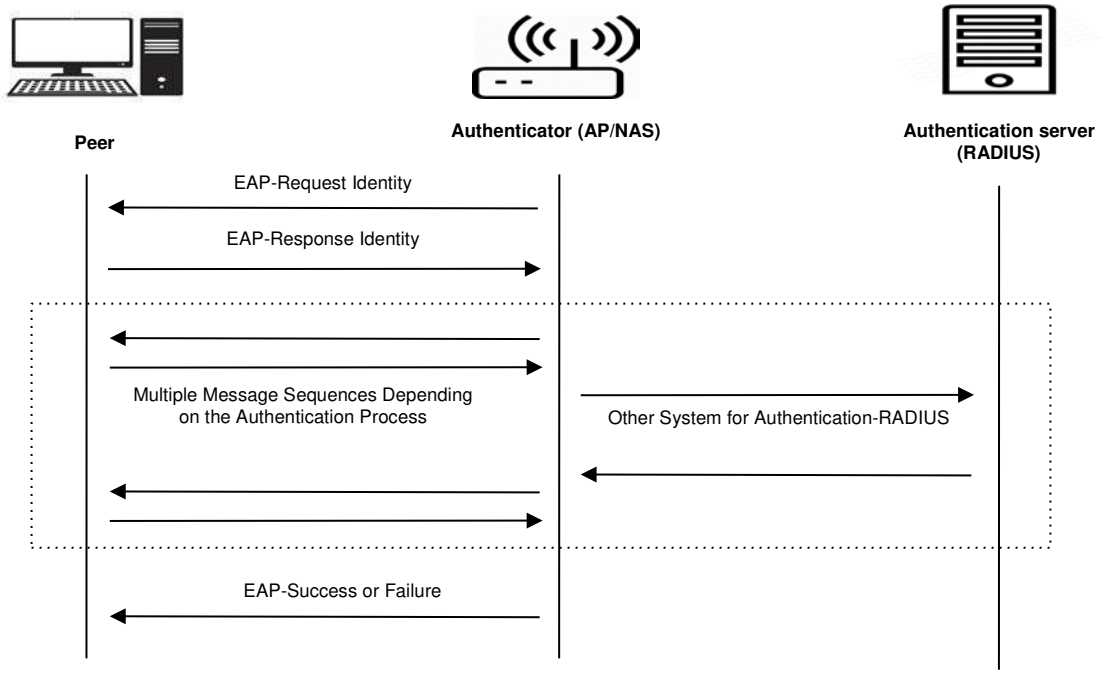
μηνυμάτων, από τους οποίους μόνο οι δύο πρέπει να γίνουν κατανοητοί. Τέλος το EAP είναι ανεξάρτητο του μέσου και για αυτό μπορεί να υποστηρίξει διάφορες τεχνολογίες όπως τις Ethernet και 802.1x.

Η διαδικασία της ανταλλαγής EAP μηνυμάτων γίνεται με τον εξής τρόπο:

- Ο NAS στέλνει ένα μήνυμα EAP-request στον χρήστη. Αυτό το μήνυμα μπορεί να περιέχει είτε αίτημα για αυθεντικοποίηση είτε απλά αίτημα για κάποιου είδους πληροφορία. Το πεδίο του τύπου σε ένα EAP-request μήνυμα υποδεικνύει το είδος της πληροφορίας που έχει ζητηθεί. Τα μηνύματα που περιλαμβάνουν το πεδίο Identity ονομάζονται EAP Identity request messages. Όταν απαιτείται αλληλεπίδραση του χρήστη είναι δυνατόν να συμπεριλαμβάνονται μηνύματα που απευθύνονται σε αυτόν. Προκειμένου να μην ανταλλάσσεται η ταυτότητα του χρήστη σε καθαρό κείμενο θα πρέπει να μεταφέρεται στον NAS μέσω κατάλληλης μεθόδου σηματοδότησης που να παρέχει εμπιστευτικότητα των μηνυμάτων.

- Ο χρηστης στη συνέχεια απαντάει με ένα EAP-response μήνυμα του ίδιου τύπου. Εαν στο πεδίο του τύπου στο EAP-request μήνυμα έχει προταθεί μία μέθοδος αυθεντικοποίησης, ο χρήστης είτε απαντάει με αυτό τον τύπο αυθεντικοποίησης είτε, εαν δεν μπορεί να τον υποστηρίξει, στέλνει ένα NAK μήνυμα. Σε αυτές τις περιπτώσεις η απάντηση του χρήστη περιλαμβάνει και πρόταση για άλλη μέθοδο αυθεντικοποίησης. Αυτό γίνεται με την δήλωση των τιμών που αντιστοιχούν στη συγκεκριμένη μέθοδο στο πεδίο type-data του NAK μηνύματος.

- Ο NAS λειτουργεί ως ενδιάμεσος που μεταφέρει τα μηνύματα μεταξύ του χρήστη και του authentication server και δεν καταλαβαίνει τις μεθόδους αυθεντικοποίησης. Αυτό διευκολύνει την διαχείριση των διαπιστευτηρίων του χρήστη καθώς αυτά δεν παραμένουν στην μνήμη του NAS.



Εικόνα 4: Ανταλλαγή μηνυμάτων EAP

Η γενική θεώρηση στο πρωτόκολλο EAP είναι ότι ο authenticator (NAS) ξεκινάει την ανταλλαγή μηνυμάτων, το οποίο σημαίνει πως ο authenticator γνωρίζει την ύπαρξη του χρήστη που ζητάει πρόσβαση. Αυτό συμβαίνει σε ένα ενσύρματο περιβάλλον. Από την άλλη πλευρά, σε ένα ασύρματο δίκτυο θα πρέπει να υπάρξει ένας μηχανισμός ανίχνευσης του χρήστη. Στο 802.1x αυτό επιτυγχάνεται με την αποστολή από τον χρήστη ενός πακέτου που ονομάζεται EAPOL-start. Αυτό το πλαίσιο προτρέπει τον NAS να ζητήσει την ταυτότητα του supplicant. Μόλις ο supplicant αποκαλύψει την ταυτότητα του ο NAS ανταλλάσει απευθείας μηνύματα με τον supplicant μέχρι η αυθεντικοποίηση να πετύχει ή να αποτύχει. Στην περίπτωση που είναι επιτυχής, η πόρτα γίνεται προσβάσιμη. Όταν ο χρήστης δεν χρειάζεται πια να είναι συνδεδεμένος στο δίκτυο στέλνει ένα πακέτο EAPOL-Logoff για να τερματίσει η συνεδρία. Σε αυτή την περίπτωση η θύρα θα γίνει πάλι μη προσβάσιμη [6].

3.2.2 Διαχείριση κλειδιών

Τα σύγχρονα πρωτόκολλα αυθεντικοποίησης παρέχουν επίσης και μηχανισμούς για διαμοιρασμό κλειδιών. Ωστόσο, η δημιουργία του κλειδιού ή η μεταφορά του εκτελούνται διαφορετικά από κάθε μέθοδο EAP. Το πρωτόκολλο EAP αρχικά σχεδιάστηκε για την μεταφορά μηνυμάτων αυθεντικοποίησης. Από την στιγμή όμως που παρέχει ένα γενικό πλαίσιο για τη μεταφορά μηνυμάτων σε έναν authentication server πάνω από AAA πρωτόκολλα, μπορεί επίσης να υποστηρίξει διαδικασίες για διαχείριση κλειδιών. Αυτή η ευελιξία του πρωτοκόλλου το καθιστά μία καλή λύση για εφαρμογή σε διαφορετικά περιβάλλοντα, ειδικά στον κόσμο των ασύρματων επικοινωνιών.

Η διαδικασία αυθεντικοποίησης και η διαχείριση κλειδιών απο το EAP διακρίνεται σε τρεις φάσεις [7]:

- **Phase 0: Authenticator discovery phase**
  Σε αυτή την αρχική φάση ο χρήστης προσπαθεί να εντοπίσει τον authenticator και διαπραγματεύεται τις δυνατότητες, όπως για παράδειγμα τον τύπο της τεχνολογίας πρόσβασης, το εύρος ζώνης και τους μηχανισμούς κρυπτογράφησης. Αυτό το στάδιο περιλαμβάνει και την επιλογή της κατάλληλης EAP μεθόδου.

- **Phase 1a: Authentication phase**
  Μετά την επιλογή της μεθόδου EAP ξεκινάει η ανταλλαγή μηνυμάτων. Ο authenticator λειτουργεί ως ενδιάμεσος. Ενθυλακώνει τα μηνύματα EAP μέσα σε κάποιο μήνυμα AAA πρωτοκόλλου (συνήθως το RADIUS), προκειμένου να επιτευχθεί η επικοινωνία με τον AAA server. Σε αυτή την φάση ανταλλάσσονται μηνύματα μεταξύ του EAP server και του χρήστη, τα οποία διαφοροποιούνται ανάλογα με τη μέθοδο που έχει επιλεγεί. Μόλις ολοκληρωθεί η φάση της αυθεντικοποίησης, η ανταλλαγή EAP μηνυμάτων σταματάει. Ωστοσο, όταν χρειάζεται διαχείριση κλειδιών (με σκοπό την ασφάλεια του καναλιού επικοινωνίας του authenticator και του χρήστη), τότε τόσο ο server όσο και ο χρήστης υπολογίζουν τα κλειδιά που απαιτούνται. Τα κλειδιά που χρησιμοποιούνται είναι ένα παροδικό κλειδί, το οποίο ονομάζεται transient EAP key (TEK) και χρησιμοποιείται για τη διασφάλιση της επικοινωνίας μεταξύ χρήστη και EAP server, και ένα κλειδί για την επικοινωνία μεταξύ χρήστη και authenticator, που ονομάζεται AAA κλειδί. Σε αυτό το στάδιο της διαδικασίας ο authenticator δεν θεωρείται έμπιστος από τον χρήστη.

- **Phase 1b: Key transport**
  Στη συνέχεια το κλειδί που έχει υπολογιστεί στέλνεται από τον server στον authenticator. Με αυτό τον τρόπο δημιουργείται μεταξύ τους ένα ασφαλές κανάλι επικοινωνίας. Αυτή η σύνδεση γίνεται συνήθως πάνω από το ιδιωτικό δίκτυο του χειριστή και ως εκ τούτου θεωρείται ασφαλής. Σε αντίθετη περίπτωση, θα πρέπει να προστατεύεται (π.χ IPsec κρυπτογράφηση).

- **Phase 2: Secure association**
  Μετά την μεταφορά του κλειδιού, ο authenticator και χρήστης μοιράζονται το ίδιο AAA κλειδί. Ο authenticator έχει λάβει το κλειδί από τον server και ο χρήστης το έχει υπολογίσει από μόνος του. Σε αυτό το στάδιο που έχουν και οι δύο τα ίδια κλειδιά και ο ένας θεωρεί τον άλλο έμπιστο μπορούν να δημιουργήσουν ένα ασφαλές κανάλι επικοινωνίας σύμφωνα με τον μηχανισμό κρυπτογράφησης που έχουν επιλέξει στη φάση 0.

Στην διαχείριση κλειδιών απαραίτητη προϋπόθεση αποτελεί ότι ο χρήστης είναι αυθεντικοποιημένος και το δίκτυο έμπιστο. Αυτό είναι απαραίτητο γιατί υπάρχει πιθανότητα ένας επιτιθέμενος να δημιουργήσει ένα ψεύτικο σημείο πρόσβασης (δρώντας σαν authenticator) και να προσομοιώσει έναν EAP/AAA server. Με αυτό τον τρόπο ο

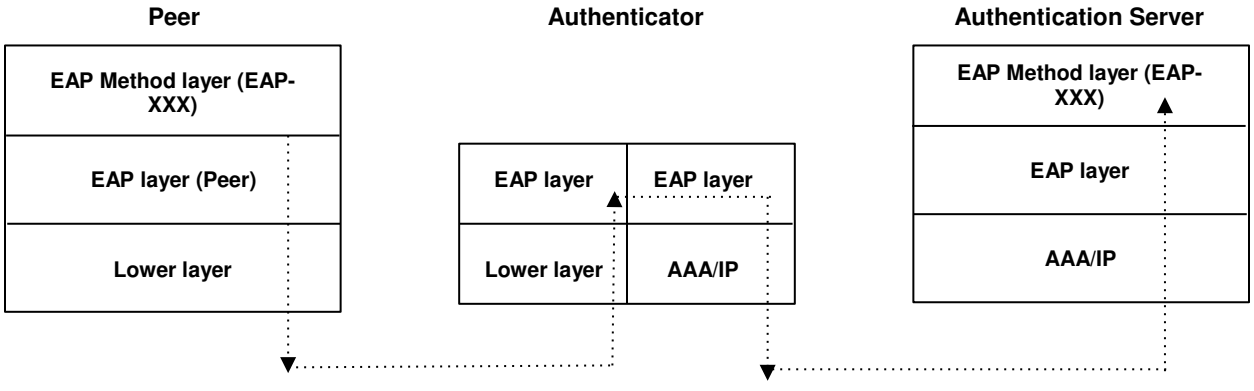
επιτιθέμενος καταφέρνει να αποκτήσει τα διαπιστευτήρια του χρήστη και να ακούσει την συνομιλία που ακολουθεί, η οποία υπάρχει περίπτωση να μην είναι κρυπτογραφημένη. Αυτός είναι ο λόγος για τον οποίο ο αμοιβαίος έλεγχος ταυτότητας είναι απαραίτητος όταν διενεργείται διαχείριση κλειδιών. Ωστόσο, ο αμοιβαίος έλεγχος ταυτότητας βασίζεται σε διαπιστευτήρια που διαρκούν μεγάλο χρονικό διάστημα, πράγμα που σημαίνει ότι και τα δύο μέρη μοιράζονται ένα προκαθορισμένο μυστικό ή χρησιμοποιούν κρυπτογράφηση ιδιωτικού κλειδιού σε συνδυασμό με πιστοποιητικά.

3.2.3 Μέθοδοι EAP

Το πρωτόκολλο EAP διευκολύνει τη διαπραγμάτευση μεταξύ του χρήστη και του server για τη μέθοδο αυθεντικοποίησης που θα χρησιμοποιηθεί και στη συνέχεια διενεργεί την αυθεντικοποίηση μέσω ενός NAS. Το EAP από μόνο του δεν κάνει την αυθεντικοποίηση αλλά προστίθεται σε αυτό μία μέθοδος που αποτελείται από τις δικές της διαδικασίες. Τα request και response μηνύματα μεταφέρουν και πληροφορίες, οι οποίες είναι απαραίτητες για την μέθοδο αυθεντικοποίησης που έχει επιλεχθεί μεταξύ του χρήστη και του server. Αυτό συμβαίνει μέχρι ο server να υποδείξει στον NAS εαν η διαδικασία έχει πετύχει ή όχι.

Όπως έχει παραπάνω αναφερθεί κατά την αρχική ανταλλαγή request και response μηνυμάτων επιλέγεται και η μέθοδος αυθεντικοποίησης. Παραδείγματα τέτοιων μεθόδων είναι οι EAP-TLS, EAP-TTLS και EAP-SIM. Επίσης η Cisco παρέχει τις μεθόδους LEAP (lightweight EAP) καο PEAP (protected EAP).

Στην παρακάτω εικόνα φαίνεται πως μεταφέρονται μέσω του EAP τα μηνύματα που καθορίζουν την μέθοδο αυθεντικοποίησης. Μόλις το μήνυμα φτάσει στα κατώτερα επίπεδα και παραδοθεί στην οντότητα διεργασιών του EAP, με βάση το πεδίο κωδικού στο μήνυμα, η οντότητα γνωρίζει το είδος του μηνύματος που έχει παραληφθεί (request ή response). Όταν το πακέτο EAP είναι response ή request και συμπεριλαμβάνει ένα πεδίο τύπου, η οντότητα γνωρίζει ποιά μέθοδος αυθεντικοποίησης θα χρησιμοποιηθεί και παραδίδει το μήνυμα στην διεργασία που έχει καθοριστεί για την επιλεγμένη μέθοδο [7].



Εικόνα 5: Αυθεντικοποίηση EAP-XXX

Τα τελικά μηνύματα με την ένδειξη success ή failure του EAP δεν περιλαμβάνουν κανένα πεδίο τύπου και ως εκ τούτου μπορούν να επεξεργαστούν από μια γενική οντότητα του

EAP, όπως ένας NAS. Αυτό είναι ένα ισχυρό χαρακτηριστικό, καθώς επιτρέπει στον NAS να κοιτάζει απλώς στο πεδίο κωδικού του μηνύματος EAP και να αναζητά μόνο την ένδειξη success ή failure για να επιτρέψετε την πρόσβαση, ενώ παράλληλα μεταδίδονται άλλα μηνύματα EAP που μεταφέρουν πληροφορίες για συγκεκριμένες μεθόδους χωρίς να χρειάζεται να κατανοήσει το περιεχόμενό τους. Όταν εισάγονται νέοι μέθοδοι ελέγχου ταυτότητας, δεν απαιτούνται αναβαθμίσεις λογισμικού στις συσκευές του δικτύου που λειτουργούν ως authenticators. Αναβάθμιση απαιτείται μονο στον χρήστη και στον authentication server, ώστε να μπορούν να υποστηρίξουν τη νέα μέθοδο.

3.2.3.1 EAP-MD5

Η μέθοδος EAP-MD5 περιγράφεται στο RFC 2284. Χρησιμοποιεί μονόδρομο αλγόριθμο κατακερματισμού σε συνδυασμό με ένα κοινό κλειδί. Όταν ένας χρήστης δημιουργεί λογαριασμό σε έναν server, ο server δημιουργεί μία σύνοψη του συνθηματικού του και το αποθηκεύει. Όταν ο χρήστης θέλει να συνδεθεί το πρωτόκολλο MD5 μετατρέπει τον κωδικό που έχει εισάγει σε σύνοψη και τον στέλνει στον server, ο οποίος με τη σειρά του συγκρίνει τις δύο συνόψεις. Ο MD5 εφαρμόζεται εύκολα και αυτό τον κάνει φιλικό προς τον χρήστη. Ωστόσο, η αυθεντικοποίηση μόνο από τη μεριά του χρήστη καθιστά τον αλγόριθμο ευάλωτο σε επιθέσεις τύπου man-in-the-middle.

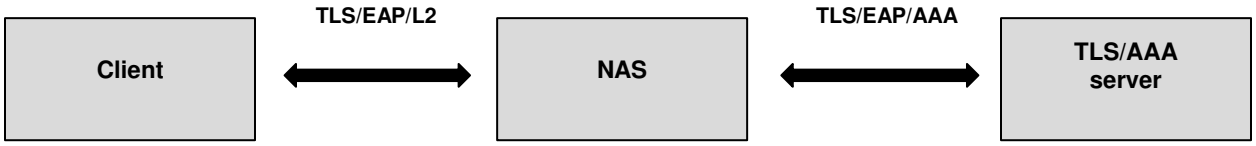
3.2.3.2 EAP-TLS

Οι περισσότερες από τις πρώτες μεθόδους EAP (π.χ. EAP-MD5) στερούνται ορισμένα σημαντικά χαρακτηριστικά όπως ο αμοιβαίος έλεγχος ταυτότητας, η διαχείριση κλειδιών και η κρυπτογράφηση. Αυτό οφείλεται στο γεγονός ότι το EAP προοριζόταν αρχικά για ενσύρματα δίκτυα.

Το TLS (Transport Layer Security) και ο προκάτοχος του το SSL (Secure Socket Layer) αποτελούν πρωτόκολλα κρυπτογράφησης, τα οποία τρέχουν απευθείας πάνω από το επίπεδο μεταφοράς. Ωστόσο, τα πρωτόκολλα του επιπέδου μεταφοράς σπάνια εμπλέκονται στην διαδικασία της αυθεντικοποίησης. Δεδομένου ότι το EAP τρέχει απευθείας στα πρωτόκολλα του επιπέδου ζεύξης, ενθυλακώνοντας TLS πακέτα μέσα στα μηνύματα EAP, λύνεται το πρόβλημα της έλλειψης του επιπέδου μεταφοράς.

Το TLS είναι ένα πρωτόκολλο με το οποίο η επικοινωνία μπορεί να πραγματοποιηθεί απευθείας μεταξύ δύο συσκευών χωρίς κάποιον ενδιάμεσο σταθμό. Αυτό επιτρέπει το TLS να μπορεί να χρησιμοποιηθεί μόνο σε μοντέλα αυθεντικοποίησης δύο μερών, στα οποία υπάρχει ένας χρήστης και ένας authenticator που ενσωματώνει και λειτουργίες server. Δεδομένου ότι το συγκεκριμένο σενάριο δεν εκπληρώνει τις προϋποθέσεις που ισχύουν σήμερα όπου πρέπει να υπάρχει ένας ξεχωριστός AAA server, το EAP-TLS χρειάζεται να μπορεί να υποστηρίζει την αυθεντικοποίηση τριών μερών με έναν ενδιάμεσο authenticator. Το πρόβλημα αυτό λύνεται με την ενσωμάτωση TLS πακέτων στα μηνύματα EAP. Όπως φαίνεται και στο παρακάτω σχήμα, το EAP-TLS μπορεί να υποστηρίξει έναν ενδιάμεσο authenticator (NAS) μεταξύ του χρήστη και του authentication server. Σε αυτή την περίπτωση ο EAP server χρησιμοποιείται παράλληλα

και ως TLS Server και με αυτό τον τρόπο δημιουργείται μια ασφαλής σύνδεση μεταξύ του authenticator και του server [7].



Εικόνα 6: Το EAP-TLS στην αυθεντικοποίηση τριών μερών

Στο διάγραμμα του σχήματος η σύνδεση που δημιουργείται είναι επί της ουσίας από άκρο σε άκρο μεταξύ του χρήστη και του TLS server. Το EAP ενθυλακώνει τα TLS πακέτα, τα οποία μεταφράζονται στις αντίστοιχες τεχνολογίες διασύνδεσης.

Η αυθεντικοποίηση στο EAP-TLS βασίζεται σε ψηφιακά πιστοποιητικά. Για αμοιβαία αυθεντικοποίηση, ο server και ο χρήστης χρειάζεται να παρουσιάσουν ένα έγκυρο πιστοποιητικό προκειμένου να αυθεντικοποιήσει ο ένας τον άλλο. Αυτό καθιστά το EAP-TLS έναν από τους πιο ασφαλείς μηχανισμούς αυθεντικοποίησης, ειδικά όταν το πιστοποιητικό του χρήστη αποθηκεύεται σε ξεχωριστή συσκευή, όπως ένα Trusted Platform Module (TPM), η λειτουργικότητα του οποίου θα αναλυθεί παρακάτω. Ενά τα ψηφιακά πιστοποιητικά αποτελούν πλεονέκτημα του EAP-TLS αποτελούν ταυτόχρονα και τρωτό του σημείο. Από τη στιγμή που τα πιστοποιητικά χρησιμοποιούνται ως μηχανισμός αυθεντικοποίησης, θα πρέπει να υπάρχει μία κατάλληλη υποδομή που θα αποδεικνύει τους ιδιοκτήτες των ιδιωτικών κλειδιών. Τον ρόλο αυτό αναλαμβάνουν οι αρχές πιστοποίησης (Certificate Authorities - CA). Ενώ αυτή η διαδικασία είναι διαχειρίσιμη στην περίπτωση των server, συχνά είναι περίπλοκη και δαπανηρή για τον χρήστη. Επιπλέον πρέπει να εξασφαλίζεται το απόρρητο των χρηστών και να μην αποκαλύπτεται η ταυτότητα τους κατά την διάρκεια της αυθεντικοποίησης. Το EAP-TLS ωστόσο δεν υποστηρίζει αυτό που ονομάζεται ψευδο-ταυτότητες.

3.2.3.3 EAP-TTLS

Η μέθοδος EAP-TTLS περιγράφεται στο RFC 5281. Λόγω των μειονεκτημάτων που σχετίζονται με το EAP-TLS, αναπτύχθηκε σύντομα μία επέκταση του πρωτοκολλου που ονομάζεται tunneled EAP-TLS (TTLS). Σύμφωνα με αυτό δεν απαιτείται ο πελάτης να αυθεντικοποιηθεί με τον ίδιο τρόπο με τον server. Αντ' αυτού, ο χρήστης περιμένει μέχρι να εγκαθιδρυθεί μία ασφαλής TLS σύνδεση, η οποία σε αυτή την περίπτωση βασίζεται μόνο στο πιστοποιητικό του server. Μόλις δημιουργηθεί αυτή η σύνδεση, ο χρήστης μπορεί για να αυθεντικοποιηθεί να χρησιμοποιήσει όποια μέθοδο επιθυμεί. Από τη στιγμή που η η επικοινωνία μέσα στο TLS tunnel είναι κρυπτογραφημένη, ο χρήστης μπορεί να χρησιμοποιήσει πολύ απλά πρωτόκολλα, όπως το CHAP ή το PAP.

Στο EAP-TTLS εισάγεται η έννοια του TTLS server, ο οποίος χρησιμοποιείται για τη δημιουργία της ασφαλούς σύνδεσης. Ενώ συνήθως ο TLS server είναι ενσωματωμένος στον AAA server, είναι πιθανό να ανήκει και σε διαφορετικό τομέα. Αυτό είναι χρήσιμο σε

περιβάλλοντα τηλεπικοινωνιών, όπου ο χρήστης συνδέεται σε έναν AAA server άλλου τομέα.

3.2.3.4 LEAP

Το LEAP (Lightweight EAP) είναι μια μέθοδος αυθεντικοποίησης που αναπτύχθηκε από τη Cisco. Λόγω του ότι η αυθεντικοποίηση βασίζεται σε μία τροποποιημένη εκδοχή του MS-CHAPv1 και ως εκ τούτου δεν χρησιμοποιεί πιστοποιητικά, ονομάστηκε Lightweight EAP. Αυτή η μέθοδος προσφέρει αμοιβαία αυθεντικοποίηση αντί για μονόδρομο, μεταξύ του χρήστη και του server. Η διαδικασία ξεκινάει με ένα κοινό μυστικό κλειδί που έχει μοιραστεί απο πριν. Αρχικά ο χρήστης στέλνει μια τυχαία αίτηση στον server, ο server αποκρυπτογραφεί το μήνυμα και στέλνει πίσω την απάντηση του κρυπτογραφόντας την με το κλειδί της συνόδου. Ο χρήστης αποκρυπτογραφεί το μήνυμα μόνο αν η τιμή του μηνύματος είναι ίδια με αυτή που έχει αποθηκευμένη. Με τον ίδιο τρόπο αυθεντικοποιεί και ο server τον χρήστη. Αυτό το χαρακτηριστικό περιορίζει τις επιθέσεις man-in-the-middle αλλά η μέθοδος εξακολουθεί να είναι ευάλωτη σε dictionary attacks.

3.2.3.5 EAP-PEAP

Η μεθοδος EAP-PEAP είναι παρόμοια με το TLS. Χρησιμοποιεί υποδομή ιδιωτικών κλειδιών και ψηφιακά πιστοποιητικά για την αυθεντικοποίηση. Σε αντίθεση με το TLS απαιτεί μόνο ένα πιστοποιητικό, καθώς πρόκειται για μέθοδο μονόδρομης αυθεντικοποίησης. Η συγκεκριμένη μέθοδος παρουσιάζει μείωση τους κόστους και της πολυπλοκότητας, απαιτώντας μόνο ένα πιστοποιητικό από τον server και όχι από τον χρήστη. Η PEAP μπορεί να φανεί χρήσιμη σε περιπτώσεις κρυπτογράφησης μηνυμάτων, ασφαλούς ανταλλαγής κλειδιών και γρήγορης επανασύνδεσης.

3.2.3.6 EAP-POTP

Η μέθοδος EAP-POTP (Protected One-Time Password) περιγράφεται στο RFC 4793 και βασίζεται στη χρήση κωδικών μιας χρήσης για την έκδοση κλειδιών αυθεντικοποίησης. Δίνει τη δυνατότητα μονόδρομης ή αμφίδρομης αυθεντικοποίησης για μεθόδους που χρησιμοποιούν το EAP. Χρησιμοποιεί αυθεντικοποίηση δύο παραγόντων για τους χρήστες, απαιτώντας έναν κωδικό μιας χρήσης και έναν προσωπικό κωδικό PIN.

3.2.3.7 EAP-PSK

Η μέθοδος EAP-PSK (Pre-shared key) περιγράφεται στο RFC 4764. Χρησιμοποιεί ένα κοινόχρηστο κλειδί για αμοιβαία αυθεντικοποίηση και παραγωγή του κλειδιού της συνόδου. Αν η αμοιβαία αυθεντικοποίηση είναι επιτυχής, τότε δημιουργείται ένα ασφαλές κανάλι επικοινωνίας και για τις δύο οντότητες προκειμένου να επικοινωνήσουν πάνω από μη ασφαλή δίκτυα όπως τα IEEE 802.11. Το EAP-PSK αποτελεί μία επεκτάσιμη μέθοδο EAP, η οποία δεν απαιτεί κάποιο μέθοδο κρυπτογραφίας δημόσιου κλειδιού. Η ανταλλαγή μηνυμάτων γίνεται στο ελάχιστο από τέσσερα μηνύματα.

3.2.3.8 EAP-SIM

Η αυθεντικοποίηση που βασίζεται στις κάρτες SIM (Subscriber Identity Module) ξεκίνησε από τον κόσμο των κινητών τηλεφώνων και έγινε γρήγορα δημοφιλής και στα ασύρματα δίκτυα. Μία κάρτα SIM είναι μία μορφή έξυπνης κάρτας που περιέχει έναν μικροεπεξεργαστή κρυπτογράφησης, ο οποίος χρησιμοποιείται για τη δημιουργία ενός μυστικού κωδικού, που χρειάζεται για την αυθεντικοποίηση και τη διαχείριση των κλειδιών. Από τη στιγμή που αυτός ο τρόπος αυθεντικοποίησης απαιτεί την φυσική παρουσία μιας κάρτας SIM, η οποία τις περισσότερες φορές προστατεύεται και από ένα επιπλέον κωδικό (Personal Identification Number - PIN), θεωρείται ένας αρκετά ισχυρός μηχανισμός αυθεντικοποίησης.

Η μέθοδος EAP-SIM περιγράφεται στο RFC 4186 και αποτελεί την πρώτη μέθοδο αυθεντικοποίησης για ασύρματα δίκτυα που βασίζεται σε κάρτα SIM. Παρέχει αμφίδρομη αυθεντικοποίηση και η συμφωνία του κλειδιού της συνόδου βασίζεται στην κάρτα SIM των GSM δικτύων. Ο χρήστης (για παράδειγμα μια συσκευή με wifi λειτουργία και υποστήριξη κάρτας SIM) επικοινωνεί με τον authenticator, ο οποίος σε πρώτη φάση επικοινωνει με τον authentication server. Ο authentication server δεν γνωρίζει τα διαπιστευτήρια από την κάρτα SIM. Θα πρέπει να προωθήσει το αίτημα στο GSM authentication Centre (AuC) πάνω από ένα SS7 (Signaling System No.7) δίκτυο. Το AuC στέλνει πίσω το GSM κρυπτογραφημένο μήνυμα, το οποίο στέλνεται πίσω στον authentication server και συγκρίνεται με το αποτέλεσμα που έχει σταλεί από τον χρήστη.

3.2.3.9 EAP-TPM

Η μέθοδος EAP-TPM κάνει χρήση του TPM για τη διαδικασία της αυθεντικοποίησης. Το TPM εισήχθη το 2002 από την Trusted Computing Group (TCG). Το TPM τοποθετείται απευθείας στην μητρική κάρτα, παρέχει κρυπτογραφικές λειτουργίες και αποθηκεύει με ασφάλεια το λεγόμενο ζεύγος κλειδιών έγκρισης, παρόμοιο με το ζεύγος ιδιωτικών/δημόσιων κλειδιών. Επιπλέον κάθε TPM χαρακτηρίζεται από έναν μοναδικό αριθμό ταυτότητας. Από αυτή την άποψη το TPM μοιάζει με μία κάρτα SIM. Ωστόσο, το TPM παρέχει επιπλέον λειτουργίες, όπως για παράδειγμα η δυνατότητα αυτόματης παραγωγής ψηφιακών πιστοποιητικών, τα οποία μπορούν να χρησιμοποιηθούν για αυθεντικοποίηση στο δίκτυο.

Η ανωτέρω μέθοδος που χρησιμοποιεί τις δυνατότητες του TPM δεν έχει ακόμη τυποποιηθεί. Η προδιαγραφή είναι διαθέσιμη σε ένα Internet Draft και ένα πρώτο πρωτότυπο έχει κατασκευαστεί σε ένα σχέδιο της Swisscom. Χωρίς να μπούμε σε τεχνικές λεπτομέρειες σε αυτό το σημείο, μπορεί κανείς να συνοψίσει ότι αυτή η μέθοδος ξεπερναει τα μειονεκτήματα των παραδοσιακών πιστοποιητικών απο τη μερια του χρήστη. Η διαδικασία περιλαμβάνει την αυτοματοποιημένη παραγωγή και διανομή των πιστοποιητικών καθώς και έναν ασφαλή και αξιόπιστο τρόπο αποθήκευσης του ιδιωτικού κλειδιού, που βασίζεται σε εξαρτήματα υλικού.

Η μέθοδος EAP-TPM είναι μία πολλά υποσχόμενη μέθοδος, λόγω του ότι ο μηχανισμός TPM έχει πλέον εφαρμοστεί σε όλα τα σύγχρονα υπολογιστικά συστήματα και για αυτό το λόγο δεν απαιτείται επιπλέον εξοπλισμός. Δεδομένου ότι χρησιμοποιεί μια παραλλαγή

ενός ψηφιακού πιστοποιητικού μπορεί να θεωρηθεί ισχυρότερος μηχανισμός από τις μεθόδους που βασίζονται στον κωδικό πρόσβασης. Επιπλέον, ολόκληρη η διαδικασία αυθεντικοποίησης μπορεί να αυτοματοποιηθεί πλήρως, με αποτέλεσμα να μην εμπλέκεται καθόλου ο χρήστης στη διαδικασία.

3.3 Πρωτόκολλο RADIUS

Τα πρωτόκολλα RADIUS και DIAMETER χρησιμοποιούνται για την επικοινωνία μεταξύ του NAS και του AAA server. Ωστόσο, από τα πρώτα χρόνια χρήσης του το πρωτόκολλο RADIUS είχε κάποια σοβαρά προβλήματα με την ασφάλεια. Τα προβλήματα αυτά προσπάθησαν να λυθούν με το πρωτόκολλο DIAMETER, το οποίο θεωρείται διάδοχος του.

Το RADIUS χρησιμοποιήθηκε αρχικά για υπηρεσίες απομακρυσμένης πρόσβασης dial-in χρηστών και προοριζόταν για να επιτρέπει στον NAS να προωθεί μηνύματα dial up χρηστών για πρόσβαση στο δίκτυο σε έναν server αυθεντικοποίησης. Η αρχική προδιαγραφή χρησιμοποιούσε τα πρωτόκολλα PAP και CHAP για να μεταφέρει τα διαπιστευτήρια των χρηστών. Αυτό συνέβαινε διότι ο αρχικός τύπος μηνυμάτων στο RADIUS βασιζόταν σε ένα μοτίβο Access-Request και Access-Response. Αρχικά το RADIUS σχεδιάστηκε ώστε να είναι επεκτάσιμο. Αυτή η ιδιότητα του πολλές φορές χρησιμοποιήθηκε για να υποστηρίξει νέες απαιτήσεις, όπως για παράδειγμα η μεταφορά EAP μηνυμάτων.

Το RADIUS είναι ένα client-server πρωτόκολλο. Είναι σημαντικό να κατανοήσει κανείς ότι ο πελάτης δεν είναι ο χρήστης ή η συσκευή που προσπαθεί να συνδεθεί αλλά ο NAS. Κατά τη διάρκεια της αυθεντικοποίησης, ο NAS προωθεί τα μηνύματα του χρήστη μεταφράζοντας τα μηνύματα EAP από πρωτόκολλα δευτέρου επιπέδου (συνήθως EAPOL) στο πρωτόκολλο RADIUS. Μετά την επιτυχή αυθεντικοποίηση, ο NAS εγκαθιδρύει ένα ασφαλές κανάλι επικοινωνίας μεταξύ του χρήστη και του ίδιου. Από τη στιγμή εκείνη και έπειτα, εάν απαιτείται λογιστική καταγραφή, συγκεντρώνει δεδομένα χρήσης υπηρεσιών και τα στέλνει στον AAA server. Ωστόσο, η εξουσιοδότηση και η λογιστική καταγραφή δεν συμπεριλαμβάνονταν στις αρχικές προδιαγραφές του πρωτοκόλλου. Πολλές από τις σημερινές λειτουργίες του πρωτοκόλλου, όπως αυτές που αναφέρονται παραπάνω, περιγράφονται στο RFC που επεκτείνει τις αρχικές προδιαγραφές του το RFC 2856.

3.3.1 Μηνύματα RADIUS

Στις βασικές προδιαγραφές του πρωτοκόλλου καθορίζονται τέσσερις τύποι μηνυμάτων που χρησιμοποιούνται για την επικοινωνία μεταξύ του server και του χρήστη. Στη συνέχεια με την επέκταση του πρωτοκόλλου οι τύπου μηνυμάτων καθορίστηκαν στους εξής οκτώ:

- Access Request: Χρησιμοποιείται για την προώθηση των αιτήσεων του χρήστη. Δημιουργούνται από τον NAS και στέλνονται στον server.

- Access Challenge: Χρησιμοποιούνται από τον server για να ζητήσει από τον NAS να εκτελέσει κάποια ενέργεια.
- Access Accept: Στέλνονται από τον server για να επιβεβαιώσει τα αιτήματα.
- Access Reject: Στέλνονται από τον server για την απόρριψη των αιτημάτων.
- Accounting request and response: Μηνύματα τα οποία περιέχουν πληροφορίες καταγραφής.
- Status Server and Status Client: Δύο πειραματικοί τύποι μηνυμάτων που δεν χρησιμοποιούνται.

Σε νεότερες εκδόσεις του πρωτοκόλλου καθορίζονται και άλλοι τύποι μηνυμάτων. Για να είναι όμως συμβατό με παλαιότερες εκδόσεις δηλώνονται ως ενημερώσεις και όχι σαν βασικές προδιαγραφές. Επιπλέον, δεν είναι απαραίτητο να χρησιμοποιηθούν νέοι τύποι μηνυμάτων για να επεκταθεί το πρωτόκολλο. Ο μηχανισμός που επιτρέπει τις επιπλέον λειτουργικότητες συμπεριλαμβάνεται στη μορφή του μηνύματος.

Ένα μήνυμα RADIUS περιλαμβάνει μία κεφαλίδα, ένα πεδίο με τον κωδικό του αντίστοιχου τύπου του μηνύματος, ένα ID, πεδίο με το μέγεθος του μηνύματος και ένα πεδίο αυθεντικοποίησης, που χρησιμοποιείται για την προστασία του περιεχομένου του μηνύματος. Τα πραγματικά δεδομένα μεταφέρονται στο πεδίο payload, το οποίο είναι δομημένο ως λίστα των χαρακτηριστικών Time-Length-Value (TLV).

Τα χαρακτηριστικά διαμορφώνονται ως εξής: κάθε χαρακτηριστικό αποτελείται από ένα πεδίο τύπου (έως και μία οκτάδα), το μήκος του χαρακτηριστικού και η τιμή του χαρακτηριστικού που μεταφέρει τα δεδομένα (εξ ου και ο όρος TLV). Η ίδια η λίστα μπορεί να είναι οποιουδήποτε μεγέθους. Ωστόσο, δεδομένου ότι το πεδίο τύπου του χαρακτηριστικού περιορίζεται σε 8 bits, μόνο 255 διαφορετικοί τύποι μπορούν να οριστούν. Το βασικό RFC 2865 καθορίζει περίπου σαράντα τύπους μηνυμάτων και πολλά Vendor-Specific Attributes (VSA) που είναι γνωστά. Αυτή η μορφή μηνύματος δίνει στο RADIUS την ευελιξία και δυνατότητα επέκτασης, χαρακτηριστικά που το έκαναν να εξακολουθεί να χρησιμοποιείται έντονα στις μέρες μας.

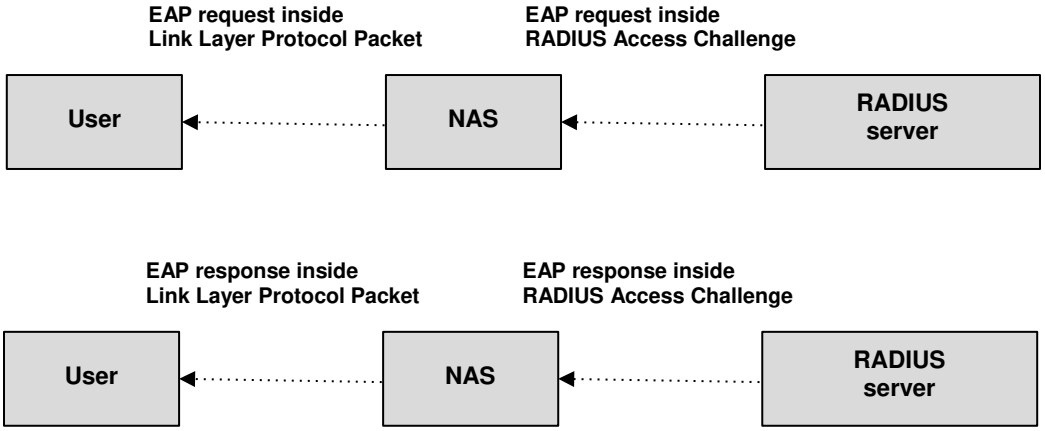
3.3.2 Αλληλεπίδραση πρωτοκόλλων RADIUS και EAP

Όπως αναφέρθηκε προηγουμένως το EAP έχει σχεδιαστεί για να παρέχει υποστήριξη για ένα γενικό τύπο πρωτοκόλλου αυθεντικοποίησης χωρίς να απαιτούνται συγκεκριμένες αναβαθμίσεις στον NAS. Δεδομένου ότι το EAP βασίζεται σε έναν backend server για να κάνει τον έλεγχο ταυτότητας, το RADIUS επεκτάθηκε για να παρέχει αυτή την υποστήριξη.

Κατά την μεταφορά των μηνυμάτων μεταξύ του NAS και του RADIUS server, τα μηνύματα EAP μεταφέρονται μέσω ενός AAA πρωτοκόλλου. Η ευελιξία του RADIUS και η επεκτασιμότητα του δίνουν τη δυνατότητας μεταφοράς μηνυμάτων άλλων πρωτοκόλλων μέσα στα μηνύματα RADIUS. Με αυτό τον τρόπο, όπως φαίνεται στην παρακάτω εικόνα,

ενθυλακώνονται τα μηνύματα του πρωτοκόλλου EAP στα μηνύματα Access Request and Access Challenge του RADIUS, που ανταλλάσσονται μεταξύ του NAS και του server και αντίστροφα [7]:

- Τα μηνύματα ερωτήσεων από τον RADIUS server πρός τον χρήστη (EAP request messages) μεταφέρονται μέσα στα Access Challenge μηνύματα RADIUS. Ο NAS αποσυνθέτει το EAP request μήνυμα από το Access Challenge και το στέλνει πάνω από ένα πρωτόκολλο δευτέρου επιπέδου στο χρήστη.
- Η απάντηση από τον χρήστη στον RADIUS server μεταφέρεται στον NAS μέσα στο EAP response μήνυμα, ο οποίος στη συνέχεια το ενσωματώνει μέσα στο Access Request μήνυμα που στέλνεται στον server.



Εικόνα 7: Ενσωμάτωση των μηνυμάτων EAP εντός των μηνυμάτων RADIUS

3.3.3 Η ασφάλεια και η αξιόπιστη μεταφορά μηνυμάτων στο RADIUS

Κατά την αρχική δημιουργία των προδιαγραφών του RADIUS, το UDP θεωρήθηκε περισσότερο κατάλληλο από το TCP λόγω του μεγάλου κόστους λειτουργίας για την δημιουργία μιας TCP συνόδου. Δυστυχώς, η έλλειψη αξιοπιστίας του UDP προκάλεσε ορισμένα σοβαρά προβλήματα στο RADIUS. Η αξιόπιστη επικοινωνία είναι ζωτικής σημασίας για τη λογιστική καταγραφή, καθώς η απώλεια λογιστικών πληροφοριών έχει ως αποτέλεσμα απώλεια εσόδων για τον διαχειριστή.

Το RADIUS παρέχει ένα ελάχιστο σύνολο μηχανισμών ασφαλείας. Ανάλογα με τον τύπο μηνύματος (Access Request, Access Response κ.λπ.) ορισμένα μέρη του μηνύματος ελέγχονται βάσει ενός κοινού μυστικού μεταξύ του authenticator και του server. Ο αλγόριθμος MD5 χρησιμοποιείται για να δημιουργεί συνόψεις των σημαντικών στοιχείων. Οι συνόψεις μεταδίδονται στη συνέχεια στο πεδίο αυθεντικοποίησης ενός RADIUS μηνύματος. Ένας μηχανισμός που ονομάζεται Attribute Hiding χρησιμοποιείται για την προστασία ιδιωτικών πληροφοριών όπως οι κωδικοί πρόσβασης. Ωστόσο, οι παρεχόμενοι μηχανισμοί απέχουν από τις σημερινές απαιτήσεις για ασφαλή επικοινωνία.

Μία λύση που χρησιμοποιείται για να ξεπεραστούν αυτά τα εμπόδια είναι η χρήση του IPsec. Το IPSec παρέχει αυθεντικοποίηση και κρυπτογράφηση για μηνύματα RADIUS και συνεπώς συνιστάται η χρήση του. Ωστόσο, το IPSec παρέχει ασφάλεια μόνο στην επικοινωνία δύο κόμβων μεταξύ τους. Εάν εμπλακεί στην επικοινωνία ένας ενδιάμεσος (proxy), τα μηνύματα πρέπει να αποκρυπτογραφούνται και να κρυπτογραφούνται πλήρως σε κάθε κόμβο, αποκαλύπτοντας έτσι προσωπικά δεδομένα. Αυτό σημαίνει ότι ο διαχειριστής πρέπει να εμπιστεύεται κάθε μεμονωμένο κόμβο στη διαδρομή επικοινωνίας, το οποίο αποτελεί εμπόδιο, ειδικά σε περιβάλλοντα περιαγωγής.

4. TRUSTED PLATFORM MODULE (TPM)

Σε αυτό το κεφάλαιο θα περιγραφούν τα χαρακτηριστικά του TPM, τα υποσυστήματα από τα οποία αποτελείται και ο τρόπος λειτουργίας του.

4.1 Η ιστορία του TPM

Ένα Trusted Platform Module (TPM) είναι ένας κρυπτογραφικός μικροεπεξεργαστής που πλέον υπάρχει στους περισσότερους εμπορικούς υπολογιστές και εξυπηρετητές και έχει σχεδιαστεί για να προστατεύει το υλικό μέσω ολοκληρωμένων κρυπτογραφικών κλειδιών. Μέχρι πρότινος τα TPMs, παρόλο που υπήρχαν σε μεγάλο αριθμό υπολογιστών, δεν ήταν γνωστά στους χρήστες λόγω του μικρού αριθμού εφαρμογών που τα χρησιμοποιούσαν. Μέσα σε λίγα χρόνια όμως, ο μεγάλος αριθμός κυβερνοεπιθέσεων έκανε τους ειδικούς στην ασφάλεια να ακολουθήσουν μία πολυεπίπεδη προσέγγιση, με ενσωματωμένη ασφάλεια σε κάθε επίπεδο. Με αρκετά επίπεδα ασφάλειας, οι οργανισμοί μπορούν να είναι πλήρως προετοιμασμένοι για επιθέσεις που γίνονται ολοένα και πιο προχωρημένες. Η προστασία από ανθρώπινα λάθη και τυχαίες διαρροές αποτελεί επίσης αναπόσπαστο μέρος αυτής της πολυεπίπεδης προσέγγισης. Στον πυρήνα αυτού του μοντέλου βρίσκεται το υλικό, το οποίο μπορεί να προστατευτεί με τη χρήση του TPM [8].

Οι τεχνικές προδιαγραφές του TPM δημιουργήθηκαν από την Trusted Computing Group, έναν διεθνή οργανισμό που ασχολείται με τη δημιουργία προδιαγραφών ασφαλείας για υπολογιστές και άλλες συσκευές. Η αρχιτεκτονική του TPM καθορίστηκε από την τεχνική επιτροπή (Technical Committee) και η ομάδα εργασίας του TPM την εφάρμοσε στην πράξη [10]. Οι προδιαγραφές αυτές τυποποιήθηκαν το 2009 από τον Οργανισμό Τυποποίησης (ISO) και την Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC) ως ISO/IEC 11889 [11].

Το πρώτο ευρέως αναπτυσσόμενο TPM ήταν το TPM 1.1b, το οποίο παρουσιάστηκε το 2003. Οι βασικές λειτουργίες του ήταν διαθέσιμες ακόμα και σε αυτή την πρώτη έκδοση. Αυτές περιλάμβαναν την παραγωγή κλειδιών (RSA κλειδιά), την αποθήκευση τους, την ταυτοποίηση συσκευών και τη βεβαίωση της ορθής λειτουργίας της συσκευής. Η βασική του λειτουργικότητα, δηλαδή η εγγύηση του απορρήτου, επιτυγχάνονταν μέσω της χρήσης ανώνυμων κλειδιών ταυτότητας, βάσει πιστοποιητικών που θα μπορούσαν να παρέχονται με το TPM. Προς αυτή την κατεύθυνση εφευρέθηκε μία νέα οντότητα δικτύου,

που αποκαλείται privacy certificate authority (CA), με στόχο να παρέχει ένα μέσο που να αποδεικνύει ότι ένα κλειδί που δημιουργήθηκε στο TPM προήλθε από ένα πραγματικό TPM χωρίς ωστόσο να προσδιορίζεται από ποιο συγκεκριμένα. Ένα από τα μειονεκτήματα αυτής της πρώτης έκδοσης του TPM ήταν η ασυμβατότητα του σε επίπεδο υλικού. Εξαιτίας αυτών των δυσλειτουργιών από το 2005 έως το 2009 δημιουργήθηκε μία νέα έκδοση του TPM το TPM 1.2.

Οι αρχικές βελτιώσεις του σε σχέση με το 1.1b περιελάμβαναν μια τυπική διεπαφή λογισμικού και κυρίως ένα τυπικό pinout πακέτο. Μία ακόμα προσθήκη στις νέες προδιαγραφές ήταν η προστασία που θα έπρεπε να έχει το TPM απέναντι στις dictionary attacks. Στη νέα έκδοση του TPM προστέθηκαν επίσης μία δεύτερη μέθοδος ανωνυμοποίησης κλειδιών, μία μέθοδος εκχώρησης βασικής εξουσιοδότησης και διαχειριστικές λειτουργίες. Σε επίπεδο υλικού προστέθηκε μία NVRAM (περίπου 2KB), ώστε να αποθηκεύεται εκεί το πιστοποιητικό έγκρισης του TPM. Στην πρώτη έκδοση του TPM θεωρήθηκε ότι κάτοχος του TPM είναι ο διαχειριστης του μηχανήματος και κάτοχος των κλειδιών ο χρήστης του. Στην έκδοση όμως 1.2 ο χρήστης θα έπρεπε να μπορεί να χρησιμοποιεί την εξουσιοδότηση του κατόχου του TPM, προκειμένου να αποφύγει τις dictionary attacks. Σχεδιάστηκε λοιπόν στο 1.2 μια τεχνική για να επιτρέπει στους χρήστες να δημιουργούν κλειδιά που θα μπορούσαν να μετεγκατασταθούν μόνο από ένα ορισμένο τρίτο μέρος. Τέτοια κλειδιά θα μπορούσαν να πιστοποιηθούν για το σκοπό αυτό και ως εκ τούτου ονομάστηκαν Certified Migratable Keys (CMKs). Τέλος στο TPM 1.2 προστέθηκε μια μπαταρία ώστε το ρολόι που βρίσκεται σε αυτό να μην χάνει ενέργεια όταν σβήνει ο υπολογιστής. Με αυτό τον τρόπο δόθηκε η δυνατότητα συγχρονισμού ενός εσωτερικού χρονοδιακόπτη με ένα εξωτερικό διακόπτη. Αυτή η λειτουργία θα μπορούσε για παράδειγμα να χρησιμοποιηθεί για τον προσδιορισμό της υπογραφής ενός συμβολαίου και για να μπορεί να προσδιοριστεί πόσος χρόνος πέρασε μεταξύ των διαδικασιών υπογραφής από το TPM [8].

Η αρχιτεκτονική του TPM 1.2 βασιζόταν στον αλγόριθμο SHA-1, ο οποίος ήταν ο πιο ισχυρός εμπορικός αλγόριθμος εκείνη την εποχή και ήταν εφικτό να χρησιμοποιηθεί σε ένα φθηνό, μικρό πακέτο. Το 2005 όμως δημοσιεύτηκε η πρώτη σημαντική επίθεση στον SHA-1. Η πράξη έδειξε πως οι αλγόριθμοι κρυπτογράφησης γίνονται όλο και ασθενέστεροι με την πάροδο του χρόνου. Παρόλο που η ανάλυση της επίθεσης έδειξε πως δεν μπορεί να εφαρμοστεί στους τρόπους που χρησιμοποιείται ο SHA-1 από το TPM, η TCG ξεκίνησε αμέσως να εργάζεται για την ανάπτυξη του προτύπου του TPM 2.0. Σύμφωνα με το νέο αυτό πρότυπο το TPM δεν θα είχε κώδικα για έναν συγκεκριμένο αλγόριθμο αλλά θα ενσωμάτωνε ένα αναγνωριστικό αλγορίθμου, ώστε να επιτρέπει τη χρήση οποιουδήποτε αλγορίθμου χωρίς αλλαγές στις προδιαγραφές του. Το TPM 2.0 θα χρησιμοποιούσε συνόψεις μεγαλύτερες από αυτές των 20 byte του SHA-1. Αυτό ήταν πιθανό να έχει ως αποτέλεσμα την αύξηση του κόστους, την αλλαγή των κλειδιών και την μείωση της απόδοσης του TPM. Ως λύση σε αυτό το πρόβλημα η ομάδα εργασίας του TPM αποφάσισε τη χρήση της κοινής πρακτικής της κρυπτογράφησης ενός συμμετρικού κλειδιού με ένα ασύμμετρο κλειδί και των δεδομένων με το συμμετρικό κλειδί.

Το TPM 1.2 ενσωμάτωνε τις παρακάτω λειτουργίες:

- Αναγνώριση συσκευών: Πριν από την εμφάνιση του TPM η ταυτοποίηση των συσκευών γινόταν με μη ασφαλή χαρακτηριστικά, όπως ήταν οι διευθύνσεις IP και MAC.

- Ασφαλής δημιουργία κλειδιών: Η ύπαρξη μιας συσκευής που δημιουργεί τυχαία κλειδιά αποτελεί τεράστιο πλεονέκτημα ασφάλειας.

- Ασφαλής αποθήκευση κλειδιών: Η ασφαλής φύλαξη των κλειδιών, ειδικά από επιθέσεις λογισμικού, αποτελεί μεγάλο πλεονέκτημα των συσκευών που έχουν ενσωματωμένο το TPM.

- Μνήμη NVRAM: Η ύπαρξη της NVRAM στο TPM βοηθάει στην διατήρηση των πιστοποιητικών όταν διαγράφεται ο σκληρός δίσκος μιας συσκευής.

- Βεβαίωση ορθής λειτουργίας της συσκευής: Με το TPM μπορεί εύκολα να γίνει αντιληπτό εάν μια συσκευή έχει παραβιαστεί.

Το TPM πέρα των παραπάνω, έχει επιπλέον και τις εξής λειτουργίες:

- Ευελιξία αλγορίθμου: Ο αλγόριθμος που χρησιμοποιείται μπορεί να αλλάξει χωρίς αλλαγή των προδιαγραφών.

- Βελτιωμένη εξουσιοδότηση: Η νέα έκδοση του TPM περιλαμβάνει διαχειριστικές λειτουργίες. Αυτή η νέα λειτουργικότητα ενοποιεί τον τρόπο που εξουσιοδοτούνται όλες οι οντότητες στο TPM και επεκτείνει τη δυνατότητα εφαρμογής πολιτικών, που επιτρέπουν αυθεντικοποίηση πολλών παραγόντων.

- Γρήγορη φόρτωση κλειδιών: Η φόρτωση κλειδιών στο TPM γίνεται γρήγορα με τη χρήση της συμμετρικής κρυπτογράφησης.

- Ευέλικτη διαχείριση: Διαφορετικά είδη εξουσιοδότησης μπορούν να διαχωριστούν, επιτρέποντας πιο ευέλικτη διαχείριση των πόρων του TPM.

- Προσδιορισμός πόρων με ονόματα: Έμμεσες αναφορές στο σχεδιασμό του TPM 1.2 οδήγησε σε κενά ασφαλείας, τα οποία διορθώθηκαν στην έκδοση 2 με τη χρήση ασφαλών κρυπτογραφημένων ονομάτων για όλους του πόρους του TPM.

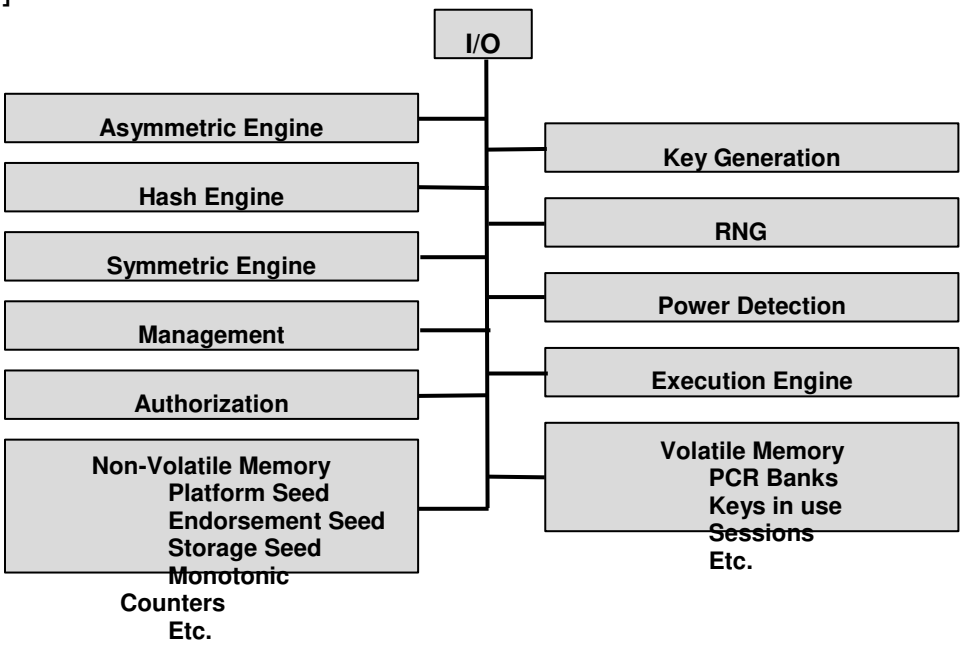
4.2 Τα χαρακτηριστικά του TPM

Το TPM παρέχει μια ολόκληρη σειρά εργαλείων που χρησιμοποιούνται για ασφαλή έλεγχο ταυτότητας. Όλες οι ιδέες πίσω από το TPM βασίζονται στη μετακίνηση της ασφάλειας στο υλικό. Σε αντίθεση με τα υπάρχοντα συστήματα ασφαλείας, που έχουν εγγενή λάθη, καθώς λειτουργούν πάνω από άγνωστο υλικό, τα συστήματα που έχουν TPM αποθηκεύουν τα ευαίσθητα δεδομένα σε μία ασφαλή τοποθεσία σε ένα ξεχωριστό

κομμάτι υλικού. Το TPM ταυτοποιεί μοναδικά το υλικό και δεν επιτρέπει σε ευαίσθητα δεδομένα να φύγουν από αυτό. Τα ευαίσθητα δεδομένα μπορούν να χρησιμοποιηθούν μέσα από το TPM, αλλά δεν μπορούν να έχουν άμεση πρόσβαση εκτός αυτού. Ακόμα κι αν κάποιος κατάφερε να αποκτήσει απεριόριστη πρόσβαση στον υπολογιστή, δεν θα είχε πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο TPM.

Το TPM είναι ένα τσιπ που πιστοποιεί το ίδιο το υλικό. Το τσιπ έχει σχεδιαστεί έτσι ώστε να επιτρέπεται μόνο ένα μικρό υποσύνολο ασφαλών ενεργειών. (π.χ. επιτρέπεται η κρυπτογράφηση ενός μηνύματος με ένα κλειδί, ωστόσο η πρόσβαση στο κλειδί είναι άμεσα περιορισμένη). Δεδομένου ότι οι περισσότερες επιθέσεις προέρχονται από άγνωστο υλικό, η δυνατότητα αναγνώρισης της συσκευής εξαλείφει τη δυνατότητα κάποιου να κλέψει ένα κλειδί και να το ξαναχρησιμοποιήσει αργότερα. Αλλά αυτό δεν είναι το μόνο πλεονέκτημα του TPM. Το TPM παρέχει μια ολόκληρη σουίτα κρυπτογραφικών εργαλείων, μερικά εκ των οποίο αναφέρθηκαν παραπάνω [9].

Τα δομικά εργαλεία του TPM καθορίζονται από την TCG και φαίνονται στην παρακάτω εικόνα [12]:



Εικόνα 8: Η Αρχιτεκτονική του TPM

4.2.1 I/O Buffer

Το I/O Buffer είναι η περιοχή επικοινωνίας μεταξύ του TPM και του συστήματος του κεντρικού υπολογιστή. Το σύστημα τοποθετεί δεδομένα εντολών στο I/O buffer και ανακτά δεδομένα απόκρισης από το buffer. Σύμφωνα με την προδιαγραφή του TPM το I/O Buffer δεν απαιτείται να είναι απομονωμένο από τα άλλα μέρη του συστήματος. Μπορεί να είναι μία κοινή μνήμη. Ωστόσο, όταν ξεκινάει η επεξεργασία μιας εντολής, η

εφαρμογή πρέπει να διασφαλίσει ότι το TPM χρησιμοποιεί τις σωστές τιμές. Για παράδειγμα, εαν το TPM εκτελεί κατακερματισμό των δεδομένων εντολών ως μέρος της διαδικασίας εξουσιοδότησης, θα πρέπει να προστατεύσει τα επικυρωμένα δεδομένα εντολών από τροποποίηση. Δηλαδή, πριν από την επικύρωση των δεδομένων, απαιτείται προστασία από τροποποίηση. Πριν τα δεδομένα τροποποιηθούν, πρέπει να βρίσκονται σε προστατευμένη τοποθεσία.

4.2.2 Υποσύστημα κρυπτογραφίας

Στο υποσύστημα κρυπτογραφίας εφαρμόζονται όλες οι κρυπτογραφικές συναρτήσεις του TPM. Μπορεί να καλείται από την ενότητα ανάλυσης εντολών (Command Parshing Module), το υποσύστημα εξουσιοδότησης (Authorization Subsystem) ή την ενότητα εκτέλεσης εντολών (Command Execution Module). Το TPM χρησιμοποιεί συμβατικές κρυπτογραφικές λειτουργίες με συμβατικούς τρόπους. Αυτές οι λειτουργίες περιλαμβάνουν:

- Συναρτήσεις κατακερματισμού.
- Ασύμμετρη κρυπτογράφηση και αποκρυπτογράφηση.
- Ασύμμετρη υπογραφή και επαλήθευση υπογραφής.
- Συμμετρική κρυπτογράφηση και αποκρυπτογράφηση.
- Συμμετρική υπογραφή (HMAC) και επαλήθευση υπογραφής.
- Δημιουργία κλειδιών.

Hash Engine

Οι συναρτήσεις κατακερματισμού μπορούν να χρησιμοποιηθούν απευθείας από εξωτερικό λογισμικό ή ως συνέπεια πολλών λειτουργιών TPM. Το TPM χρησιμοποιεί κατακερματισμό για να παρέχει έλεγχο ακεραιότητας και έλεγχο ταυτότητας όπως επίσης και μονόδρομες συναρτήσεις. Ένα TPM πρέπει να εφαρμόσει έναν εγκεκριμένο αλγόριθμο κατακερματισμού που έχει περίπου την ίδια ισχύ ασφαλείας με τον ισχυρότερο ασύμμετρο αλγόριθμό του.

Μια συνάρτηση κατακερματισμού συμβολίζεται με $H_{algorithm}()$, όπου ο δείκτης algorithm υποδεικνύει τον αλγόριθμο κατακερματισμού ή την παράμετρο που περιέχει το αναγνωριστικό του αλγορίθμου κατακερματισμού. Σε ορισμένες περιπτώσεις, ο δείκτης αλγορίθμου λείπει, οπότε ο αλγόριθμος θα καθορίζεται από το περιεχόμενο. Η ενότητα Command Dispatch θα χρησιμοποιήσει τη συνάρτηση κατακερματισμού κατά την επικύρωση ορισμένων τύπων εξουσιοδοτήσεων. Οι συναρτήσεις κατακερματισμού χρησιμοποιούνται επίσης για την υποστήριξη άλλων λειτουργιών στο TPM όπως το PCR Extend.

Asymmetric Engine

Ένα TPM χρησιμοποιεί ασύμμετρους αλγόριθμους για πιστοποίηση, αναγνώριση και κοινή χρήση μυστικών. Ένα TPM μπορεί να υποστηρίξει οποιονδήποτε ασύμμετρο

αλγόριθμο στον οποίο η TCG έχει εκχωρήσει ένα αναγνωριστικό. Ένα ασύμμετρο αναγνωριστικό αλγορίθμου θα δείξει μια οικογένεια αλγορίθμων και μεθόδων που χρησιμοποιούνται με αυτόν τον αλγόριθμο. Επί του παρόντος, οι μόνοι υποστηριζόμενοι ασύμμετροι αλγόριθμοι είναι ο RSA και το ECC χρησιμοποιώντας βασικές καμπύλες. Ένα TPM απαιτείται να εφαρμόζει τουλάχιστον έναν ασύμμετρο αλγόριθμο.

Symmetric Engine

Το TPM χρησιμοποιεί συμμετρική κρυπτογράφηση για να κρυπτογραφήσει ορισμένες παραμέτρους εντολών (συνήθως πληροφορίες ελέγχου ταυτότητας) και για κρυπτογράφηση προστατευμένων αντικειμένων που είναι αποθηκευμένα εκτός αυτής. Η λειτουργία Cipher Feedback (CFB) είναι η μόνη λειτουργία κρυπτογράφησης μπλοκ που απαιτείται από αυτήν την προδιαγραφή.

Κάθε συμμετρική κρυπτογράφηση μπλοκ που υποστηρίζεται από ένα TPM μπορεί να χρησιμοποιηθεί για κρυπτογράφηση παραμέτρων. Ωστόσο, δεν επιτρέπεται η χρήση αδύναμων κλειδιών. Επιπλέον, ένα TPM θα πρέπει να υποστηρίζει τη μέθοδο XOR, η οποία είναι βασισμένη σε κρυπτογράφηση ροής. Η XOR μπορεί να χρησιμοποιηθεί μόνο για εμπιστευτική διέλευση παραμέτρων.

Όταν συνδυάζεται με ασύμμετρο κλειδί (όπως σε ένα κλειδί αποκρυπτογράφησης ECC) ένα συμμετρικό κλειδί απαιτείται να έχει το ίδιο επίπεδο ασφαλείας με το ασύμμετρο κλειδί με το οποίο είναι συνδεδεμένο. Όταν χρησιμοποιείται συμμετρικό κλειδί για κρυπτογράφηση δεδομένων, τα κρυπτογραφημένα δεδομένα έχουν έναν αλγόριθμο HMAC. Ο HMAC ελέγχεται πριν από την αποκρυπτογράφηση των δεδομένων. Η επαλήθευση ότι τα αποκρυπτογραφημένα δεδομένα σχετίζονται σωστά με το συμμετρικό κλειδί προορίζεται κάνει πιο δύσκολη την ανάλυση ισχύος.

Key Generation

Η δημιουργία κλειδιών παράγει δύο διαφορετικούς τύπους κλειδιών. Το πρώτο, ένα συνηθισμένο κλειδί, παράγεται χρησιμοποιώντας τη γεννήτρια τυχαίων αριθμών (RNG) για τον υπολογισμό. Το αποτέλεσμα του υπολογισμού είναι ένα μυστικό κλειδί τιμή που διατηρείται σε προστατευμένη τοποθεσία. Ο δεύτερος τύπος, ένα πρωτεύον κλειδί, προέρχεται από μια τιμή, όχι από το RNG άμεσα. Το RNG συνήθως δημιουργεί αυτή την τιμή που είναι μόνιμα αποθηκευμένη στο TPM. Η δημιουργία ενός πρωτεύοντος κλειδιού από μία τιμή είναι με βάση τη χρήση μιας εγκεκριμένης λειτουργίας παράδοσης κλειδιών (Key Derivation Function - KDF).

Η προδιαγραφή του TPM 2.0 δεν θέτει κανένα ανώτατο όριο στο χρόνο που επιτρέπεται να δημιουργήσει ένα κλειδί. Ο χρόνος για την δημιουργία κλειδιών ενδέχεται να περιοριστεί από τις προδιαγραφές της πλατφόρμας. Ανάλογα με την εφαρμογή, το TPM μπορεί να δημιουργήσει ένα κλειδί με τη χρήση bits από το RNG ή αντλώντας το κλειδί από μια άλλη μυστική τιμή.

Random Number Generator (RNG)

Το RNG είναι η πηγή τυχαιότητας στο TPM. Το TPM χρησιμοποιεί τυχαίες τιμές για τη δημιουργία κλειδιών και για τυχαιότητα στις υπογραφές. Το RNG είναι μια Προστατευόμενη Ικανότητα του TPM χωρίς έλεγχο πρόσβασης και αποτελείται από:

- Μία πηγή εντροπίας και έναν συλλέκτη
- Έναν καταχωρητή κατάστασης
- Μία λειτουργία ανάμειξης (συνήθως, μια εγκεκριμένη λειτουργία κατακερματισμού).

Ο συλλέκτης εντροπίας συλλέγει εντροπία από πηγές εντροπίας και αφαιρεί την προκατάληψη. Η συγκεντρωμένη εντροπία χρησιμοποιείται στη συνέχεια για την ενημέρωση του καταχωρητή κατάστασης παρέχοντας είσοδο στη λειτουργία ανάμειξης για να παράγει τυχαίους αριθμούς.

Η λειτουργία ανάμειξης μπορεί να υλοποιηθεί με μια ψευδο-τυχαία γεννήτρια αριθμών (Pseudo-Random Number Generator - PRNG). Ένας PRNG μπορεί να παράγει αριθμούς που είναι προφανώς τυχαίοι από μια μη τυχαία είσοδο (όπως, ένας μετρητής). Ο συνδυασμός ενός εγκεκριμένου PRNG με μια είσοδο που έχει πολύ μεγαλύτερη εντροπία από έναν μετρητή αποδίδει έναν RNG με ιδιότητες όχι χειρότερες από τον υποκείμενο PRNG και πιθανώς πολύ καλύτερες. Ο RNG πρέπει να πληροί τις απαιτήσεις πιστοποίησης της προβλεπόμενης αγοράς. Το TPM πρέπει να παρέχει επαρκή τυχαιότητα για κάθε χρήση από μια εσωτερική λειτουργία. Κατά την πρόσβαση από μια εξωτερική κλήση, θα πρέπει να μπορεί να παρέχει 32 οκτάδες τυχαιότητας. Μεγαλύτερα αιτήματα ενδέχεται να αποτύχουν εάν δεν υπάρχει επαρκής τυχαιότητα. Κάθε πρόσβαση RNG παράγει μια νέα τιμή ανεξάρτητα από τη χρήση των δεδομένων. Δεν υπάρχει διάκριση μεταξύ της πρόσβασης για εσωτερικούς και της πρόσβασης για εξωτερικούς σκοπούς.

4.2.3 Υποσύστημα εξουσιοδότησης

Το υποσύστημα εξουσιοδότησης καλείται από τη μονάδα Command Dispatch στην αρχή και στο τέλος της εκτέλεσης εντολών. Πριν από την εκτέλεση της εντολής, το υποσύστημα εξουσιοδότησης ελέγχει ότι παρέχεται κατάλληλη εξουσιοδότηση για χρήση καθεμιάς από τις προστατευμένες τοποθεσίες. Ορισμένες εντολές έχουν πρόσβαση σε προστατευμένες τοποθεσίες που δεν απαιτούν εξουσιοδότηση. Η πρόσβαση σε ορισμένες τοποθεσίες μπορεί να απαιτεί εξουσιοδότηση ενός παράγοντα και η πρόσβαση σε άλλες προστατευμένες τοποθεσίες ενδέχεται να απαιτεί τη χρήση μιας πολιτική έγκρισης. Οι μόνες κρυπτογραφικές συναρτήσεις που απαιτούνται από το υποσύστημα εξουσιοδότησης είναι ο κατακερματισμός και η HMAC. Εάν εφαρμοστεί το TPM2_PolicySigned () ενδέχεται να απαιτηθεί ένας ασύμμετρος αλγόριθμος.

4.2.4 Random Access Memory (RAM)

Η μνήμη τυχαίας προσπέλασης (RAM) κρατά προσωρινά δεδομένα TPM. Τα δεδομένα στη μνήμη RAM του TPM ενδέχεται να χαθούν όταν αφαιρεθεί η ισχύς TPM. Επειδή ενδέχεται να χαθούν οι τιμές στη μνήμη RAM στις προδιαγραφές αναφέρεται ως volatile memory, ακόμη και αν η απώλεια δεδομένων εξαρτάται από την εφαρμογή. Οι τιμές στη μνήμη TPM του RAM δεν είναι όλες σε προστατευμένες τοποθεσίες. Ένα τμήμα της μνήμης RAM του TPM περιέχει το I/O Buffer με ιδιότητες που αναφέρθηκαν προηγουμένως.

4.2.5 Non-Volatile (NV) Memory

Η μονάδα της μνήμης NV αποθηκεύει τη μόνιμη κατάσταση που σχετίζεται με το TPM. Ένα μέρος της μνήμης NV είναι διαθέσιμο για κατανομή και χρήση από την πλατφόρμα και οντότητες εξουσιοδοτημένες από τον κάτοχο του TPM. Η μνήμη NV περιέχει προστατευμένες τοποθεσίες, οι οποίες είναι προσβάσιμες μόνο μέσω προστατευμένων δυνατότητων. Εάν η προδιαγραφή δεν είναι σαφής σχετικά με την αποθήκευση μιας παραμέτρου, αυτή η παράμετρος μπορεί να αποθηκευτεί είτε στη μνήμη RAM είτε στην NV, σύμφωνα με την προτίμηση του προμηθευτή. Εάν η μνήμη NV του TPM υποστεί κάποια φθορά, τότε το TPM θα πρέπει να ανιχνεύσει εάν τα δεδομένα που είναι γραμμένα σε μια τοποθεσία της μνήμης NV είναι τα ίδια με αυτα που είναι αποθηκευμένα αυτήν τη στιγμή και να μην εκτελέσει την εγγραφή στην NV εάν είναι τα ίδια. Το λειτουργικό σύστημα ή η πλατφόρμα μπορεί να ορίσει μια ειδική δομή δεδομένων NV (ένας δείκτης NV) για την αποθήκευση μόνιμων τιμών δεδομένων. Η μνήμη NV μπορεί επίσης να χρησιμοποιηθεί για την αποθήκευση ενός φορτωμένου αντικειμένου. Όταν ένα αντικείμενο αναφέρεται σε μια εντολή TPM, το TPM μπορεί να μετακινήσει αυτό το αντικείμενο σε μια υποδοχή αντικειμένου, ώστε η πρόσβαση να είναι πιο αποτελεσματική. Το TPM πρέπει να διασφαλίσει ότι διατίθεται επαρκής μνήμη μνήμης RAM για να επιτρέψει αυτή την κίνηση.

4.2.6 Power Detection

Αυτή η ενότητα διαχειρίζεται τις καταστάσεις ισχύος του TPM σε συνδυασμό με τις καταστάσεις ισχύος πλατφόρμας. Όλες οι προδιαγραφές του TCG που ορίζουν τη σύνδεση του TPM με κάποια πλατφόρμα θα πρέπει να περιλαμβάνουν την απαίτηση να ενημερώνεται το TPM για όλες τις αλλαγές της κατάστασης της ισχύος. Το TPM υποστηρίζει μόνο τις καταστάσεις λειτουργίας ON και OFF.

4.2.7 Execution Engine

Το TPM έχει μία μηχανή εκτέλεσης του κώδικα των προγραμμάτων που χρησιμοποιεί. Η μηχανή αυτή ανταποκρίνεται σε εξωτερικές εντολές επιλέγοντας τον κώδικα του απαιτούμενου προγράμματος και εκτελώντας τον στο TPM.

4.3 TPM Services

Όπως αναφέρθηκε και παραπάνω το TPM παρέχει βασικές υπηρεσίες ασφάλειας. Θεμέλιο για την παροχή αυτών των υπηρεσιών είναι η έννοια της «ρίζας εμπιστοσύνης» (roots of trust) από την οποία μπορούν να κατασκευαστούν και οι άλλες υπηρεσίες, όπως η πιστοποιημένη εκκίνηση (authenticated boot), η ασφαλής αποθήκευση (secure storage) και η επιβεβαίωση (attestation).

4.3.1 Roots of Trust

Μία αξιόπιστη πλατφόρμα, όπως το TPM, έχει ως θεμέλιο κάποιο αξιόπιστο στοιχείο. Δεδομένου ότι η εμπιστοσύνη που παρέχει η πλατφόρμα είναι χτισμένη πάνω σε αυτό το στοιχείο, είναι γνωστό ως Root of Trust. Το στοιχείο αυτό είναι ανάλογο με τις αρχές πιστοποίησης (Certificate Authorities - CA) σε μία υποδομή δημοσίου κλειδιού (Public Key Infrastructure - PKI). Παρόλο που οι χρήστες ενδέχεται να μην εμπιστεύονται το δημόσιο κλειδί που παρουσιάζεται σε ένα πιστοποιητικό ή ακόμη και την αρχή που υπέγραψε το πιστοποιητικό, αρκεί να υπάρχει κάποιος στην κορυφή της αλυσίδας πιστοποιητικών που εμπιστεύεται ο χρήστης. Η οντότητα στην κορυφή της αλυσίδας πιστοποιητικών αναφέρεται συχνά ως root CA και τα πιστοποιητικά που εκδίδει ως root Certificates. Στα περισσότερα προγράμματα περιήγησης ιστού, είναι εγκατεστημένα μαζί με την εφαρμογή πολλά root Certificates, τα οποία εμπιστεύονται οι χρήστες. Αποτυχία αυτού του μηχανισμού σπάει την πολιτική ασφαλείας του PKI. Στην αρχιτεκτονική του TPM, που ορίζεται από την TCG, υπάρχουν τρία root of trust: ένα Root of Trust for Measurement (RTM), ένα Root of Trust for Storage (RTS) και ένα Root of Trust for Reporting (RTR).

Το Root of Trust for Measurement (RTM) δημιουργεί μετρήσεις για τις διαδικασίες που εκτελούνται στην πλατφόρμα. Αυτό πρέπει ιδανικά να είναι ένα αξιόπιστο στοιχείο που ξεκινά πολύ νωρίς κατά τη διαδικασία εκκίνησης και ως εκ τούτου είναι σε θέση να παράγει μετρήσεις για όλα τα άλλα στοιχεία που φορτώνονται μετά από αυτό. Το TPM αποτελεί ιδανικό υποψήφιο για να είναι το Core Root of Trust Measurement (CRTM), αλλά στην πράξη το CRTM υλοποιείται στο BIOS. Το Root of Trust for Storage (RTS) είναι ένα αξιόπιστο στοιχείο που παρέχει εμπιστευτικότητα και ακεραιότητα. Το RTS είναι αξιόπιστο για την αποθήκευση είτε δεδομένων είτε κλειδιών. Επειδή το TPM αποτρέπει την μη εξουσιοδοτημένη πρόσβαση στη μνήμη του, μπορεί να λειτουργήσει ως RTS. Τέλος, το Root of Trust for Reporting (RTR) είναι ένα αξιόπιστο στοιχείο που παράγει αναφορές για τυχόν μετρήσεις ακεραιότητας που μπορεί να έχουν γίνει. Το TPM μπορεί να λειτουργήσει και ως RTR.

4.3.2 Boot Process

Η πρωτη διαδικασία που λαμβάνει χώρα κατά την εκκίνηση του TPM είναι η εκκίνηση του BIOS ή του Trusted Boot Block (TBB), το οποίο περιλαμβάνει το CRTM. Το CRTM είναι ένα αξιόπιστο στοιχείο και η ακεραιότητά του δεν μετράται από οποιονδήποτε εξωτερικό

κώδικα, αλλά μπορεί να εκτελεί έναν αυτοέλεγχο της ακεραιότητας του. Το CRTM πρέπει να κάνει μετρήσεις στο BIOS πριν το φορτώσει. Μόλις το BIOS φορτώσει παίρνει τον έλεγχο και μετρά την ακεραιότητα του OS Loader. Στη συνέχεια, ο έλεγχος περνά στο OS Loader, το οποίο μετρά την ακεραιότητα του λειτουργικού συστήματος. Αυτή η διαδικασία συνεχίζεται μέχρι να εκτελεστεί ο κώδικας των εφαρμογών.

Οι μετρήσεις ακεραιότητας σε κάθε στάδιο πραγματοποιούνται δημιουργώντας μια σύνοψη SHA-1 του κώδικα που πρόκειται να φορτωθεί. Αυτή η σύνοψη αποθηκεύεται σε έναν από τους καταχωρητές PCR, οι οποίοι είναι αρχικοποιημένοι στο μηδέν. Κάθε νέα μέτρηση ακεραιότητας, ωστόσο, δεν αντικαθιστά απλώς την παλιά τιμή PCR. Η διαδικασία ενημέρωσης (ή επέκτασης) της τιμής PCR συνενώνει τα 20 bytes δεδομένων που διατηρούνται ήδη στο PCR με τα 20 bytes των νέων δεδομένων που προκύπτουν από τον κατακερματισμό του νέου κώδικα. Αυτά τα 40 bytes δεδομένων στη συνέχεια κατακερματίζονται ξανά με τη χρήση του αλγορίθμου SHA-1 και το αποτέλεσμα γραφεται στο αρχικό PCR. Σε ψευδοκώδικα: PCR *hash*(PCR *hash*(*newcode*)). Με αυτόν τον τρόπο το PCR μπορεί να αποθηκεύσει απεριόριστο αριθμό μετρήσεων.

Για να ερμηνευτεί η τιμή που περιέχεται στο PCR, είναι απαραίτητο να γνωρίζει κανείς τις ατομικές συνόψεις που έχουν προστεθεί σε αυτή. Αυτά τα δεδομένα αποθηκεύονται εξωτερικά στο σημείο που αναφέρεται από την TCG ως Stored Measurement Log. Έτσι, εάν τα δεδομένα στο Stored Measurement Log είναι γνωστά και οι τιμές PCR είναι γνωστές και αξιόπιστες, μπορεί να επαληθευτεί η κατάσταση της πλατφόρμας.

4.3.3 Secure Storage

Κατά την διαδικασία ανάληψης ιδιοκτησίας δημιουργείται ένα Storage Root Key ή SRK. Αυτό το κλειδί δημιουργείται από το TPM και δεν φεύγει ποτέ από τη συσκευή. Η πρόσβαση σε αυτό είναι δυνατή μόνο με την επίδειξη γνώσης ενός κοινόχρηστου κωδικού, που σε αυτήν την περίπτωση είναι τα δεδομένα εξουσιοδότησης SRK (SRK authorisation data) . Αυτός ο κοινός κωδικός είναι παρόμοιος με τα δεδομένα εξουσιοδότησης του κατόχου και φορτώνονται ταυτόχρονα στο TPM, κατά τη διάρκεια της διαδικασία ανάληψης ιδιοκτησίας. Όπως και με τα δεδομένα εξουσιοδότησης κατόχου, τα δεδομένα εξουσιοδότησης SRK κρυπτογραφούνται από το κλειδί έγκρισης πριν σταλούν στο TPM.

Το SRK σχηματίζει τη ρίζα μιας βασικής ιεραρχίας κλειδιών. Αυτή η βασική ιεραρχία κλειδιών επιτρέπει τα δεδομένα ή τα κλειδιά, που είναι κρυπτογραφημένα, να μπορούν να αποκρυπτογραφηθούν μόνο με πρόσβαση στο TPM. Τα δεδομένα κρυπτογραφούνται κάτω από ένα συγκεκριμένο κλειδί αποθήκευσης. Το κλειδί αποθήκευσης είναι επίσης κρυπτογραφημένο και αποθηκεύεται εκτός του TPM. Για πρόσβαση σε αυτά τα δεδομένα το κρυπτογραφημένο κλειδί αποθήκευσης φορτώνεται στο TPM, μέσω του διαχειριστή προσωρινής μνήμης κλειδιών, και αποκρυπτογραφούνται από το κλειδί ρίζα. Δεδομένου ότι το SRK δεν αφήνει ποτέ το TPM, και ότι το TPM είναι φυσικά συνδεδεμένο με μια

αξιόπιστη πλατφόρμα, τα δεδομένα μπορούν να αποκρυπτογραφηθούν μόνο σε αυτή την πλατφόρμα.

Το TPM παρέχει δύο μηχανισμούς για ασφαλή αποθήκευση: binding και sealing. Η λειτουργία binding κρυπτογραφεί τα δεδομένα χρησιμοποιώντας ένα κλειδί που διαχειρίζεται ένα συγκεκριμένο TPM όπως περιγράφεται παραπάνω. Η λειτουργία sealing προστίθεται σε αυτό επιτρέποντας μόνο τη διαδικασία αποκρυπτογράφησης να προχωρήσει μόνο εάν η πλατφόρμα βρίσκεται σε συγκεκριμένη διαμόρφωση. Αυτή η διαμόρφωση καθορίζεται από δεδομένα που διατηρούνται στους καταχωρητές PCR. Έτσι, όταν τα δεδομένα είναι σφραγισμένα, όχι μόνο πρέπει να χρησιμοποιείται η ίδια πλατφόρμα για την αποσφράγιση των δεδομένων, αλλά και αυτή η πλατφόρμα πρέπει να είναι σε μια προκαθορισμένη διαμόρφωση πριν από την ανάκτηση τους.

4.3.4 Attestation

Τα κλειδιά AIK (Attestation Identity Keys) παρέχουν το απόρρητο του χρήστη όταν αυτός επικοινωνεί με διαφορετικές πηγές. Αν και το Endorsement Key (EK) μπορεί να χρησιμοποιηθεί για την ασφάλεια των επικοινωνιών με διαφορετικές πηγές, δεδομένου ότι το EK είναι μοναδικό για το TPM, αυτό θα μπορούσε ενδεχομένως να επιτρέψει να συνδεθεί η ταυτότητας της πλατφόρμας με κάθε πηγή που επιλέγει να επικοινωνήσει. Η ιδέα των AIK είναι να παρέχει μια μοναδική ταυτότητα για το TPM, για χρήση με κάθε διαφορετική πηγή. Σε κάθε περίπτωση, τα AIK λειτουργούν ως ψευδώνυμο για τα EK. Το διαπιστευτήριο AIK είναι ένα πιστοποιητικό που περιέχει το δημόσιο κλειδί AIK το οποίο αποδεικνύει ότι το αντίστοιχο ιδιωτικό κλειδί συνδέεται με ένα γνήσιο TPM. Αυτή η απόδειξη είναι εγγυημένη από μία υπογραφή στο διαπιστευτήριο που δημιουργήθηκε από ένα αξιόπιστο τρίτο μέρος γνωστό ως Αρχή Πιστοποίησης Απορρήτου.

Για να αποκτηθεί ένα AIK αποστέλλεται ένα αίτημα στην Αρχή Πιστοποίησης Απορρήτου μαζί με τα διαπιστευτήρια έγκρισης. Αυτή είναι η δεύτερη περίπτωση όπου εκτίθεται το δημόσιο EK. Τα διαπιστευτήρια έγκρισης αποδεικνύουν στην Αρχή Πιστοποίησης Απορρήτου ότι το αίτημα προήλθε από ένα γνήσιο TPM. Σε απάντηση στο αίτημα, η Αρχή Πιστοποίησης Απορρήτου δημιουργεί και υπογράφει τα διαπιστευτήρια AIK και τα κρυπτογραφεί κάτω από το δημόσιο EK που περιέχεται στα διαπιστευτήρια έγκρισης. Έτσι τα AIK δεσμεύονται κρυπτογραφικά στο TPM που περιέχει το ιδιωτικό EK.

Το TPM διαχειρίζεται το ιδιωτικό AIK κλειδί, το οποίο μπορεί να χρησιμοποιείται ελεύθερα για τη δημιουργία υπογραφών. Ειδικότερα, το ιδιωτικό AIK μπορεί να υπογράψει τα περιεχόμενα των καταχωρητών PCR. Έτσι μπορεί να χρησιμοποιηθεί το TPM για να επιβεβαιώσει την διαμόρφωση της πλατφόρμας.

5. RELATED WORK

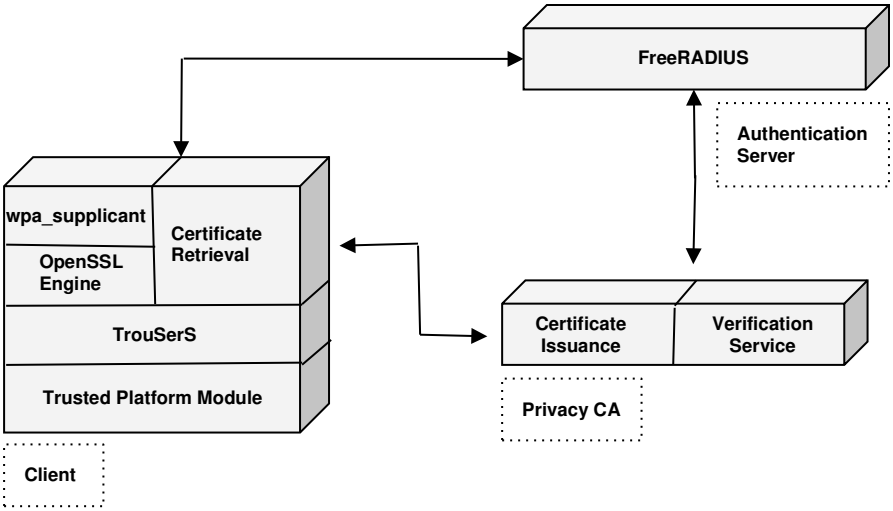
Σε αυτό το κεφάλαιο θα παρουσιαστεί η υλοποίηση του πρωτοκόλλου EAP-TPM στα πλαίσια προηγούμενων ερευνών και τα προβλήματα που αντιμετωπίστηκαν κατά την πρακτική εφαρμογή του.

5.1 EAP-TPM

Το 2007 οι Carolin Latze, Ulrich Ultes-Nitsche και Florian Baumgartner πρότειναν τη χρήση του TPM για την αυτόματη δημιουργία πιστοποιητικών, τα οποία θα χρησιμοποιούνται για την αυθεντικοποίηση των κόμβων σε ασύρματα δίκτυα. Η νέα αυτή μέθοδος του πρωτοκόλλου EAP ονομάστηκε EAP-TPM. Το EAP-TPM έχει ως στόχο να μετατρέψει ένα ασφαλές πρωτόκολλο αυθεντικοποίησης, όπως το EAP-TLS, σε ένα φιλικό προς το χρήστη πρωτόκολλο χωρίς να μειωθεί το επίπεδο ασφάλειας. Η ιδέα αυτού του πρωτοκόλλου προήλθε από τον τρόπο λειτουργίας των δικτύων GSM. Σε ένα GSM δίκτυο δεν υπάρχει η ανάγκη να ρυθμίσει οτιδήποτε ο χρήστης. Μπορεί με την αγορά ενός κινητού τηλεφώνου και μιας κάρτας SIM να συνδεθεί σε ένα GSM δίκτυο. Όταν κυκλοφόρησε το GSM, περιλάμβανε μία διαχείριση ταυτοτήτων και με βάση την ταυτότητα χρησιμοποιούνταν ένα πρωτόκολλο αυθεντικοποίησης σε κάθε συσκευή που είχε δυνατότητα σύνδεσης στο δίκτυο. Σε αντίθεση, όταν κυκλοφόρησε το πρότυπο 802.11, επικεντρωνόταν στην μετάδοση δεδομένων και όχι στη διαχείριση της ταυτότητας των χρηστών και στην αυθεντικοποίηση τους. Όλα τα πρωτόκολλα αυθεντικοποίησης που κυκλοφόρησαν αργότερα και χρησιμοποιούνται μέχρι σήμερα δεν μπορούν να συγκριθούν με το GSM. Με την εμφάνιση των TPMs, για πρώτη φορά υπάρχει ένα είδος ενσωματωμένου διακριτικού υλικού, που προσδιορίζει την ταυτότητα στον κόσμο των δικτύων υπολογιστών συγκρίσιμο με την κάρτα SIM των δικτύων GSM [19].

5.1.1 Η αρχιτεκτονική του συστήματος

Για την εφαρμογή της παραπάνω ιδέας χρησιμοποιήθηκε ένα σύστημα αποτελούμενο από τρία στοιχεία: έναν client, έναν authentication server και μία privacy CA [20]. Ο client είναι αυτός που θέλει να αυθεντικοποιηθεί στο δίκτυο, ο authentication server αυθεντικοποιεί τον client και η privacy CA είναι η αρχή που εκδίδει τα πιστοποιητικά και παρέχει την υπηρεσία επαλήθευσης. Ο client θα πρέπει να ζητήσει νέα ταυτότητα πριν συνδεθεί στο ασφαλές EAP-TPM δίκτυο. Μετά από αυτό ξεκινάει η διαδικασία της αυθεντικοποίησης με τον authentication server. Κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης ο server θα πρέπει να επαληθεύσει το πιστοποιητικό του client. Δεδομένου ότι τα πιστοποιητικά του TPM είναι ελαφρώς διαφορετικά από τα X.509 πιστοποιητικά, θα πρέπει να υπάρξει μία υπηρεσία επαλήθευσης, η οποία θα κάνει τη δουλειά για τον EAP-TLS authenticator.



Εικόνα 9: Η αρχιτεκτονική του προτεινόμενου συστήματος

Η έκδοση TPM που χρησιμοποιήθηκε στο σενάριο που θα αναλυθεί παρακάτω ήταν το TPM 1.2. Όπως αναφέρθηκε και σε προηγούμενα κεφάλαια το TPM είναι ένα κομμάτι υλικού, που συνήθως συνδέεται με την μητρική κάρτα, παρέχοντας κρυπτογραφικές συναρτήσεις και ασφαλή αποθήκευση κλειδιών. Επιπλέον το TPM μπορεί να χρησιμοποιηθεί για τη συλλογή μετρήσεων που σχετίζονται με την ακεραιότητα ενός μηχανήματος. Μία ακόμα λειτουργία του είναι η ασφαλής σύνδεση σε ένα δίκτυο. Ένας client που συνδέεται σε έναν συγκεκριμένο server μπορεί να ζητήσει τις μετρήσεις που συνδέονται με την ακεραιότητα του μηχανήματος από το TPM που είναι ενσωματωμένο σε αυτόν, ώστε να αποφασίσει εάν ο συγκεκριμένος server είναι έμπιστος. Την ίδια διαδικασία μπορεί να επαναλάβει με τη σειρά του και ο server για την ακεραιότητα του client. Το TPM παρουσιάζει και κάποια ακόμα ενδιαφέροντα χαρακτηριστικά, τα οποία οδήγησαν στην ιδέα για υλοποίηση του πρωτοκόλλου EAP-TPM. Για παράδειγμα έχει τη δυνατότητα να ταυτοποιείται μοναδικά και για αυτό το λόγο περιλαμβάνει ένα ζεύγος κλειδιών που ονομάζονται endorsement key pair, από το οποίο το ιδιωτικό κλειδί δεν αποκαλύπτεται ποτέ. Κάθε TPM έχει ενσωματωμένα κάποια πιστοποιητικά τα οποία αποδεικνύουν ότι είναι λειτουργικό και έρχεται σε συμφωνία με τα standards. Σε περίπτωση που το TPM ζητήσει μια νέα ταυτότητα, στέλνει αυτά τα πιστοποιητικά σε συνδυασμό με το δημόσιο μέρος ενός RSA κλειδιού στην αρχή πιστοποίησης. Η αρχή πιστοποίησης ελέγχει στη συνέχεια αυτά τα πιστοποιητικά και εκδίδει τη νέα ταυτότητα. Επιπλέον υπάρχει πιθανότητα να περιλαμβάνονται σε αυτό το νέο πιστοποιητικό και μετρήσεις της ακεραιότητας της πλατφόρμας, ώστε να μπορεί να επαληθευτεί η κατάσταση εμπιστοσύνης της πλατφόρμας.

5.1.2 Υλοποίηση

Το TPM πρέπει να παρέχει αρκετές κρυπτογραφικές μεθόδους και προστατευμένη αποθήκευση. Αλλά πρέπει επίσης να είναι φθηνό στην κατασκευή ώστε να είναι μια ευρέως χρησιμοποιούμενη συσκευή. Για αυτό η TCG αποφάσισε τη διάκριση μεταξύ μεθόδων που πρέπει να εκτελούνται σε προστατευμένο περιβάλλον και εκείνων που

ενδέχεται να εκτελούνται σε περιβάλλον μόνο λογισμικού που ονομάζεται TCG Software Stack (TSS). Για το TCG Software Stack υπάρχουν ήδη πολλές υλοποιήσεις. Δεδομένου του περιορισμού, οτι οι εφαρμογές που χρειάζεται να τροποποιηθούν χρησιμοποιούν την γλώσσα προγραμματισμού C, χρησιμοποιήθηκε το TrouSerS [26], που αποτελεί τη μόνη εφαρμογή TSS που είναι ανοιχτού κώδικα και χρησιμοποιεί τη γλώσσα C. Το TrouSerS έρχεται με ένα μόνιμο αρχείο αποθήκευσης για την αποθήκευση ορισμένων μη κρίσιμων πληροφοριών στο σκληρό δίσκο προκειμένου να εξοικονομηθεί μνήμη στο TPM. Αυτό το αρχείο περιέχει για παράδειγμα πληροφορίες σχετικά με το αν χρειάζεται ένα κλειδί αυθεντικοποίηση ή όχι και μπορεί να περιέχει το δημόσιο τμήμα των κλειδιών, του οποίου το ιδιωτικό κλειδί βρίσκεται μέσα στο TPM.

Μετά τη δημιουργία ενός νέου RSA κλειδιού, το οποίο θα χρησιμοποιηθεί ως κλειδί ταυτότητας, το TSS πρέπει να συλλέξει όλες τις απαραίτητες πληροφορίες που χρειάζονται για να ζητήσει μια νέα ταυτότητα. Αυτές οι πληροφορίες περιλαμβάνουν: Τα διαπιστευτήρια έγκρισης, τα οποία προσδιορίζουν το TPM μοναδικά, τα διαπιστευτήρια συμμόρφωσης, το οποία υποδηλώνουν ότι το TPM είναι γνήσιο, τα διαπιστευτήρια πλατφόρμας, το οποία υποδηλώνουν ότι η πλατφόρμα είναι γνήσια και το δημόσιο τμήμα του κλειδιού ταυτότητας που δημιουργήθηκε πρόσφατα. Για την υλοποίηση της αρχής πιστοποίησης (Privacy CA) χρησιμοποιήθηκε μια online έκδοση που χαρτογραφεί απευθείας τις μεθόδους που χρησιμοποιεί ο client, οι οποίες παρέχονται από το TrouSers. Αφού επαληθευτούν όλα αυτά τα πιστοποιητικά και οι πληροφορίες δημοσίου κλειδιού, που στέλνονται από τον client, η PCA υπογράφει το πιστοποιητικό και το στέλνει πίσω στον client, ο οποίος μπορεί πλέον να το χρησιμοποιήσει.

Όπως αναφέρθηκε και παραπάνω η λειτουργία του TPM βασίζεται σε πιστοποιητικά. Το TPM περιλαμβάνει το Endorsement Key Pair, το οποίο δεν γνωστοποιείται και το ταυτοποιεί μοναδικά. Επιπλέον έχει τη δυνατότητα να υποστηρίξει διαφορετικές ταυτότητες για την υλοποίηση διαφορετικών σκοπών. Για παράδειγμα ο χρήστης μπορεί να χρησιμοποιήσει άλλη ταυτότητα για το e-banking και άλλη ταυτότητα για το online shopping. Αυτές οι ταυτότητες στην ουσία είναι X.509 πιστοποιητικά, τα οποία εκδίδονται από την PCA και δεν μπορούν να χρησιμοποιηθούν απευθείας στην διαδικασία της TLS αυθεντικοποίησης. Αυτό συμβαίνει γιατί το πιστοποιητικό που εκδίδεται κατά τη διαδικασία είναι ένα έγκυρο πιστοποιητικό X.509, αλλά το κλειδί, που ανήκει σε αυτό το πιστοποιητικό περιορίζεται σε απλή υπογραφή SHA-1. Παρόλο λοιπόν που αυτό ονομάζεται κλειδί ταυτότητας δεν μπορεί να χρησιμοποιηθεί για να υπογράψει ένα νέο X.509 πιστοποιητικό ή στην διαδικασία ενός TLS Handshake. Το πρόβλημα έγκειται στην επέκταση *basicContraint* του πιστοποιητικού ταυτότητας. Σύμφωνα με την TCG, η επέκταση πρέπει να οριστεί με την τιμή *CA:false*. Αυτό σημαίνει ότι δεν υπάρχει πιθανότητα να δημιουργηθεί ένα έγκυρο X.509 πιστοποιητικό κάτω από το πιστοποιητικό ταυτότητας. Αυτό οφείλεται στους περιορισμούς στους οποίους υπόκειται η δομή των πιστοποιητικών X.509. Για να χρησιμοποιηθούν τα κλειδιά πιστοποίησης στην TLS διαδικασία αυθεντικοποίησης θα πρέπει να μεταφερθεί το δημόσιο μέρος τους στον TLS server. Λόγω του ότι το πρότυπο TLS απαιτεί X.509 πιστοποιητικά, οι συγγραφείς αποφάσισαν να χρησιμοποιήσουν στην υλοποίηση τους ελαφρώς τροποποιημένα

πιστοποιητικά X.509. Το πρόβλημα ωστόσο που έπρεπε να αντιμετωπιστεί είναι ότι αυτά τα πιστοποιητικά δεν μπορούν να επαληθευτούν από υλοποιήσεις του προτύπου TLS, όπως είναι το OpenSSL. Για να ξεπεραστεί αυτό το πρόβλημα, προτάθηκε η χρήση μιας υπηρεσία επαλήθευσης που παρέχεται για παράδειγμα από την PCA με τον τρόπο που αναφέρεται παρακάτω.

Από την έκδοση 0.9.6 του OpenSSL προστέθηκε μία νέα λειτουργικότητα που ονομάζεται OpenSSL Engine και υλοποιείται σε επίπεδο υλικού ή λογισμικού προκειμένου να εκτελέσει κρυπτογραφικές λειτουργίες. Η λειτουργικότητα αυτή μπορεί για παράδειγμα να χρησιμοποιηθεί σε έξυπνες κάρτες. Το 2007 η IBM υλοποίησε αυτή τη λειτουργία και σε TPMs. Οι συγγραφείς χρησιμοποίησαν το OpenSSL TPM Engine [24] για την ενσωμάτωση του TPM στο wpa_supplicant [23], το οποίο αποτελεί εφαρμογή λογισμικού ανοιχτού κώδικα, που υποστηρίζει μία μεγάλη ποικιλία ενσύρματων και ασύρματων μεθόδων αυθεντικοποίησης, όπως το WEP, το WPA και το WPA2 καθώς και μεθόδους EAP.

Για την αυθεντικοποίηση χρησιμοποιήθηκε ως authentication server ο FreeRadius, ο οποίος είναι έργο ελεύθερου λογισμικού και υλοποιεί το πρωτόκολλο RADIUS. Το εν λόγω λογισμικό είναι γραμμένο στην γλώσσα προγραμματισμού C και είναι εύκολα επεκτάσιμο καθώς η κάθε μέθοδος αυθεντικοποίησης είναι ξεχωριστό module. Στην πρώτη προσπάθεια υλοποίησης του EAP-TPM χρησιμοποιήθηκαν ελαφρώς τροποποιημένα πιστοποιητικά X.509, τα οποία επέτρεπαν την χρήση της μεθόδου EAP-TLS με μικρές αλλαγές. Η μόνη αλλαγή που έπρεπε να γίνει ήταν στην επαλήθευση του πιστοποιητικού λόγω του ότι τα πιστοποιητικά του TPM δεν αποτελούν έγκυρα X.509 πιστοποιητικά. Για να μπορέσουν λοιπόν να επαληθευτούν αυτά τα πιστοποιητικά, η PCA θα έπρεπε να παρέχει μία υπηρεσία επαλήθευσης. Ο server FreeRadius επαληθεύει τα πιστοποιητικά του client χρησιμοποιώντας το OpenSSL. Σε περίπτωση που το OpenSSL δεν μπορεί να επαληθεύσει κάποιο πιστοποιητικό, ο server θα πρέπει να ανοίξει την προέκταση του πιστοποιητικού για να προσδιορίσει εάν είναι ένα πιστοποιητικό προερχόμενο από TPM η όχι. Στην περίπτωση που το πιστοποιητικό προέρχεται από ένα TPM, ο FreeRadius στέλνει τις προεκτάσεις που σχετίζονται με τα X.509 πιστοποιητικά στην υπηρεσία επαλήθευσης, η οποία απαντάει με SUCCESS ή FAILURE. Με βάση αυτή την απάντηση, ο FreeRadius αποφασίζει εαν θα αυθεντικοποιήσει τον client ή όχι. Προκειμένου να αποφευχθούν οι επιθέσεις κατά την διαδικασία της επαλήθευσης, ο FreeRadius επικοινωνεί με την υπηρεσία επαλήθευσης χρησιμοποιώντας αμοιβαία SSL αυθεντικοποίηση.

Σε μια έγκυρη υλοποίηση, ο client γνωρίζει την ακολουθία των πιστοποιητικών, η οποία είναι η εξής:

Πιστοποιητικό της PCA → Πιστοποιητικό ταυτότητας του client → Πιστοποιητικό του client που χρησιμοποιείται για αυθεντικοποίηση.

Όπως αναφέρθηκε παραπάνω, το πιστοποιητικό ταυτότητας περιέχει την τιμή CA:false, που υποδηλώνει, ότι αυτή η ακολουθία δεν είναι έγκυρη ακολουθία των X.509

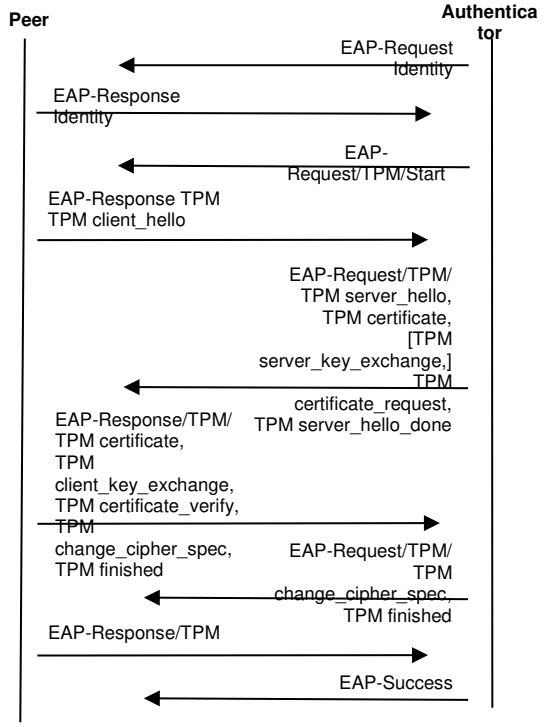
πιστοποιητικών. Το έγκυρο μέρος τελειώνει με το πιστοποιητικό ταυτότητας. Επιπλέον, σε μια έγκυρη υλοποίηση, ο client στέλνει ολόκληρη την ακολουθία στον server, ο οποίος στη συνέχεια μπορεί να επαληθεύσει εύκολα το πιστοποιητικό του client. Στην υλοποίηση που περιγράφεται ο πελάτης θα στείλει μόνο το τελευταίο πιστοποιητικό και όχι ολόκληρη την ακολουθία. Η PCA όμως γνωρίζει ολόκληρη την αλυσίδα. Αυτό σημαίνει ότι η εγκατάσταση της υπηρεσίας επαλήθευσης στην PCA λύνει το πρόβλημα. Για να είναι σε θέση η υπηρεσία επαλήθευσης να αντιστοιχίσει το πρώτο μέρος της ακολουθίας (Πιστοποιητικό της PCA → Πιστοποιητικό ταυτότητας του client) του πιστοποιητικού του client, θα πρέπει να γνωρίζει τον σειριακό αριθμό του εγκεκριμένου πιστοποιητικού ταυτότητας. Αυτός ο αριθμός θα σταλεί στις επεκτάσεις του client. Χρησιμοποιώντας αυτόν τον αριθμό και τις ειδικές επεκτάσεις του TPM, η PCA θα μπορεί να επαληθεύσει το πιστοποιητικό του client.

5.1.3 Αυθεντικοποίηση

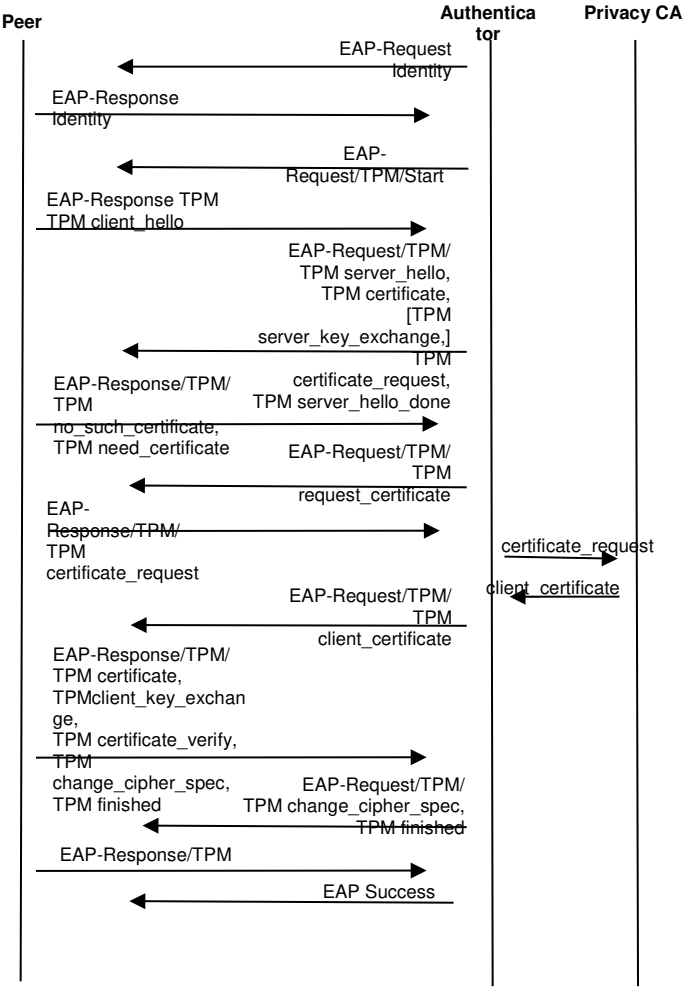
Η αυθεντικοποίηση στο πρωτόκολλο EAP-TPM είναι δύο ειδών: αυθεντικοποίηση με διαμόρφωση, όπου ο χρήστης πρέπει να ζητήσει τα πιστοποιητικά του προτού συνδεθεί με τον EAP-TPM authenticator και αυθεντικοποίηση με μηδενική διαμόρφωση, όπου ο χρήστης θα λάβει ένα πιστοποιητικό, χωρίς να κάνει κάποια ενέργεια ο ίδιος, κατά τη διαδικασία της αυθεντικοποίησης. Η πρώτη περίπτωση είναι κατάλληλη για χειριστές που χρησιμοποιούν λογιστική καταγραφή, καθώς με αυτό τον τρόπο είναι δυνατή η εγγραφή πιστοποιητικών σε χρήστες, ενώ η δεύτερη περίπτωση είναι κατάλληλη για εταιρικά περιβάλλοντα ή γενικά περιβάλλοντα που δεν χρησιμοποιούν λογιστική καταγραφή. Για να επεκταθεί το EAP-TPM σε ένα σχήμα μηδενικής διαμόρφωσης, πρέπει να υπάρχει κάποιου είδους αυτόματη ανάκτηση πιστοποιητικών κατά τη διάρκεια του TLS handshake.

Το EAP-TPM βασίζεται στο EAP-TLS και χρησιμοποιεί αμοιβαία αυθεντικοποίηση, αλλά από τη στιγμή που μόνο το TLS 1.2 κάνει χρήση των βασικών υπογραφών κατά την χειραψία , είναι δυνατόν να χρησιμοποιηθούν απευθείας πιστοποιητικά ταυτότητας στο EAP-TPM μόνο με τη χρήση της έκδοσης 1.2 του TLS ή υψηλότερης. Στην πρώτη περίπτωση της αυθεντικοποίησης με διαμόρφωση, δημιουργείται ένα πιστοποιημένο κλειδί για την TLS χειραψία χρησιμοποιώντας το πιστοποιητικό ταυτότητας. Μετά από αυτό πρέπει να δημιουργηθεί ένα self-signed πιστοποιητικό με τη χρήση του πιστοποιητικού ταυτότητας, το οποίο θα είναι το πιστοποιητικό του client. Προκειμένου να μπορέσει ο authentication server να πιστοποιήσει ότι ο client χρησιμοποιεί ένα έγκυρο πιστοποιητικό, το πιστοποιητικό ταυτότητας θα πρέπει να στέλνεται με την επέκταση των συμπληρωματικών δεδομένων. Αυτή η μέθοδος απαιτεί ο χρήστης να έχει ζητήσει ένα πιστοποιητικό ταυτότητας πριν συνδεθεί στο ασφαλές EAP-TPM δίκτυο. Η διαδικασία της αυθεντικοποίησης ξεκινάει με τον authenticator, ο οποίος ρωτάει τον client για την ταυτότητα στέλνοντας του ένα μήνυμα `EAP-Request/Identity`. Ο client απαντάει με ένα μήνυμα `EAP-Response/Identity`, στο οποίο περιλαμβάνεται το αναγνωριστικό της ταυτότητας δικτύου του (Network Address Identifier - NAI). Στη συνέχεια ο

authenticator στέλνει ένα μήνυμα `EAP-Request/TPM/Start` για να υποδείξει την πραγματική έναρξη της EAP-TPM συνομιλίας, η οποία θα ακολουθηθεί από μία κανονική TLS χειραψία. Στο τέλος η EAP αυθεντικοποίηση κλείνει με την αποστολή ενός `EAP-Response/TPM` μηνύματος από τον client και ενός `EAP-Success` μηνύματος από τον authenticator.



Εικόνα 10: Αυθεντικοποίηση με διαμόρφωση

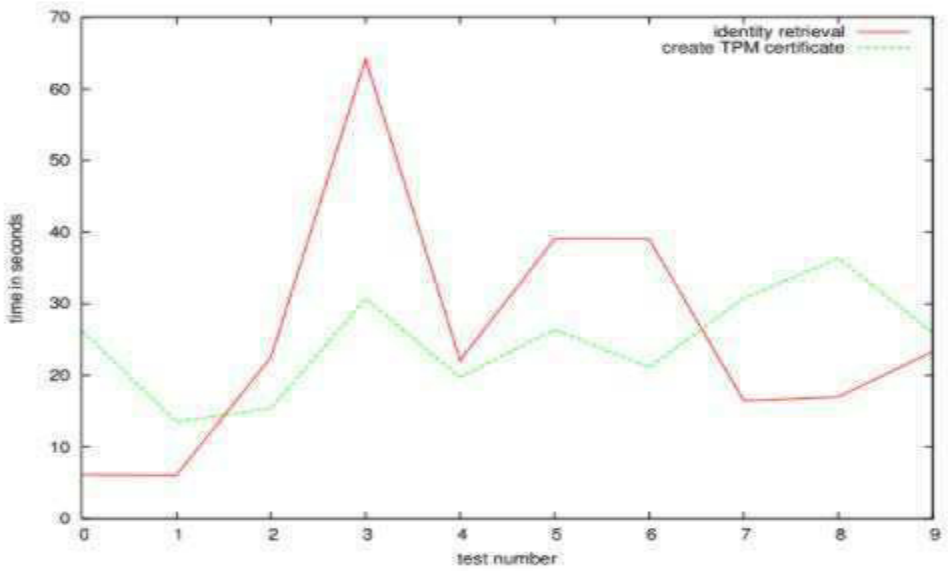


Εικόνα 11: Αυθεντικοποίηση με μηδενική διαμόρφωση

Πέραν της παραπάνω περίπτωσης υπάρχει και η διαδικασία της αυθεντικοποίησης χωρίς διαμόρφωση, κατά την οποία ο χρήστης παίρνει το πιστοποιητικό κατά την διάρκεια της πρώτης σύνδεσης. Η υλοποίηση της εν λόγω διαδικασίας προτάθηκε το 2009 από τους προαναφερόμενους συγγραφείς. Το EAP-TPM παρέχει ένα χαρακτηριστικό, το οποίο επιτρέπει στο χρήστη να ζητήσει το πιστοποιητικό ταυτότητας του κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης. Στο EAP-TPM με μηδενική διαμόρφωση, ο ελεγκτής πρέπει να καθορίσει τις αποδεκτές PCA εντός του πεδίου certificate_authorities στο μήνυμα certificate_request. Αφού λάβει τα μηνύματα EAP-Request/TPM, TPM server_hello, TPM certificate, [TPM server_key_exchange,] TPM certificate_request,

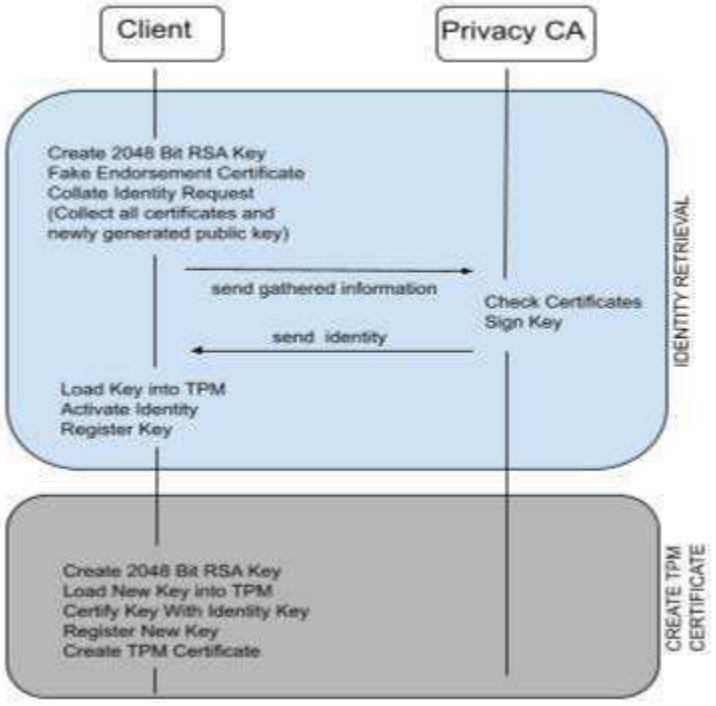
TPM server_hello_done, ο κόμβος πρέπει να ελέγξει αν έχει έγκυρο πιστοποιητικό από τις PCA που καθορίζονται στο TPM Certificate_request-> Certificate_authorities ή όχι. Σε περίπτωση που έχει κάποιο έγκυρο πιστοποιητικό, ο έλεγχος ταυτότητας συνεχίζεται. Σε αντίθετη περίπτωση, πρέπει να απαντήσει με EAP-Response/TPM/TPM no_such_certificate, TPM need_certificate, όπου το no_such_certificate είναι μια ειδοποίηση με προειδοποίηση επιπέδου (1) και περιγραφή no_certificate (41) [25]. Η απάντηση από τον διακομιστή περιλαμβάνει επίσης την επιθυμητή PCA προκειμένου να υπάρχει κάποιο είδος αναγνώρισης. Σε περίπτωση που η PCA που υπάρχει στην απάντηση δεν ταιριάζει με την ζητούμενη, ο client γνωρίζει ότι κάτι πήγε στραβά κατά τη διάρκεια του handshake και πρέπει να τερματιστεί η συνεδρία ελέγχου ταυτότητας. Σε περίπτωση που οι τιμές ταιριάζουν, ο client μπορεί να ζητήσει τη νέα του ταυτότητα στέλνοντας αίτημα ταυτότητας στην επιθυμητή PCA, η οποία στη συνέχεια εκδίδει μια νέα ταυτότητα. Στη συνέχεια, ο client πρέπει να δημιουργήσει ένα νέο ζεύγος κλειδιών RSA και να το πιστοποιήσει χρησιμοποιώντας τη νέα ταυτότητα. Η διαδικασία αυτή θα πρέπει να γίνει σε συγκεκριμένο χρονικό διάστημα.

Ο Server από την πλευρά του θα πρέπει να κάνει ανάλυση της κίνησης μεταξύ του client και της PCA. Αυτό συμβαίνει γιατί θα πρέπει να ξέρει πότε ο client λαμβάνει την νέα του ταυτότητα για να κλείσει τις πόρτες ξανά. Αφού κλείσει την σύνδεση πρέπει να ξεκινήσει ένα χρονόμετρο για όσο ο client δημιουργεί ένα νέο ζεύγος κλειδιών RSA και ένα νέο πιστοποιητικό TPM πριν συνεχίζει με το handshake. Εάν ο χρόνος ξεπεράσει ένα συγκεκριμένο όριο θα πρέπει να σταματήσει το handshake. Στην παρακάτω εικόνα φαίνεται ο χρόνος που χρειάζεται για να ζητηθεί ένα νέο πιστοποιητικό ταυτότητας από κάποια Αρχή Πιστοποίησης (κόκκινο χρώμα) και ο χρόνος που χρειάζεται για να δημιουργηθεί και να πιστοποιηθεί ένα νέο κλειδί χρησιμοποιώντας το πιστοποιητικό ταυτότητας (πράσινο χρώμα).



Εικόνα 12: Ο απαιτούμενος χρόνος για την δημιουργία ενός νέου πιστοποιητικού ταυτότητας

Ο χρόνος που απαιτείται για την δημιουργία ενός πιστοποιητικού TPM είναι περίπου στα 30 δευτερόλεπτα ενώ ο χρόνος για να ζητηθεί ένα νέο πιστοποιητικό ταυτότητας είναι μεγαλύτερος.



Εικόνα 13: Η διαδικασία δημιουργίας ενός πιστοποιητικού

Αυτό συμβαίνει γιατί στην δεύτερη περίπτωση στον χρόνο συμπεριλαμβάνεται ο χρόνος που απαιτείται για να συλλεχθούν όλες οι απαραίτητες πληροφορίες που θα σταλούν στην PCA και ο χρόνος που απαιτείται για να δημιουργηθεί ένα νέο κλειδί ταυτότητας. Επιπλέον η νέα ταυτότητα θα πρέπει να δηλωθεί στο TCG software stack προκειμένου να μπορεί να χρησιμοποιηθεί. Ο χρόνος που θα πρέπει να περιμένει ο Server πριν σταματήσει το handshake είναι τα 30 δευτερόλεπτα. Ωστόσο αυτός ο χρόνος υπάρχει πιθανότητα να επηρεαστεί και από παράγοντες όπως είναι τεχνικά προβλήματα στον client, που επηρεάζουν την δημιουργία του πιστοποιητικού ή άλλου είδους καθυστερήσεις στον client. Σε αυτές τις περιπτώσεις θα πρέπει να σταματήσει το TLS handshake και να ξεκινήσει ένα νέο αφού ολοκληρωθεί η παραγωγή του πιστοποιητικού.

5.1.4 Δοκιμή σε Πραγματικό Περιβάλλον

Το 2009 δόθηκε η δυνατότητα στους Carolin Latze, Ulrich Ultes-Nitsche και Josua Hiller να υλοποιήσουν για πρώτη φορά το EAP-TPM σε πραγματικό περιβάλλον και συγκεκριμένα στο δοκιμαστικό PWLAN της Swisscom [22]. Για την υλοποίηση χρησιμοποιήθηκε ένας FreeRADIUS ως authentication Server, ο οποίος ενσωματώθηκε στην υποδομή του PWLAN. Από την πλευρά του client χρησιμοποιήθηκε ως peer ο wpa_supplicant και η GnuTLS ως βιβλιοθήκη του SSL, καθώς η πιο δημοφιλής

βιβλιοθήκη (OpenSSL) δεν υποστήριζε ακόμα το TLS 1.2. Μία από τις προκλήσεις λοιπόν ήταν η εφαρμογή ενός module στον FreeRADIUS που να χρησιμοποιεί την βιβλιοθήκη.

Σκοπός της διαδικασίας ήταν να παρουσιαστεί η διαδικασία απόκτησης νέας ταυτότητας και να αποδειχθεί πόσο εύκολη διαδικασία είναι ακόμα και για άπειρους χρήστες. Επιπλέον παρουσιάστηκε όλη η διαδικασία αυθεντικοποίησης με λεπτομέρειες και περιγράφηκε πόσο εύκολη είναι η διαδικασία ανάπτυξης του EAP-TPM σε μία υπάρχουσα υποδομή PWLAN. Για να υλοποιηθούν όλα αυτά χρησιμοποιήθηκαν 2 notebooks, τα όποια το ένα αναπαριστούσε τον peer και το άλλο την Αρχή Πιστοποίησης. Επιπλέον χρησιμοποιήθηκε και ένα access point το οποίο συνδέθηκε μέσω VPN στο PWLAN. Ο Χρόνος που χρειάστηκε για να γίνει η απαραίτητη παραμετροποίηση του εξοπλισμού ήταν λιγότερο από μία ώρα.

5.2 EAP-TPM στην Ασφάλεια Ασύρματων Δικτύων Πόλεων

Το 2008 οι Y. Chen, A. Studer and A. Perrig δημοσίευσαν ένα paper στο οποίο παρουσιάζουν μία παραλλαγή του πρωτοκόλλου TLS, το οποίο αξιοποιεί τις δυνατότητες του TPM για την αυθεντικοποίηση των χρηστών και των συσκευών σε ασύρματα δίκτυα πόλεων. Στην έρευνα τους προτάθηκαν δύο παραλλαγές του πρωτοκόλλου, στην πρώτη γίνεται χρήση του TPM attestation και στην δεύτερη του TPM sealed storage [27].

5.2.1 Απειλές

Λόγω της φύσης των ασύρματων δικτύων πόλεων είναι πολύ εύκολο να γίνουν στόχοι κακόβουλων χρηστών. Οι πιθανές απειλές που μπορούν να δεχτούν τέτοιου είδους δίκτυα είναι συνοπτικά:

- Απόκτηση κωδικών χρηστών.
- Κλοπή συσκευών.
- Εγκατάσταση κακόβουλου λογισμικού στις συσκευές.
- Κακόβουλοι χρήστες που θέλουν δωρεάν πρόσβαση στο ασύρματο δίκτυο.
- Κακόβουλοι χρήστες που σκανάρουν την κίνηση του δικτύου και εισάγουν σε αυτό κακόβουλα πακέτα.

Για την αντιμετώπιση λοιπόν αυτού του προβλήματος προτάθηκαν δύο λύσεις που περιλαμβάνουν την τροποποίηση του πρωτοκόλλου EAP-TLS με την προσθήκη των λειτουργιών του TPM. Και στις δύο περιπτώσεις η αυθεντικοποίηση του χρήστη γίνεται με έναν κωδικό και η αυθεντικοποίηση της συσκευής με ψηφιακή υπογραφή. Στην πρώτη μορφή του πρωτοκόλλου η TPM attestation function χρησιμοποιείται για να υπογράψει την κατακερματισμένη έκδοση της ταυτότητας του χρήστη και του κωδικού του . Στην δεύτερη μορφή του πρωτοκόλλου χρησιμοποιείται το TPM sealed storage ώστε μόνο κάποιος χρήστης με κατάλληλο ζεύγος κωδικού και ταυτότητας να μπορεί να λάβει το ιδιωτικό κλειδί για να συνεχίσει την χειραψία TLS

5.2.2 EAP-TLS with TPM Attestation Based Device and User Authentication

Στην μία περίπτωση της υλοποίησης αξιοποιούνται οι δυνατότητες του TPM για τον συνδυασμο της υπογραφής που περιλαμβάνεται σε ένα μήνυμα μιας χειραψίας με τα δεδομένα μιας συσκευής. Κατά τη διάρκεια της συνεδρίας, το TPM attestation key χρησιμοποιείται για την υπογραφή τροποποιημένου CCF μηνύματος που περιέχει πληροφορίες για τον χρήστη (ταυτότητα, κωδικός) και το λογισμικό που εκτελείται στη συσκευή, πέραν των υπόλοιπων δεδομένων που περιέχονται σε ένα παραδοσιακό μήνυμα CCF (η σύνοψη των μηνυμάτων TLS και το κύριο μυστικό). Ο διακομιστής χρησιμοποιεί το τροποποιημένο CCF μήνυμα για να επαληθεύσετε ότι εκτελείται ο κατάλληλος κωδικός σύνδεσης, ο χρήστης εισήγαγε το κατάλληλο ζεύγος ταυτότητας και κωδικού για τη συγκεκριμένη συσκευή και το ότι η προβλεπόμενη συσκευή δημιούργησε το μήνυμα. Σε αυτή την προτεινόμενη μορφή του πρωτοκόλλου προστίθενται ή αλλάζουν τρία βήματα από την αρχική χειραψία EAP-TLS.

Όταν χρησιμοποιείται το TPM attestation, ο server μπορεί να επαληθεύσει ότι η συσκευή εκτελεί έγκυρη έκδοση του κώδικα σύνδεσης. Το κύριο μειονέκτημα αυτού του πρωτοκόλλου είναι οι αλλαγές που γίνονται στο CCF μήνυμα. Με αυτές τις αλλαγές, οι servers πρέπει να επαληθεύσουν μία υπογραφή και να επιβεβαιώσουν ότι η τιμή της υπογραφής αντιστοιχεί σε ένα PCR με τη σωστή διαμόρφωση λογισμικού, τις σωστές πληροφορίες του χρήστη και την σύνοψη του κύριου μυστικού και των μηνυμάτων του handshake. Οι τρέχουσες υπογραφές του πρωτοκόλλου TLS περιλαμβάνουν μόνο τη σύνοψη των μηνυμάτων και το κύριο μυστικό. Αυτό απαιτεί χρήση επιπλέον κώδικα για να διασφαλιστεί η λήψη από τον server του κατάλληλου μηνύματος.

5.2.3 EAP-TLS with TPM Sealed Storage Based Device and User Authentication

Στην δεύτερη περίπτωση υλοποίησης αξιοποιείται το TPM sealed storage για να περιορίσει την πρόσβαση στο ιδιωτικό κλειδί υπογραφής της συσκευής. Το TPM sealed storage επιτρέπει σε έναν server να "κλειδώνει" δεδομένα ώστε μόνο το υλικό με το κατάλληλο λογισμικό και δεδομένα (π.χ. κωδικό πρόσβαση) να μπορεί να έχει πρόσβαση στα δεδομένα. Για την αρχική σφράγιση δεδομένων, ο χρήστης πρέπει να εκτελέσει ένα πρόγραμμα εγγραφής το οποίο δημιουργεί ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού και σφραγίζει το ιδιωτικό κλειδί έτσι ώστε μόνο το λογισμικό σύνδεσης μπορεί να έχει πρόσβαση στο ιδιωτικό κλειδί όταν ο χρήστης εισάγει τον κατάλληλο συνδυασμό ταυτότητας/κωδικού. Το πρόγραμμα εγγραφής αποθηκεύει επίσης ένα αντίγραφο του δημόσιου κλειδιού και ενός πιστοποιητικού υπογεγραμμένο από τον πάροχο, ώστε οποιοδήποτε πρόγραμμα να έχει πρόσβαση σε αυτά τα δεδομένα. Σύμφωνα με αυτή την υλοποίηση όταν ο χρήστης προσπαθήσει να συνδεθεί σε ένα ασύρματο δίκτυο πόλεως, ο κώδικας σύνδεσης θα εκτελέσει κανονικά το EAP-TLS μέχρι να χρειαστεί να δημιουργήσει την υπογραφή του client. Εκείνη τη στιγμή, το πρόγραμμα επεκτείνει την PCR με την σύνοψη του λογισμικού σύνδεσης, της ταυτότητας και του κωδικού πρόσβασης. Εάν η PCR περιέχει τις κατάλληλες τιμές, μπορεί να πραγματοποιηθεί μια λειτουργία αποσφράγισης η οποία "ξεκλειδώνει" το ιδιωτικό κλειδί της συσκευής. Έχοντας πρόσβαση στο κλειδί υπογραφής και τον κωδικό μπορεί να δημιουργηθεί η υπογραφή πάνω από τον κατακερματισμό των μηνυμάτων TLS και το κύριο μυστικό. Αν υποθέσουμε

ότι το κλειδί υπογραφής δεν έχει διαρρεύσει σημαίνει ότι κάποιος χρήστης με την κατάλληλη ταυτότητα και κωδικό πρόσβασης χρησιμοποιεί αυτήν τη συσκευή.

Αυτή η μορφή του πρωτοκόλλου έχει πολλά πλεονεκτήματα σε σύγκριση με την προηγούμενη, αλλά υπάρχουν κάποιες περιπτώσεις που θα μπορούσαν να αποδυναμώσουν την ασφάλεια. Σε αυτή την δεύτερη μορφή του το πρωτοκόλλου συμμορφώνεται με τα τρέχοντα μηνύματα TLS και αποσυνδέει το TPM attestation key από το κλειδί του client. Με αυτό τον τρόπο το πρωτόκολλο απλοποιεί την ανάπτυξη ενώ επιτυγχάνεται ο ίδιος έλεγχος πρόσβασης με το πρώτη υλοποίηση του πρωτόκολλο (μόνο πιστοποιημένοι χρήστες με την αντίστοιχη συσκευή τους μπορούν να ολοκληρώσουν το TLS handshake). Ορισμένοι χρήστες ενδέχεται να έχουν προβλήματα απορρήτου στην πρώτη υλοποίηση αφού, το TPM attestation key χρησιμοποιείται για την υπογραφή των μηνυμάτων σύνδεσης και τυχόν άλλων βεβαιώσεων που πραγματοποιεί το TPM. Στην δεύτερη πρόταση για την υλοποίηση του πρωτοκόλλου μειώνεται αυτή την ανησυχία από την στιγμή που χρησιμοποιείται ένα ανεξάρτητο κλειδί για την υπογραφή των μηνυμάτων επαλήθευσης του client. Ένα μειονέκτημα ωστόσο είναι ότι πρέπει να εμπιστευτούμε τον κώδικα και σύστημα κατά τη διαχείριση του μη σφραγισμένου κλειδιού. Αφού το κλειδί αποθηκεύεται προσωρινά στη μνήμη υπάρχει πιθανότητα ο κώδικαε θα μπορούσε να έχει πρόσβαση στο κλειδί και να εκτελεί ανεπιθύμητες ενέργειες (π.χ. αντιγραφή του κλειδιού σε άλλη συσκευή ή αντιγράψτε το κλειδί, ώστε οι χρήστες να μην χρειάζεται να πληκτρολογούν ξανά τον κωδικό πρόσβασής τους).

5.3 Συμπεράσματα

Οι προαναφερόμενες υλοποιήσεις έδειξαν πως είναι πολύ εύκολο στην πράξη μία εφαρμογή του πρωτοκόλλου EAP-TLS να συμπεριλάβει και το TPM. Από την πλευρά του client, ο supplicant θα πρέπει να υποστηρίζει την πρόσβαση στο TPM για να μπορεί να αποθηκεύει τα ιδιωτικά κλειδιά σε ένα ασφαλές περιβάλλον. Στην πλευρά του server τα πράγματα είναι λίγο πιο πολύπλοκα, εξαιτίας των περιορισμών που αναλύθηκαν προηγουμένως για τα X.509 πιστοποιητικά.

Η υλοποίηση του EAP-TPM μπορεί γίνει σε συστήματα Linux και οι μόνες εφαρμογές που χρειάζονται τροποποίηση είναι ο supplicant και ο FreeRADIUS server, γεγονός που σημαίνει πως το πρότυπο που έχει προταθεί μπορεί να τρέξει σε οποιοδήποτε Linux σύστημα υποστηρίζει το TPM, είτε πρόκειται για κάποιον υπολογιστή είτε για κάποια ενσωματωμένη συσκευή.

Πέραν της διευκόλυνσης που προσφέρεται στους χρήστες των ασύρματων δικτύων το EAP-TPM μπορεί να διασφαλίσει και την ασφάλεια σε ασύρματα δίκτυα πόλεων με την μοναδική ταυτοποίηση στο δίκτυο των χρηστών και στων συσκευών εκμεταλλευόμενο τις δυνατότητες του TPM.

Χρησιμοποιώντας αυτόν τον τρόπο αυθεντικοποίησης η σύνδεση με τις κινητές συσκευές σε ασύρματα δίκτυα θα γίνει εξίσου δημοφιλής με την σύνδεση σε GSM δίκτυα. Επιπλέον, η χρήση του πρωτοκόλλου και σε υπολογιστές θα ενθαρρύνει ακόμα περισσότερους

χρήστες να κάνουν χρήση των δημόσιων hotspot αλλά και εταιρικά περιβάλλοντα να χρησιμοποιήσουν αυτό τον εύκολο τρόπο σύνδεσης στο δίκτυο τους.

6. FREERADIUS

Σε αυτό το κεφάλαιο θα γίνει μία συνοπτική παρουσίαση της λειτουργίας του server FreeRADIUS και κάποιων βασικών του ρυθμίσεων.

6.1 Εισαγωγή

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο ο εξυπηρετητής RADIUS λειτουργεί στις UDP θύρες 1812 για αυθεντικοποίηση και 1813 για λογιστική καταγραφή. Ο πελάτης RADIUS είναι συνήθως μια συσκευή που παρέχει πρόσβαση σε ένα TCP/IP δίκτυο δεδομένων (Network Access Server – NAS), όπως για παράδειγμα ένα Ethernet switch ή ένα WiFi σημείο πρόσβασης (Access Point – AP). Ο πελάτης λειτουργεί ως διαμεσολαβητής ανάμεσα στον εξυπηρετητή RADIUS και σε έναν χρήστη ή σε μια συσκευή που επιθυμεί να αποκτήσει πρόσβαση στο δίκτυο. Ένας εξυπηρετητής RADIUS μπορεί να λειτουργήσει επίσης και ως πελάτης, δηλαδή ως διακομιστής μεσολάβησης (proxy server), ενός άλλου εξυπηρετητή RADIUS, σχηματίζοντας τελικά μια αλυσίδα. Ο εξυπηρετητής RADIUS αποφασίζει εάν θα πρέπει να επιτραπεί η δικτυακή πρόσβαση σε έναν χρήστη (αυθεντικοποίηση). Επιπλέον, έχει τη δυνατότητα να δώσει εντολή στον πελάτη να επιβάλει ορισμένους περιορισμούς στον χρήστη (εξουσιοδότηση), όπως για παράδειγμα το χρονικό περιορισμό μιας συνόδου ή το όριο της ταχύτητας σύνδεσης. Η ευθύνη επιβολής όμως, των προτεινόμενων ρυθμίσεων στη σύνοδο του χρήστη, βρίσκεται στην πλευρά του πελάτη.

Το έργο ελεύθερου λογισμικού FreeRADIUS αποτελεί μια υλοποίηση του πρωτοκόλλου RADIUS. Η ανάπτυξη του FreeRADIUS ξεκίνησε το 1999 με την ενεργή συμμετοχή εθελοντών από την κοινότητα του ανοιχτού λογισμικού, οδηγώντας στη δημιουργία ενός νέου ανταγωνιστικού εξυπηρετητή RADIUS ανοιχτού κώδικα, ο οποίος κατάφερε να εδραιωθεί στην αγορά αποκτώντας μια πολύ καλή φήμη [28].

Η δημοτικότητα του FreeRADIUS οφείλεται στο γεγονός ότι αποτελεί λογισμικού ανοιχτού κώδικα, επιτρέποντας την προσαρμογή, αλλαγή, επέκταση ή διόρθωση μέρους του κώδικα που απαιτείται. Το FreeRADIUS αναπτύσσεται στο πλαίσιο του GNU General Public License και είναι ελεύθερο για διανομή και χρήση. Επίσης, συμπεριλαμβάνει πολλά τμήματα για την υποστήριξη διαφόρων επιπλέον λειτουργιών, όπως για παράδειγμα LDAP ή SQL ή για τη χρήση των γλωσσών προγραμματισμού Perl και Python. Ένα άλλο πλεονέκτημα που προκύπτει από την ευρεία αποδοχή που έχει σε εταιρικές εγκαταστάσεις μεγάλου αριθμού χρηστών, είναι το γεγονός ότι σε περίπτωση εμφάνισης προβλήματος είναι εύκολη η αναζήτηση λύσεων που έχουν προταθεί ήδη από άλλους προγραμματιστές που έχουν αντιμετωπίσει το ίδιο ή παρόμοιο ζήτημα. Εξαιτίας του ότι το FreeRADIUS αποτελεί λογισμικό ανοιχτού κώδικα υποστηρίζει γρήγορα νέα χαρακτηριστικά και λειτουργικότητες του RADIUS πρωτοκόλλου και επιπλέον, βρίσκεται διαθέσιμο για μια πληθώρα λειτουργικών συστημάτων. Τέλος, υπάρχει διαθέσιμη εμπορική υποστήριξη από την ομάδα των βασικών σχεδιαστών του λογισμικού.

Το μειονέκτημα που χαρακτηρίζει το FreeRADIUS είναι η πολυπλοκότητα που προκύπτει από τις πολλές δυνατότητες παραμετροποίησης που παρέχει. Χρειάζεται μεγάλη

προσοχή στην εγκατάσταση και στη ρύθμιση των διαφόρων ιδιοτήτων του συστήματος. Οι διάφορες ευπάθειες που είχαν εντοπιστεί κατά καιρούς έχουν αντιμετωπιστεί στις νεότερες εκδόσεις.

Οι ανταγωνιστές του FreeRADIUS είναι διαφορετικά προϊόντα, καθώς και εναλλακτικές τεχνολογικές λύσεις. Ανάμεσα στους ανταγωνιστές εξυπηρετητές RADIUS περιλαμβάνονται οι Cisco ACS, Microsoft IAS και Radiator. Ανταγωνιστικές AAA τεχνολογίες είναι το Diameter, το TACACS+ και το LDAP το οποίο όμως υποστηρίζει μόνο αυθεντικοποίηση.

6.2 Εγκατάσταση FreeRADIUS

Για την εγκατάσταση του FreeRadius σε έναν Linux Server υπάρχουν δύο μέθοδοι: Η πρώτη μέθοδος είναι η μεταγλώττιση του πηγαίου κώδικα και στη συνέχεια η εγκατάστασή του χρησιμοποιώντας τα παραγόμενα δυαδικά αρχεία και η δεύτερη μέθοδος, η οποία και θα περιγραφεί, είναι η απευθείας χρησιμοποίηση των προμεταγλωττισμένων δυαδικών αρχείων. Το λειτουργικό σύστημα για το οποίο θα περιγραφεί η διαδικασία εγκατάστασης είναι το Ubuntu 18.04.

Οι εντολές που απαιτείται να εκτελεστούν για την εγκατάσταση του FreeRADIUS είναι οι ακόλουθες [28]:

```
$> sudo su

#> apt-get install freeradius
```

Μετά την επιτυχή ολοκλήρωση των παραπάνω εντολών έχει εγκατασταθεί ένας λειτουργικός FreeRADIUS server, ο οποίος περιλαμβάνει τις προκαθορισμένες ρυθμίσεις και λειτουργίες. Ο FreeRADIUS server θα πρέπει να λειτουργεί με όσο το δυνατόν λιγότερα προνόμια σε ένα περιβάλλον παραγωγής. Για αυτό το σκοπό, δημιουργείται κατά την εγκατάσταση ένας χρήστης και μία ομάδα με όνομα *freerad*, τα οποία προσδιορίζονται στις οδηγίες *user* και *group* αντίστοιχα που περιλαμβάνονται στο αρχείο ρυθμίσεων *radiusd.conf*.

Διασφάλιση ορθής εκκίνησης

Εκτελώντας την εντολή *freeradius –X* με δικαιώματα root, ξεκινά ο FreeRADIUS server σε κατάσταση εντοπισμού σφαλμάτων, αναφέροντας τυχόν προβλήματα. Για τη διακοπή της εκτέλεσής του θα πρέπει να πληκτρολογηθεί *Ctrl + C*. Στην περίπτωση κατά την οποία εμφανιστεί ένα μήνυμα σφάλματος το οποίο αναφέρει ότι η θύρα 1812 χρησιμοποιείται, ο FreeRADIUS server λειτουργεί ήδη. Για να σταματήσει η λειτουργία του, θα πρέπει να εκτελεστεί παρακάτω script τερματισμού.

```
$>sudo /etc/init.d/freeradius stop
```

Αντιστοίχως, για την εκκίνηση του FreeRADIUS server θα πρέπει να χρησιμοποιηθεί η παρακάτω εντολή εκκίνησης:

```
$> sudo /etc/init.d/freeradius start
```

Τέλος, για την επανεκκίνηση του FreeRADIUS server θα πρέπει να χρησιμοποιηθεί η παρακάτω εντολή επανεκκίνησης:

```
$> sudo /etc/init.d/freeradius restart
```

Μετά από κάθε επανεκκίνηση του συστήματος, θα πρέπει να εξασφαλιστεί ότι θα ξεκινήσει αυτομάτως η λειτουργία του FreeRADIUS, μαζί με τις υπόλοιπες υπηρεσίες του συστήματος. Για την ενεργοποίηση της υπηρεσίας του FreeRADIUS κατά την εκκίνηση, θα πρέπει να εκτελεστεί η παρακάτω εντολή:

```
$> sudo update-rc.d freeradius defaults
```

Αντιστρόφως, για την απενεργοποίηση της υπηρεσίας του FreeRADIUS κατά την εκκίνηση, θα πρέπει να εκτελεστεί η παρακάτω εντολή:

```
$> sudo update-rc.d -f freeradius remove
```

Προκειμένου να ελεγχθεί ότι ο FreeRADIUS server λειτουργεί, μπορεί να εκτελεστεί μία από τις παρακάτω εντολές:

```
#> pidof freeradius
```

ή

```
#> ps aux | grep radius
```

Τέλος, η παρακάτω εντολή μπορεί να χρησιμοποιηθεί προκειμένου να διαπιστωθεί η διεπαφή και οι θύρες UDP που χρησιμοποιούνται από τον FreeRADIUS server:

```
#> netstat -unap | grep radius
```

Βασικές Ρυθμίσεις

Μετά την ολοκλήρωση της εγκατάστασης του FreeRADIUS server, θα πρέπει να ακολουθήσει η διαμόρφωσή του βάσει των εκάστοτε αναγκών. Η διαμόρφωση του FreeRADIUS πραγματοποιείται με τη χρήση αρχείων ρυθμίσεων. Τα αρχεία αυτά βρίσκονται αποθηκευμένα στον κατάλογο */etc/freeradius*. Για την τροποποίηση αυτών των αρχείων απαιτείται η σύνδεση με δικαιώματα root.

Ο FreeRADIUS περιλαμβάνει έναν προκαθορισμένο client ο οποίος ονομάζεται localhost. Ο client αυτός μπορεί να αξιοποιηθεί από τα προγράμματα RADIUS client που βρίσκονται εγκατεστημένα στο localhost, για την πραγματοποίηση δοκιμών και την επίλυση προβλημάτων. Ο ορισμός του localhost client βρίσκεται εντός του αρχείου *clients.conf* και η μοναδική αλλαγή που γίνεται αρχικά αφορά την ιδιότητα secret, έτσι ώστε αυτός να περιλαμβάνει τις παρακάτω ρυθμίσεις:

```
client localhost {
```

```
        ipaddr = 127.0.0.1

        secret = localtest

        require_message_authenticator = no

        nastype = other

}
```

Για την προσθήκη ενός πραγματικού σημείου πρόσβασης, το οποίο για παράδειγμα ονομάζεται ap1, θα πρέπει να προστεθεί μία αντίστοιχη ενότητα στο αρχείο *clients.conf*, με τις παρακάτω ρυθμίσεις:

```
client ap1 {

        ipaddr = 192.168.1.1

        secret = AP1Secret

        require_message_authenticator = yes

        nastype = other

}
```

Θέτοντας *require_message_authenticator = yes*, επιβάλλεται η παρουσία του AVP Message-Authenticator στα πακέτα που αποστέλλονται από τον NAS καθώς και η ορθότητα της τιμής του. Η τιμή που περιλαμβάνει είναι η σύνοψη του πακέτου RADIUS και η επαλήθευση του από τον FreeRADIUS server επιβεβαιώνει την ακεραιότητα του πακέτου. Ο έλεγχος της ακεραιότητας των πακέτων πραγματοποιείται από τον server μόνο για τα αιτήματα αυθεντικοποίησης και όχι για τα πακέτα λογιστικής καταγραφής.

Για τον ορισμό ενός χρήστη με όνομα alice και συνθηματικό alicepass, θα πρέπει να προστεθούν οι παρακάτω γραμμές στην αρχή του αρχείου *users*.

```
"alice" Cleartext-Password := "alicepass", Login-Time := 'Al0900-2200'

        Framed-IP-Address = 192.168.1.100,

        Reply-Message = "Hello, %{User-Name}"
```

Για τη δοκιμή των βασικών ρυθμίσεων του FreeRADIUS, θα πρέπει ο server να τεθεί σε κατάσταση εντοπισμού σφαλμάτων και να χρησιμοποιηθεί το πρόγραμμα *radtest* για την αποστολή πακέτων Access-Request. Κατά τη φάση αυτή ελέγχεται η ορθή λειτουργία του localhost client και ο σωστός ορισμός του χρήστη alice. Η ορθή λειτουργία του πραγματικού σημείου πρόσβασης επιβεβαιώνεται σε επόμενο στάδιο, αφού προηγουμένως ολοκληρωθεί η παραμετροποίηση επιπλέον απαιτούμενων συστατικών στοιχείων.

Για την εκκίνηση του FreeRADIUS server σε κατάσταση εντοπισμού σφαλμάτων, πρέπει προηγουμένως να επιβεβαιωθεί ότι δεν λειτουργεί ήδη. Αυτό μπορεί να γίνει χρησιμοποιώντας το script τερματισμού του:

```
$> sudo su

#> /etc/init.d/freeradius stop

#> freeradius -X
```

Εφόσον η εκκίνηση του FreeRADIUS server ολοκληρωθεί με επιτυχία, θα πρέπει η τελευταία γραμμή του τερματικού να αναφέρει το εξής:

```
Ready to process requests.
```

Για τη δοκιμή αυθεντικοποίησης του χρήστη alice, πρέπει να εκτελεστεί από ένα δεύτερο παράθυρο τερματικού η παρακάτω εντολή:

```
$> radtest alice alicepass 127.0.0.1 100 localtest
```

Μετά από την εκτέλεση της παραπάνω εντολής, θα εμφανιστεί στο τερματικό του FreeRADIUS server το πακέτο Access-Request, καθώς και η απόκρισή του σε αυτό το αίτημα. Το αίτημα και η απόκριση θα εμφανιστούν επίσης και στο τερματικό στο οποίο εκτελέστηκε το radtest:

```
Sending Access-Request of id 162 to 127.0.0.1 port 1812

User-Name = "alice"

User-Password = "alicepass"

NAS-IP-Address = 127.0.1.1

NAS-Port = 100

rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=162, length=46

Framed-IP-Address = 192.168.1.100

Reply-Message = "Hello, alice"

Session-Timeout = 23700
```

6.3 Γενική επισκόπηση λειτουργίας του FreeRADIUS server

6.3.1 Clients

Ο προσδιορισμός των clients του FreeRADIUS server γίνεται εντός του αρχείου *clients.conf*.

Ενότητες

Ο ορισμός ενός client γίνεται με τη χρήση μίας ενότητας *client*. Το FreeRADIUS χρησιμοποιεί ενότητες προκειμένου να ορίσει και να ομαδοποιήσει διάφορα αντικείμενα. Μία ενότητα ξεκινά με μία λέξη κλειδί η οποία υποδηλώνει τον τύπο της ενότητας ακολουθούμενη ορισμένες φορές από μία λέξη η οποία αποτελεί το όνομά της. Το όνομα αυτό δίνει τη δυνατότητα προσδιορισμού διαφορετικών ενοτήτων του ίδιου τύπου, όπως είναι για παράδειγμα οι διάφοροι clients που ορίστηκαν στο αρχείο *clients.conf*. Στη συνέχεια ακολουθούν αγκύλες οι οποίες περικλείουν διάφορες ρυθμίσεις που αφορούν τη συγκεκριμένη ενότητα. Οι ενότητες είναι δυνατό να περικλείουν επίσης άλλες ενότητες, δημιουργώντας μία ιεραρχική δομή. Το αρχείο *clients.conf* δεν αποτελεί το μοναδικό αρχείο στο οποίο μπορεί να χρησιμοποιηθούν οι ενότητες client. Όπως περιγράφεται σε επόμενο κεφάλαιο, είναι δυνατό να χρησιμοποιηθούν και εντός μίας ενότητας server, κατά τον ορισμό ενός εικονικού server.

Ταυτοποίηση client

Η ταυτοποίηση ενός client από τον FreeRADIUS server πραγματοποιείται μέσω της IP διεύθυνσής του. Αν αποσταλεί στον server ένα αίτημα από έναν άγνωστο client, αυτό θα αγνοηθεί.

Κοινό μυστικό

Για την επικοινωνία μεταξύ του client και του server, απαιτείται η κατοχή ενός κοινού μυστικού μεταξύ των δύο επικοινωνούντων μερών, το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση και αποκρυπτογράφηση συγκεκριμένων AVPs. Για παράδειγμα, το User-Password AVP κρυπτογραφείται χρησιμοποιώντας αυτό το κοινό μυστικό.

Message-Authenticator

Κατά τον καθορισμό ενός client, είναι δυνατό να επιβληθεί η παρουσία του Message-Authenticator AVP σε όλα τα αιτήματα.

Nastype

Η τιμή της ιδιότητας nastype καθορίζει τον τρόπο συμπεριφοράς του Perl script *checkrad*. Το checkrad χρησιμοποιείται για να εξακριβωθεί αν ένας χρήστης χρησιμοποιεί πόρους του NAS, αποστέλλοντας κατάλληλα αιτήματα προς αυτό και χρησιμοποιώντας τη μέθοδο που αντιστοιχεί στο nastype που έχει ορισθεί για τον client.

6.3.2 Χρήστες

Οι χρήστες προσδιορίζονται στο αρχείο users. Τα περιεχόμενα αυτού του αρχείου χρησιμοποιούνται για την Αυθεντικοποίηση (Authentication) και την Εξουσιοδότηση (Authorization) των χρηστών. Ο προσδιορισμός των χρηστών είναι δυνατόν να γίνει και σε άλλα σημεία αποθήκευσης.

Files module

Το module *files (rlm_files)* διαβάζει τα περιεχόμενα του αρχείου *users* προκειμένου να εξακριβώσει αν υφίσταται ο χρήστης που προσδιορίζεται στο Access-Request πακέτο και αν είναι εξουσιοδοτημένος να χρησιμοποιήσει το NAS. Επίσης, προσδιορίζει τις ιδιότητες (attributes) οι οποίες θα πρέπει να επιστραφούν στον client. Το module *files* μπορεί να θέσει επίσης την ιδιότητα Auth-Type, η οποία προσδιορίζει τη μέθοδο αυθεντικοποίησης που θα χρησιμοποιηθεί. Για παράδειγμα, αν ο ορισμός ενός χρήστη περιλαμβάνει το στοιχείο ελέγχου Cleartext-Password, η μέθοδος αυθεντικοποίησης που θα χρησιμοποιηθεί θα είναι η PAP (Auth-Type=PAP). Τέλος, το module *files* παρέχει σε άλλα modules ένα «γνωστό ορθό συνθηματικό», αν αυτό έχει οριστεί. Για παράδειγμα, στην περίπτωση του χρήστη που ορίστηκε προηγουμένως, παρέχει στο module *pap (rlm_pap)* την τιμή που έχει προσδιοριστεί στο στοιχείο ελέγχου *Cleartext- Password*.

PAP module

Το module *PAP (rlm_pap)* χρησιμοποιήθηκε στο προηγούμενο παράδειγμα για την αυθεντικοποίηση του χρήστη. Στην περίπτωση κατά την οποία το *Auth-Type* έχει την τιμή *PAP*, ελέγχεται αν το «γνωστό ορθό συνθηματικό» είναι το ίδιο με αυτό που δόθηκε στην ιδιότητα *User-Password*, προκειμένου να γίνει αποδεκτό το αίτημα αυθεντικοποίησης. Να σημειωθεί ότι το αίτημα αυθεντικοποίησης ενδέχεται τελικά να μη γίνει αποδεκτό, λόγω απόρριψης του από άλλα modules της αλυσίδας αυθεντικοποίησης.

Αρχείο users

Το αρχείο users χρησιμοποιείται για τον προσδιορισμό των χρηστών. Περιλαμβάνει μία εγγραφή για κάθε χρήστη, η οποία αποτελείται από τον κωδικό του ακολουθούμενο από μηδέν ή περισσότερα στοιχεία ελέγχου που διαχωρίζονται μεταξύ τους με το χαρακτήρα κόμμα. Στη συνέχεια ακολουθούν μηδέν ή περισσότερες γραμμές στοιχείων απάντησης που διαχωρίζονται μεταξύ τους με το χαρακτήρα κόμμα και έχουν μία εσοχή η οποία δημιουργείται από ένα χαρακτήρα tab.

6.3.3 Αρχεία ρυθμίσεων

Η διαμόρφωση του FreeRADIUS server είναι λογικά διαιρεμένη σε ένα σύνολο αρχείων. Το κύριο αρχείο ρυθμίσεων στο οποίο υπάρχουν αναφορές και σε διάφορα επιπρόσθετα αρχεία, είναι το *radiusd.conf*. Οι προεπιλεγμένες ρυθμίσεις είναι κατάλληλες για την πλειονότητα των εγκαταστάσεων και συνήθως απαιτούνται ελάχιστες τροποποιήσεις. Τα περιεχόμενα των επιπρόσθετων αρχείων και καταλόγων συμπεριλαμβάνονται με τη χρήση της λέξης κλειδί *$INCLUDE* εντός του αρχείου *radiusd.conf*.

6.3.4 Βιβλιοθήκες και λεξικά

Ο FreeRADIUS χρησιμοποιεί πολλά modules τα οποία είναι βιβλιοθήκες με ονόματα της μορφής *rlm_<όνομα module>*. Βρίσκονται αποθηκευμένα σε έναν κατάλογο ο οποίος προσδιορίζεται από την παράμετρο *libdir* του αρχείου *radiusd.conf*. Επίσης, χρησιμοποιούνται λεξικά για την αντιστοίχιση των AVP (Attribute-Value Pairs) και VSA

(Vendor Specific Attributes) ονομάτων σε αριθμούς. Υπάρχει ένα κύριο λεξικό το οποίο βρίσκεται στον κατάλογο */etc/freeradius* και ονομάζεται *dictionary*. Στο αρχείο αυτό υπάρχει μία οδηγία *$INCLUDE* η οποία προσδιορίζει έναν κατάλογο στο οποίο βρίσκονται επιπλέον λεξικά με ονόματα της μορφής *dictionary.<vendor name>*. Το αρχείο *dictionary.freeradius.internal* περιλαμβάνει τα AVPs τα οποία χρησιμοποιούνται εσωτερικά από το FreeRADIUS, όπως τα *Cleartext-Password*, *Auth-Type* και *Login-Time*.

6.3.5 Ενότητα Listen

Το FreeRADIUS εξυπηρετεί εξ' ορισμού αιτήματα σε όλες τις διαθέσιμες διεπαφές. Αυτό μπορεί να διαφοροποιηθεί προσδιορίζοντας μία συγκεκριμένη NIC ή διεύθυνση IP, είτε για το σύνολο των αιτημάτων είτε ανά εικονικό server ή τύπο αιτήματος.

6.3.6 Αρχεία διαμόρφωσης

Τα subdirectories από τα οποία αποτελείται ένας FreeRADIUS Server και βοηθούν στην οργάνωση των configuration files είναι τα παρακάτω [49]:

- **Mods-available:** Ένας κατάλογος που περιέχει δείγματα διαμορφώσεων για όλες τις ενότητες τα οποία οι διαχειριστές δικτύου μπορούν να ενεργοποιήσουν προαιρετικά. Όλη η διαμόρφωση της μονάδας τεκμηριώνεται εδώ. Τα παραδείγματα περιλαμβάνουν πολλές ενότητες που αποστέλλονται με το διακομιστή, αλλά που ενδέχεται να μην είναι ενεργοποιημένες σε κάθε μεμονωμένη διαμόρφωση. Τα αρχεία σε αυτόν τον κατάλογο φορτώνονται από το αρχείο radiusd.conf.
    - Το module `always` χρησιμοποιείται για εντοπισμό σφαλμάτων. Σε κάθε περίπτωση επιστρέφει πάντα ένα προκαθορισμένο αποτέλεσμα χωρίς να κάνει τίποτα άλλο. Όταν χρησιμοποιείται στην ενότητα `checksimul` επιτρέπει είτε απαγορεύει πολλαπλές συνδέσεις. Η επιλογή `mpp` ελέγχει αυτήν τη συμπεριφορά: όταν οριστεί σε `no`, δεν επιτρέπει πολλές συνδέσεις ενώ όταν οριστεί σε `yes`, επιτρέπονται πολλαπλές συνδέσεις.
    - Το module `attr_filter` φιλτράρει χαρακτηριστικά στα πακέτα. Μπορεί να διαγράψει χαρακτηριστικά ή να τους επιτρέψει να έχουν μόνο συγκεκριμένες τιμές. Η μορφή του αρχείου είναι η ίδια με το αρχείο users.

      Ενότητες Επεξεργασίας

      authorize, accounting, post-auth, preacct, pre-proxy, post-proxy, recv-coa, send-coa

- Το module `cache` αποθηκεύει προσωρινά τα χαρακτηριστικά και τα παράγει στη συνέχεια σε μια μεταγενέστερη εκτέλεση της λειτουργικής μονάδας. Επιτρέπει την προσωρινή αποθήκευση πληροφοριών μεταξύ των αιτημάτων είτε την προσωρινή αποθήκευση αποτελεσμάτων από αναζητήσεις βάσης δεδομένων.

  Ενότητες Επεξεργασίας

  authorize, post-auth, pre-proxy, post-proxy

- Το module `cui` γράφει το χαρακτηριστικό Chargeable-User-Identity σε μια βάση δεδομένων SQL. Είναι μια παραλλαγή του sql module.

- Το module `rlm_dhcp` χρησιμοποιείται για την αποκωδικοποίηση χαρακτηριστικών RADIUS που περιέχουν επιλογές DHCP.

- Το module `rlm_digest` εκτελεί έλεγχο ταυτότητας HTTP, συνήθως για διακομιστές SIP.

  Ενότητες Επεξεργασίας

  authorize, authenticate

- Το module `dynamic_clients` φορτώνει δυναμικά τους ορισμούς των πελατών. Θα πρέπει να χρησιμοποιείται μόνο στο εσωτερικό του εικονικού διακομιστή `dynamic_clients.`

  Ενότητες Επεξεργασίας

  authorize

- Το module `rlm_eap` περιέχει τη διαμόρφωση για τύπους EAP (PEAP, TTLS κ.λπ.).

  Ενότητες Επεξεργασίας

  authorize, authenticate, post-auth, post-proxy

- Το module `echo` αποτελεί παραλλαγή του module `exec`.

- Το module `rlm_passwd-etc_group` είναι ένα παράδειγμα του module `passwd`, το οποίο διαβάζει το αρχείο /etc/group.

- Το module `exec` εκτελεί προγράμματα και είναι χρήσιμο για την εκτέλεση προγραμμάτων τρίτων στον FreeRADIUS.

  Ενότητες Επεξεργασίας

accounting, post-auth

- Το module `expr` εφαρμόζει μαθηματικές εκφράσεις.
- Το module `files` διαβάζει αρχεία που έχουν ειδική μορφή.

  Ενότητες Επεξεργασίας

  authorize, post-auth, preacct, pre-proxy, post-proxy
- Το module `idn` μετατρέπει διεθνοποιημένα ονόματα τομέα σε ASCII. Η μορφή ASCII μπορεί στη συνέχεια να χρησιμοποιηθεί για συγκρίσεις ονομάτων.
- Το module `rlm_eap – inner_eap` αποτελεί Δείγμα διαμόρφωσης για το module `EAP` που εμφανίζεται μέσα σε μια μέθοδο tunelled. Χρησιμοποιείται για τον περιορισμό των τύπων EAP που μπορούν να εμφανιστούν στο inner tunnel.
- Το module `rlm_ippool` κάνει διαχείριση των διευθύνσεων ip από την πλευρά του server και πρέπει να προστεθεί στις ενότητες post-auth και accounting. Επιπλέον απαιτείται η ύπαρξη του χαρακτηριστικού Pool-Name, έτσι ώστε ο διαχειριστής να μπορεί να προσθέσει το χαρακτηριστικό Pool-Name στα προφίλ χρηστών και να χρησιμοποιεί διαφορετικές ομάδες για διαφορετικούς χρήστες. Το χαρακτηριστικό Pool-Name αποτελεί ένα στοιχείο ελέγχου, όχι ένα στοιχείο απάντησης.
- Το module `krb5` εφαρμόζεται για αυθεντικοποίηση μέσω του Kerberos.
- Το module `ldap` υποστηρίζει την αναζήτηση ερωτημάτων διακομιστών LDAP μέσω του πρωτοκόλλου Lightweight Directory Access Protocol (LDAP).
- Το module `linelog` καταγράφει μια γραμμή κειμένου σε ένα αρχείο. Τόσο το όνομα αρχείου όσο και η γραμμή κειμένου επεκτείνονται δυναμικά. Συνιστάται να μην χρησιμοποιούνται δεδομένα από το πακέτο ως μέρος του ονόματος αρχείου. Η χρήση δεδομένων από το πακέτο μπορεί να δώσει τη δυνατότητα σε πιθανούς εισβολείς να δημιουργήσουν ή να αφαιρέσουν αυθαίρετα αρχεία στο διακομιστή.
- Το module `logintime` υποστηρίζει ορισμένα χαρακτηριστικά που σχετίζονται με την ημερομηνία. Το χαρακτηριστικό `Login-Time` καθορίζει το χρονικό διάστημα κατά το οποίο ένας χρήστης μπορεί να συνδεθεί στο σύστημα.

- Το module `mac2ip` είναι ένα δείγμα διαμόρφωσης για το module `passed`, το οποίο διαβάζει αρχεία `flat-text`. Το αρχείο έχει τη μορφή <mac>, <ip>.

- Το module `mac2vlan` είναι ένα απλό αρχείο για τη χαρτογράφηση μιας διεύθυνσης MAC σε ένα VLAN. Το αρχείο πρέπει να έχει τη μορφή MAC, VLAN.

- Το module `mschap` υποστηρίζει έλεγχο ταυτότητας MS-CHAP και MS-CHAPv2. Επιβάλλει επίσης το χαρακτηριστικό `SMB-Account-Ctrl`.

- Το module `ntlm_auth` είναι μια παραλλαγή του module exec. Χρησιμεύει ως βήμα δοκιμής πριν από τη χρήση του MS-CHAP και του `ntlm_auth`. Δεν πρέπει να χρησιμοποιείται σε περιβάλλοντα παραγωγής.

- Το module `opendirectory` χρησιμοποιείται μόνο όταν ο διακομιστής εκτελείται στο ίδιο σύστημα με το OpenDirectory. Η διαμόρφωση της μονάδας είναι κωδικοποιημένη από την Apple και δεν μπορεί να αλλάξει.

  Ενότητες Επεξεργασίας

  authorize, authenticate

- Το module `otp` παρέχει έλεγχο ταυτότητας με One-Time Password (otp) για ένα σύστημα που δεν χρησιμοποιείται πλέον. Αυτό το module δεν πρέπει να χρησιμοποιείται.

- Το module `pam` εκτελεί τον έλεγχο κωδικών πρόσβασης μέσω του framework Pluggable Authentication Module (PAM).

  Ενότητες Επεξεργασίας

  authenticate

- Το module `pap` εκτελεί έλεγχο ταυτότητας για αιτήματα Access-Request που περιέχουν ένα χαρακτηριστικό User-Password.

  Ενότητες Επεξεργασίας

  authorize, authenticate

- Το module `passwd` διαβάζει και αποθηκεύει προσωρινά line-oriented αρχεία που είναι της μορφής '/etc/passwd'. Λαμβάνει ως δεδομένο ότι κάθε γραμμή αποτελείται από μια σειρά εγγραφών, που χωρίζονται από ένα οριοθέτη. Οι εγγραφές διαβάζονται από το αρχείο, αποθηκεύονται στην κρυφή μνήμη και στη συνέχεια τοποθετούνται σε ένα πακέτο. Το module `passwd` επιτρέπει την εξουσιοδότηση μέσω οποιουδήποτε αρχείου τύπου

passwd και την εξαγωγή οποιωνδήποτε χαρακτηριστικών από αυτά τα αρχεία.

Ενότητες Επεξεργασίας

authorization, accounting, post-proxy, recv-coa, send-coa

- Το module `perl` επιτρέπει στον server να καλεί ένα Perl Script. Σε αντίθεση με την εσωτερική γλώσσα, η Perl είναι μια πραγματική γλώσσα προγραμματισμού.
- Το module `preprocess` επεξεργάζεται τα εισερχόμενα αιτήματα RADIUS πριν παραδοθούν σε άλλες λειτουργικές μονάδες. Επιπλέον, ξαναγράφει κάποια ασυνήθιστα χαρακτηριστικά που δημιουργήθηκαν από ορισμένα NAS και τα μετατρέπει σε μια πιο τυπική μορφή.

  Ενότητες Επεξεργασίας

  authorize, preacct

- Το module `radutmp` γράφει ένα αρχείο τύπου utmp που παραθέτει τους χρήστες που είναι συνδεδεμένοι. Το αρχείο χρησιμοποιείται κυρίως για έλεγχο ταυτόχρονης χρήσης για να δει ποιος είναι συνδεδεμένος την κάθε χρονική στιγμή.

  Ενότητες Επεξεργασίας

  accounting, checksimul

- Το module `realm` χωρίζει το χαρακτηριστικό User-Name στα τμήματα "user" και "realm". Εάν βρεθεί το realm, το χαρακτηριστικό control:Proxy-To-Realm παίρνει την τιμή του realm.

  Ενότητες Επεξεργασίας

  authorize, preacct, recv-coa

- Το module `redis` είναι ένα αρχείο διαμόρφωσης για την ενότητα redis. Αυτή η ενότητα παρέχει συνδέσεις μόνο σε μια βάση δεδομένων redis και δυναμική επέκταση.
- Το module `rediswho` παρακολουθεί τη σύνδεση ενός χρήστη radutmp μέσω της μονάδας redis.

  Ενότητες Επεξεργασίας

  accounting

- Το module `replicate` αντιγράφει πακέτα σε έναν ή περισσότερους οικιακούς servers.
- Το module `smsotp` επεκτείνει τον FreeRADIUS με μια διεπαφή `socks` για τη δημιουργία και την επικύρωση κωδικών μιας χρήσης.
- Το module `soh` παρέχει υποστήριξη για το πρωτόκολλο Statement of Health (SoH) της Microsoft.

  Ενότητες Επεξεργασίας

  authorize
- Το module `sometimes` χρησιμοποιείται για σκοπούς εντοπισμού σφαλμάτων.
- Το module `sql` χρησιμοποιείται για τη διαμόρφωση της λειτουργικής μονάδας SQL. Τα σχήματα και τα ερωτήματα της βάσης δεδομένων βρίσκονται στους υποκαταλόγους sql/<DB>/main/schema.sql και sql/<DB>/main/queries.conf.
- Το module `sqlcounter` χρησιμοποιείται για τη διαμόρφωση του module IP Pool που βασίζεται σε SQL (rlm_sqlippool).
- Το module `sradutmp` παρέχει μια «ασφαλή» έκδοση του module radutmp, όπου το αρχείο sradutmp μπορεί να αναγνωστεί παγκοσμίως.

  Ενότητες Επεξεργασίας

  accounting, checksimul
- Το module `unix` ανακτά κωδικούς πρόσβασης και ενημερώνει το module `radutmp`.

  Ενότητες Επεξεργασίας

  authorization, accounting
- Το module `utf8` επιβάλλει το UTF-8 στα strings που προέρχονται από το NAS.
- Το module `wimax` υπολογίζει στοιχεία για το WiMAX. Αυτό το module πρέπει να χρησιμοποιείται μόνο σε δίκτυα WiMAX.

  Ενότητες Επεξεργασίας

  authorize, preacct, post-auth

- Το module `yubikey` αποκρυπτογραφεί και επικυρώνει τα στατικά και δυναμικά μέρη του OTP token.

- **Mods-enabled:** Ένας κατάλογος για την αποθήκευση αρχείων διαμόρφωσης. Η διαμόρφωση αφορά modules που έχουν ενεργοποιηθεί. Αυτά τα modules χρησιμοποιούνται από τον FreeRADIUS στη διαμόρφωση που εκτελείται. Σε πολλές περιπτώσεις, τα αρχεία αυτού του καταλόγου είναι σύνδεσμοι προς το αντίστοιχο αρχείο στον κατάλογο mods-available.
- **Mods-config:** Ένας κατάλογος που περιέχει επιπλέον αρχεία διαμόρφωσης για πολλές ενότητες. Αυτά τα αρχεία περιλαμβάνουν Perl Scripts, SQL Schemas κ.λπ.
- **Sites-available:** Ένας κατάλογος που περιέχει δείγματα "virtual-servers". Τα περισσότερα από αυτά δεν χρησιμοποιούνται. Ωστόσο υπάρχουν ως τεκμηρίωση και ως παραδείγματα "βέλτιστων πρακτικών".
- **Sites-enabled:** Ένας κατάλογος που περιέχει τη διαμόρφωση για "virtual-servers" που χρησιμοποιούνται από τον FreeRADIUS. Πρόκειται συνήθως για συνδέσμους προς αρχεία στον κατάλογο sites-available.

6.3.7 Αρχεία καταγραφής

Κατά την εκτέλεση του FreeRADIUS server, γίνεται καταγραφή συμβάντων σε αρχεία καταγραφής. Το αρχείο στο οποίο καταγράφονται τα συμβάντα προσδιορίζεται στο αρχείο *radiusd.conf* και είναι εξ' ορισμού το */var/log/freeradius/radius.log*. Επίσης, στην ενότητα *log* του *radiusd.conf* προσδιορίζονται τα συμβάντα που καταγράφονται. Ένα δεύτερο αρχείο καταγραφής είναι το */var/log/freeradius/radwtmp*, στο οποίο περιλαμβάνονται εγγραφές λογιστικής καταγραφής οι οποίες αντιστοιχούν σε συνδέσεις χρηστών μέσω ενός NAS. Για τον προσδιορισμό των χρηστών που έχουν πραγματοποιήσει συνδέσεις καθώς και της χρονικής διάρκειας αυτών των συνδέσεων μπορεί να εκτελεστεί η εντολή *radlast*, Για να λειτουργήσει η εντολή αυτή θα πρέπει είναι ενεργοποιημένο το *unix module* στην ενότητα *accounting* του εικονικού server. Τέλος, η εντολή *radwho* διαβάζει το αρχείο */var/log/freeradius/sradutmp* και εμφανίζει τους χρήστες με ενεργές συνόδους. Το αρχείο *sradutmp* δεν υπάρχει εξ' ορισμού και για να δημιουργηθεί θα πρέπει να ενεργοποιηθεί το *module sradutmp* στην ενότητα *accounting* του εικονικού server.

6.3.8 Διαδικασία Αυθεντικοποίησης

Όταν ο FreeRADIUS λαμβάνει μία αίτηση αυτή διεκπεραιώνεται αρχικά από την ενότητα `authorize`.

```
# Executing section authorize from
  file/etc/freeradius/sites-enabled/default
```

Η ενότητα `authorize` καθορίζεται σε έναν virtual-server. Τα χαρακτηριστικά ενός virtual-server είναι τα παρακάτω:

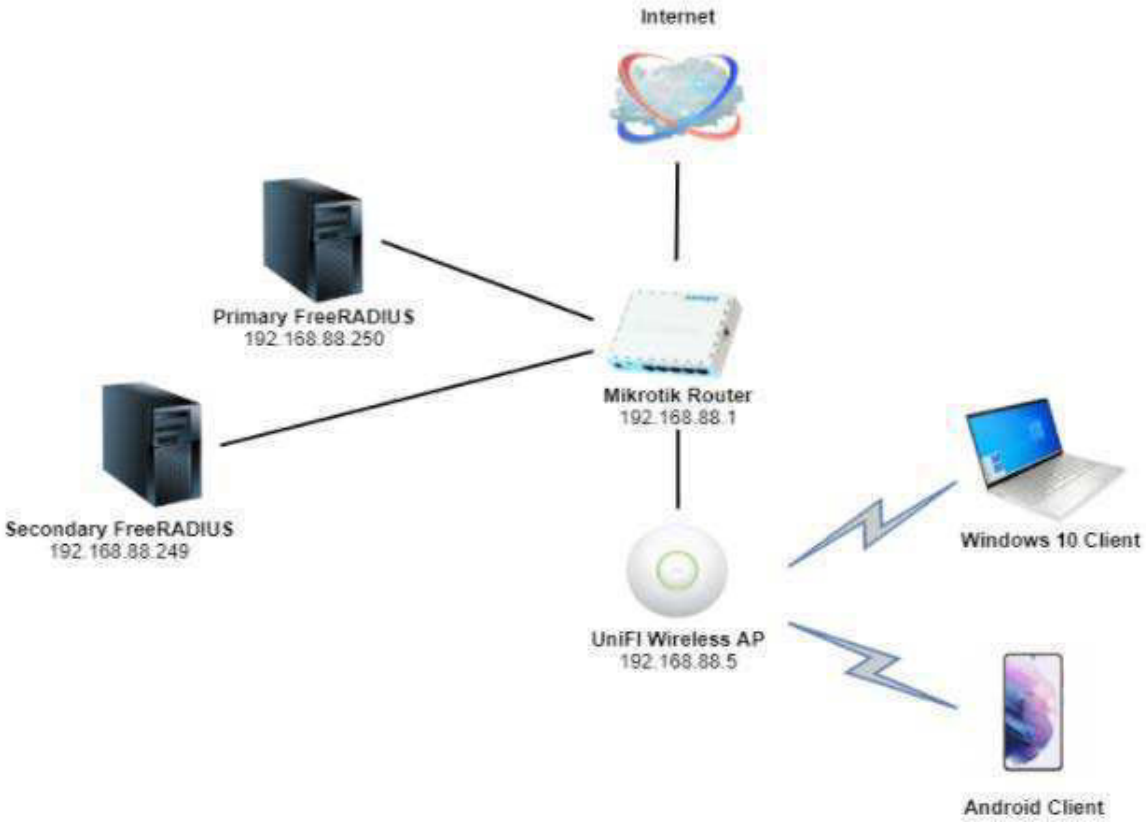
- Καθορίζονται στον κατάλογο sites-available, ο οποίος βρίσκεται κάτω από τον κατάλογο διαμόρφωσης του FreeRADIUS.
- Ενεργοποιούνται με την δημιουργία ενός link από το αρχείο του καταλόγου sites-available στο αρχείο του καταλόγου sites-enabled.
- Ο default virtual-server χειρίζεται όλες τις τυπικές αιτήσεις.
- Κάθε virtual server, συμπεριλαμβανομένου και του default, έχουν διάφορες ενότητες. Κάθε virtual server μπορεί να περιλαμβάνει τις εξής ενότητες: `listen, client, authorize, authenticate, post-auth, pre-proxy, post-proxy, preacct, accounting, and session`.

Όταν το αίτημα διεκπεραιώνεται από την ενότητα `authorize`, διάφορες ενότητες του FreeRADIUS κοιτούν τα AVP που περιέχονται στο Access-Request πακέτο. Αυτές οι ενότητες προσπαθούν να προσδιορίσουν τους μηχανισμούς και τις ενότητες που θα χρησιμοποιηθούν για την πιστοποίηση του χρήστη. Η ενότητα `authorize` μπορεί να αποφασίσει να απορρίψει ένα αίτημα με βάση την τιμή ενός συγκεκριμένου AVP. Αυτό θα έχει ως αποτέλεσμα ένα πακέτο Access-Reject να επιστρέψει στον client. Σε αυτή την περίπτωση δεν θα υπάρχει ανάγκη για έλεγχο ταυτότητας. Στην συνέχεια στην ενότητα `authorize` καθορίζεται ο τύπος της αυθεντικοποίησης (Auth-Type). Αυτό με τη σειρά του καθορίζει ποιο module μέσα στην ενότητα `authenticate` θα χρησιμοποιηθεί. Τέλος εκτελείται η ενότητα `post-auth` και το αποτέλεσμα στέλνεται πίσω στον client.

7. ΥΛΟΠΟΙΗΣΗ

Σε αυτό το κεφάλαιο περνάμε πλέον στο κύριο μέρος της εργασίας, όπου θα αναλυθεί η παραμετροποίηση του ασύρματου δικτύου καθώς και του εξοπλισμού που θα χρησιμοποιηθεί για την υλοποίηση του πρωτοκόλλου EAP-TPM.

7.1 Αρχιτεκτονική



Εικόνα 14: Τοπολογία δικτύου δοκιμαστικού περιβάλλοντος

7.2 Παραμετροποίηση του FreeRADIUS

Για την υλοποίηση του πρωτοκόλλου EAP-TPM χρησιμοποιήθηκε ο FreeRADIUS server, ο οποίος εγκαταστάθηκε σε λειτουργικό σύστημα Ubuntu Server 20.04. Η διαδικασία εγκατάστασης του FreeRADIUS περιγράφεται παρακάτω:

Αρχικά χρησιμοποιήθηκαν οι εντολές για την εγκατάσταση του FreeRADIUS server με τις προκαθορισμένες ρυθμίσεις και λειτουργίες.

```
$> sudo su

#> apt-get install freeradius
```

Στη συνέχεια στο αρχείο *clients.conf* προστέθηκε ένα πραγματικό σημείο πρόσβασης με τις παρακάτω ρυθμίσεις:

```
client ap1 {
      ipaddr = 192.168.88.5
      secret = AP1Secret
      require_message_authenticator = yes
      nastype = other
}
```

Ο FreeRADIUS server μπορεί να χρησιμοποιεί μία βάση δεδομένων SQL για την αποθήκευση στοιχείων των χρηστών και των NAS. Στην συγκεκριμένη υλοποίηση εγκαταστάθηκε η βάση δεδομένων MySQL με την παρακάτω διαδικασία:

Εγκατάσταση των FreeRADIUS modules.

```
#> apt-get install freeradius-mysql freeradius-utils -y
```

Εγκατάσταση της PHP.

```
#> apt-get install php-common php-gd php-curl php-mysql -y
```

Εγκατάσταση του MySQL server.

```
#> apt-get install mysql-server mysql-client -y
```

Δημιουργία του σχήματος της βάσης δεδομένων.

```
#> mysql -uroot -ppassword
mysql> CREATE DATABASE radius;
mysql> exit
```

Συμπλήρωση της βάσης με το σχήμα *radius.*

```
cd /etc/freeradius/3.0/mods-config/sql/main/mysql/
mysql -uroot -ppassword radius < schema.sql
mysql -uroot -ppassword radius < setup.sql
```

Ρύθμιση του FreeRADIUS ώστε να χρησιμοποιεί την SQL.

```
cd /etc/freeradius/3.0/mods-enabled
ln -s ../mods-available/sql sql
cd /etc/freeradius/3.0/sites-available/
vim default
```

Σε όλες τις κατηγορίες αντικαθιστούμε το λεκτικό “file” με το λεκτικό “sql”.

```
authorize {
.....
sql
....
}
accounting {
......
sql
....
}
post-auth {
......
sql
....
}
session{
......
sql
.....}
```

Τέλος τροποποιούμε το αρχείο sql.

```
cd /etc/freeradius/3.0/mods-available

vim sql

driver = "rlm_sql_mysql"

dialect = "mysql"

      server = "localhost"

      port = 3306

      login = "root"

      password = "password"

      radius_db = "radius"

      read_clients = yes
```

7.3 Secondary Freeradius

Για λόγους διαθεσιμότητας εγκαταστάθηκε και ένας δεύτερος FreeRadius server, ο οποίος παραμετροποιήθηκε με τον ίδιο ακριβώς τρόπο με τον πρώτο. Σε περίπτωση σφάλματος του κύριου FreeRADIUS server οι αιτήσεις για αυθεντικοποίηση εξυπηρετούνται από τον εφεδρικό.

Master FreeRADIUS: 192.168.88.250

Slave FreeRADIUS: 192.168.88.249

Επιπλέον έγινε συγχρονισμός των βάσεων τους με την παρακάτω διαδικασία [48]:

1ο Βήμα - Ρύθμιση του Master FreeRADIUS

Στο αρχείο `/etc/mysql/mysql.conf.d/mysqld.cnf` κάναμε τις εξής τροποποιήσεις:

```
server-id = 1
log_bin = /var/log/mysql/mysql-bin.log
binlog_do_db = radius
#bind-address = 127.0.0.1
```

Επανεκκίνηση του service mysql ώστε να πραγματοποιηθούν οι αλλαγές.

```
mysql> service mysql restart
```

Δημιουργία χρήστη για την αντιγραφή των δεδομένων μεταξύ των FreeRADIUS servers.

```
mysql> create user 'slave_user'@'%' identified by 'P@ssw0rd';
mysql> grant replication slave on *.* to 'slave_user'@'%';
```

Με την επόμενη εντολή εξάγαμε πληροφορίες, οι οποίες χρησιμοποιήθηκαν στην συνέχεια της διαδικασίας.

```
mysql> show master status;

+------------------+----------+--------------+------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000001 |      107 | radius       |                  |
+------------------+----------+--------------+------------------+
1 row in set (0.00 sec)
```

2ο Βήμα - Ρύθμιση του Slave FreeRADIUS

Για την παραμετροποίηση του Slave FreeRADIUS ακολουθήσαμε ξανά τα παραπάνω βήματα και στην συνέχεια αξιοποιήσαμε τις πληροφορίες που πήραμε στο τελευταίο βήμα εκτελώντας τις παρακάτω εντολές:

```
mysql> slave stop;

mysql> CHANGE MASTER TO MASTER_HOST = '192.168.88.250', MASTER_USER =
       'Slave_user', MASTER_PASSWORD = 'P@ssw0rd', MASTER_LOG_FILE =
       'mysql-bin.000001', MASTER_LOG_POS = 107;

mysql> slave start;
```

Στην συνέχεια εξάγαμε πληροφορίες, οι οποίες χρησιμοποιήθηκαν στην συνέχεια για την παραμετροποίηση του master FreeRADIUS.

```
mysql> show master status;

+------------------+----------+--------------+------------------+
| File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+------------------+----------+--------------+------------------+
| mysql-bin.000002 |      107 | radius       |                  |
+------------------+----------+--------------+------------------+
1 row in set (0.00 sec)
```

3ο Βήμα - Ολοκλήρωση της διαδικασίας

Τέλος εισάγαμε τα στοιχεία του παραπάνω πίνακα στον master FreeRADIUS εκτελώντας την παρακάτω εντολή:

```
mysql> slave stop;

mysql> CHANGE MASTER TO MASTER_HOST = '192.168.88.249', MASTER_USER =
       'Slave_user', MASTER_PASSWORD = 'P@ssw0rd', MASTER_LOG_FILE =
       'mysql-bin.000002', MASTER_LOG_POS = 107;

mysql> slave start;
```

Μετά το πέρας των παραπάνω βημάτων οι βάσεις δεδομένων των δύο FreeRADIUS συγχρονίστηκαν ώστε οποιαδήποτε αλλαγή γίνει στην βάση του ενός να καταχωρείται αυτόματα και στην βάση του άλλου. Με αυτό τον τρόπο εξασφαλίστηκε ότι σε περίπτωση σφάλματος του ενός server ο άλλος θα είναι ενημερωμένος με τα στοιχεία που έχουν καταχωρηθεί στην βάση του πρώτου, όπως για παράδειγμα τα στοιχεία των NAS.

7.4 Δημιουργία Πιστοποιητικών

Για την δημιουργία των πιστοποιητικών αρχικά έγινε μεταφορά των απαραίτητων αρχείων στον κατάλογο /etc/freeradius/3.0/certs και διαγραφή των δοκιμαστικών πιστοποιητικών [28]:

```
$> sudo su
#> cp /usr/share/doc/freeradius/examples/certs/* /etc/freeradius/3.0/certs
#> cd /etc/freeradius/3.0/certs
#> rm –f *.pem *.der *.csr *.crt *.key *.p12 serial.* index.txt*
```

Ρύθμιση των παραμέτρων του αρχείου ca.cnf, το οποίο χρησιμοποιείται για τη δημιουργία του αυτουπογραφόμενου πιστοποιητικού της αρχής πιστοποίησης.

```
sudo vim /etc/freeradius/3.0/certs/ca.cnf
```

a. Ενότητα CA_default

```
default_md = sha1
```

b. Ενότητα req

```
input_password = ……
output_password = ……
```

c. Ενότητα certificate_authority

```
countryName = ……
stateOrProvinceName = ……
localityName = ……
organizationName = ……
emailAddress = ……
commonName = "……"
```

Ρύθμιση των παραμέτρων του αρχείου server.cnf, το οποίο χρησιμοποιείται για τη δημιουργία του πιστοποιητικού του authentication server.

```
sudo vim /etc/freeradius/3.0/certs/server.cnf
```

a. Ενότητα CA_default

```
default_md = sha1
```

b. Ενότητα req

```
input_password = ……
output_password = ……
```

c. Ενότητα certificate_authority

```
countryName = ……
stateOrProvinceName = ……
localityName = ……
organizationName = ……
emailAddress = ……
commonName = "……"
```

Ρύθμιση των παραμέτρων του αρχείου client.cnf, το οποίο χρησιμοποιείται για τη δημιουργία του πιστοποιητικού του χρήστη.

```
sudo vim /etc/freeradius/3.0/certs/client.cnf
```

a. Ενότητα CA_default

```
default_md = sha1
```

b. Ενότητα req

```
input_password = ……
output_password = ……
```

c. Ενότητα certificate_authority

```
countryName = ……
stateOrProvinceName = ……
localityName = ……
organizationName = ……
emailAddress = ……
commonName = "……"
```

Εκτέλεση της παρακάτω εντολής για τη δημιουργία των ψηφιακών πιστοποιητικών:

```
root@ubuntu:/etc/freeradius/3.0/certs# make
```

Το αρχείο client.p12 περιλαμβάνει το ιδιωτικό κλειδί του χρήστη και θα πρέπει να αποθηκευτεί στον υπολογιστή του μαζί με το πιστοποιητικό της αρχής πιστοποίησης ca.der (το οποίο θα πρέπει να μετονομαστεί σε ca.crt για το Android). Το ιδιωτικό κλειδί του χρήστη απαιτείται για την αυθεντικοποίησή του εφόσον χρησιμοποιηθεί η μέθοδος EAP-TLS, ενώ το ψηφιακό πιστοποιητικό της αρχής πιστοποίησης είναι απαραίτητο για

την επαλήθευση του ψηφιακού πιστοποιητικού του authentication server όταν η μέθοδος που χρησιμοποιείται είναι μία εκ των EAP-TTLS, PEAP ή EAP-TLS.

Στη συνέχεια ρυθμίστηκαν οι παρακάτω παράμετροι στο αρχείο /etc/freeradius/3.0/sites-enabled/default:

```
server {
    listen {
        type = auth
        port = 1812
        ipaddr = 192.168.88.250
    }
    authorize {
        preprocess
        suffix
        filter_username
        eap {
                ok = return
        }
        expiration
        logintime
    }
    preacct {
        preprocess
        acct_unique
        suffix
    }
    accounting {
        detail
        radutmp
        attr_filter.accounting_response
    }
    session {
        radutmp
    }
    post-auth {
        remove_reply_message_if_eap
        Post-Auth-Type REJECT {
                attr_filter.access_reject
                eap
                remove_reply_message_if_eap

        }
    }
}
```

Τέλος ρυθμίστηκαν οι παρακάτω παράμετροι στο αρχείο /etc/freeradius/3.0/mods-enabled/eap:

```
eap {
        default_eap_type = tls
        timer_expire = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = ${max_requests}
        tls-config tls-common {
```

```
                private_key_password = server456
                private_key_file = /etc/freeradius/3.0/certs/server.key
                certificate_file = /etc/freeradius/3.0/certs/server.crt
                ca_file = /etc/freeradius/3.0/certs/ca.pem
                dh_file = ${certdir}/dh
                random_file = /dev/urandom
                ca_path = /etc/ssl/FreeRADIUS/
                cipher_list = "HIGH"
                ecdh_curve = "prime256v1"
                cipher_server_preference = yes
                verify {
                        tmpdir = /tmp/radiusd
                        client = "/usr/bin/openssl verify -CAfile ${..ca_file}
%{TLS-Client-Cert-Filename}"
                }
        }
        tls {
                tls = tls-common
        }
}
```

7.5 Mikrotik

Ως δρομολογητής χρησιμοποιήθηκε το Mikrotik hEX RB750Gr3, στο οποίο έγινε η βασική παραμετροποίηση με τα παρακάτω βήματα [40]:

1ο Βήμα - Set Bridge interface and IP Address

```
/interface bridge add name=local
/interface bridge port add interface=ether2 bridge=local
/ip address add address=192.168.88.1/24 interface=local
```

2ο Βήμα - Set up DHCP Server

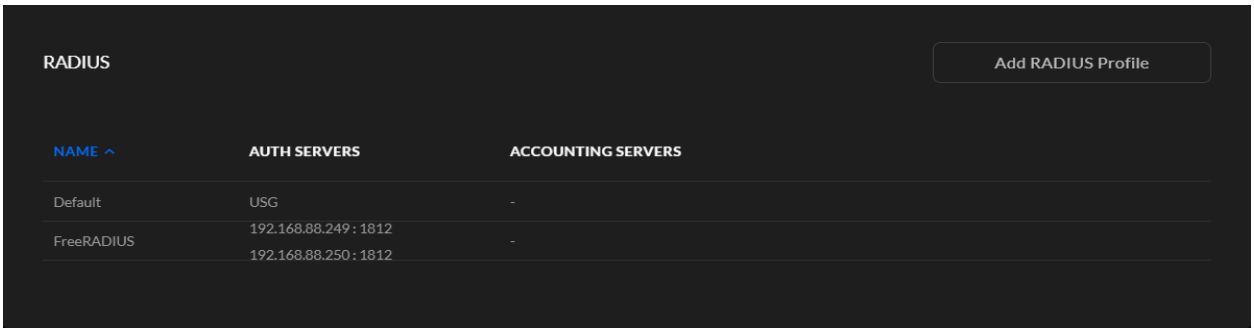
```
[admin@MikroTik] /ip dhcp-server setup [enter]

dhcp server interface: local [enter]

dhcp address space: 192.168.88.0/24 [enter]

gateway for dhcp network: 192.168.88.1 [enter]

addresses to give out: 192.168.88.2-192.168.88.254 [enter]

dns servers: 192.168.88.1 [enter]

lease time: 10m [enter]
```

7.6 UniFi Access Point

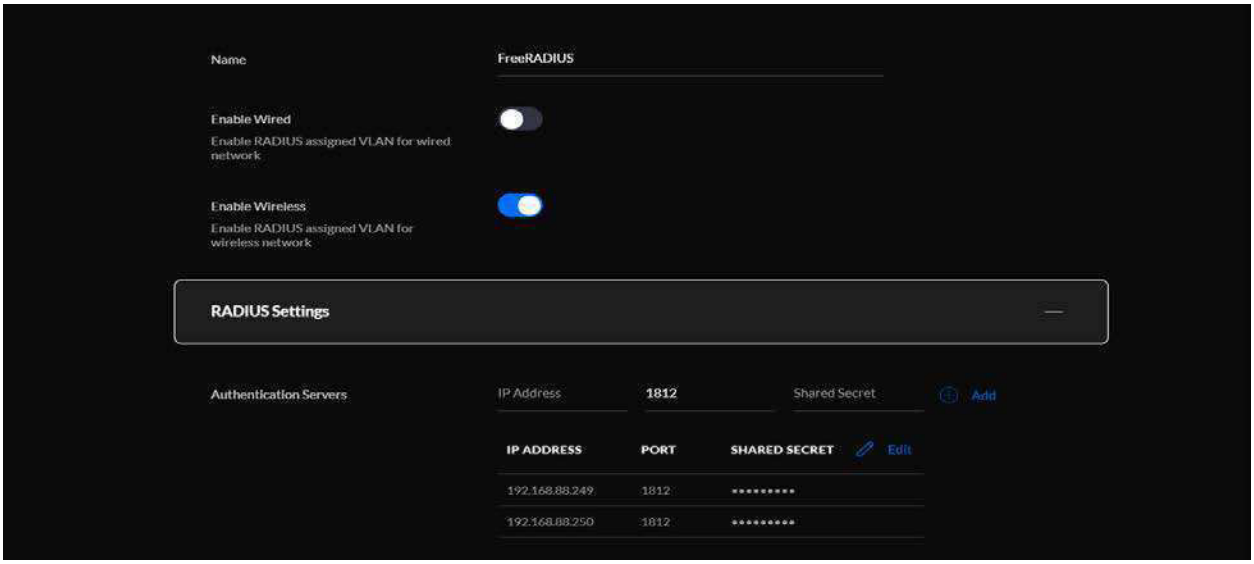
Για την έναρξη μιας συνόδου μεταξύ ενός supplicant και του AP θα πρέπει στο AP να γίνουν οι κατάλληλες ρυθμίσεις προκειμένου τα radius πακέτα να δρομολογούνται στον radius radius server ο οποίος είναι υπεύθυνος για το Authorization, το Authentication και το Accounting.

Στα πλαίσια αυτής της υλοποίησης χρησιμοποιήθηκε ως AP ένα UniFi, το οποίο παραμετροποιήθηκε όπως φαίνεται στις παρακάτω εικόνες:

Στην ενότητα Settings → Advanced Features → RADIUS δημιουργήθηκε το προφίλ με την ονομασία “FreeRADIUS” στο οποίο καταχωρήθηκαν τα στοιχεία των Primary και Secondary FreeRADIUS.



Εικόνα 15: UniFi AP - Καρτέλα Settings → Advanced Features → RADIUS (1/4)

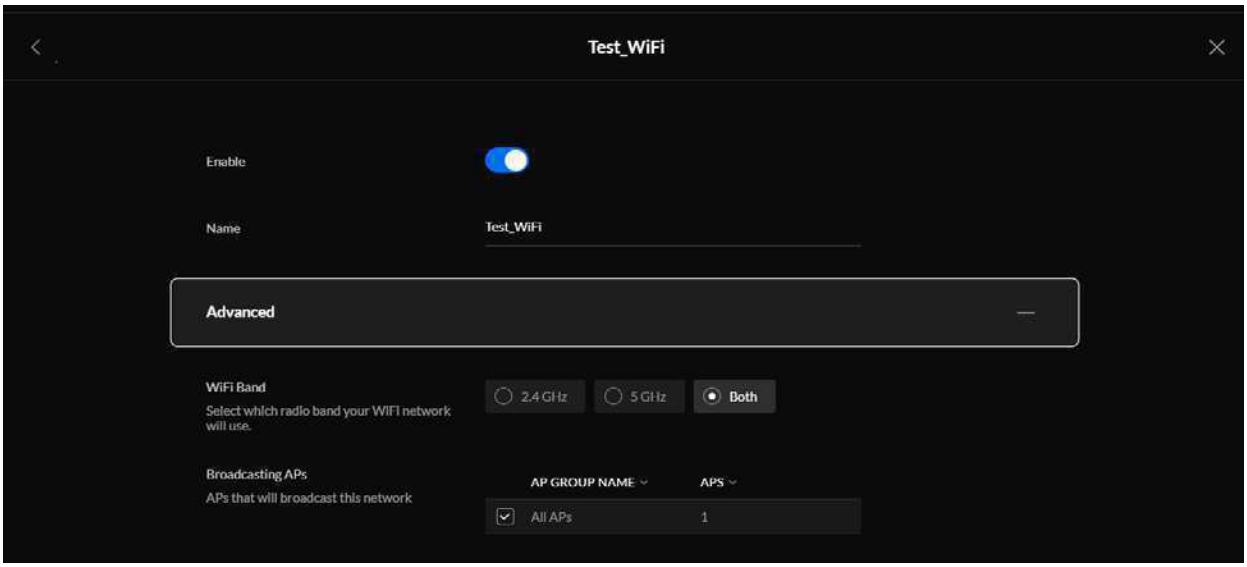


Εικόνα 16: UniFi AP - Καρτέλα Settings → Advanced Features → RADIUS (2/4)

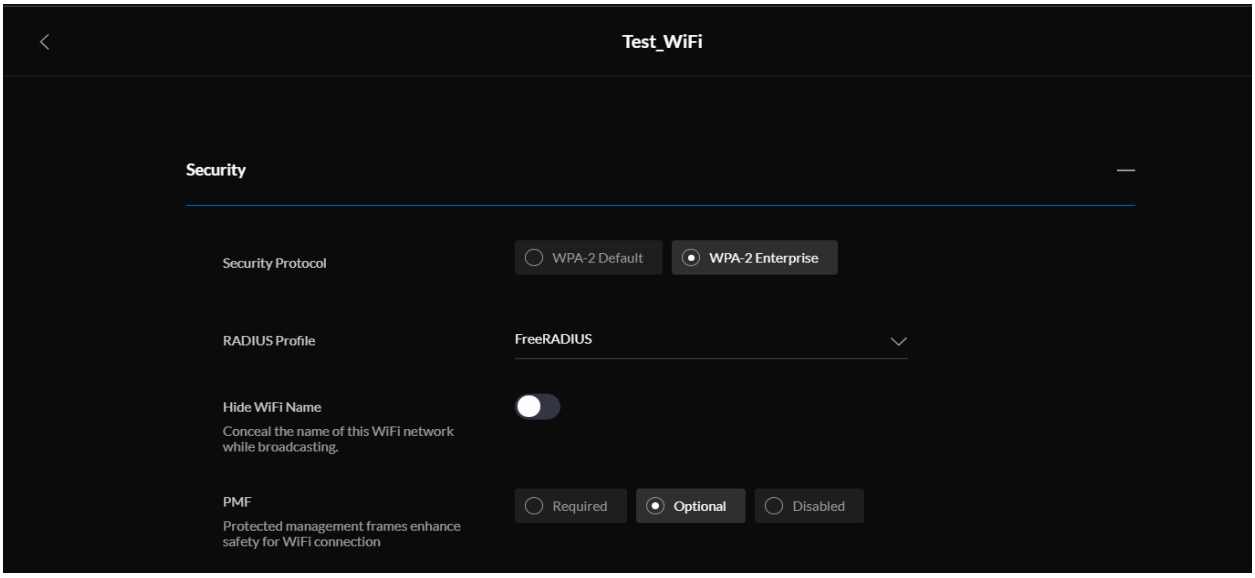
IP Address: 192.168.88.250 (Primary FreeRADIUS)
Radius Port: 1812
Shared Key: AP1Secret

IP Address: 192.168.88.249 (Secondary FreeRADIUS)
Radius Port: 1812
Shared Key: AP1Secret

Στην ενότητα Settings → WiFi δημιουργήθηκε το προφίλ TestWiFi με τις παρακάτω ρυθμίσεις:



Εικόνα 17: UniFi AP - Καρτέλα Settings → Advanced Features → RADIUS (3/4)



Εικόνα 18: UniFi AP - Καρτέλα Settings → Advanced Features → RADIUS (4/4)

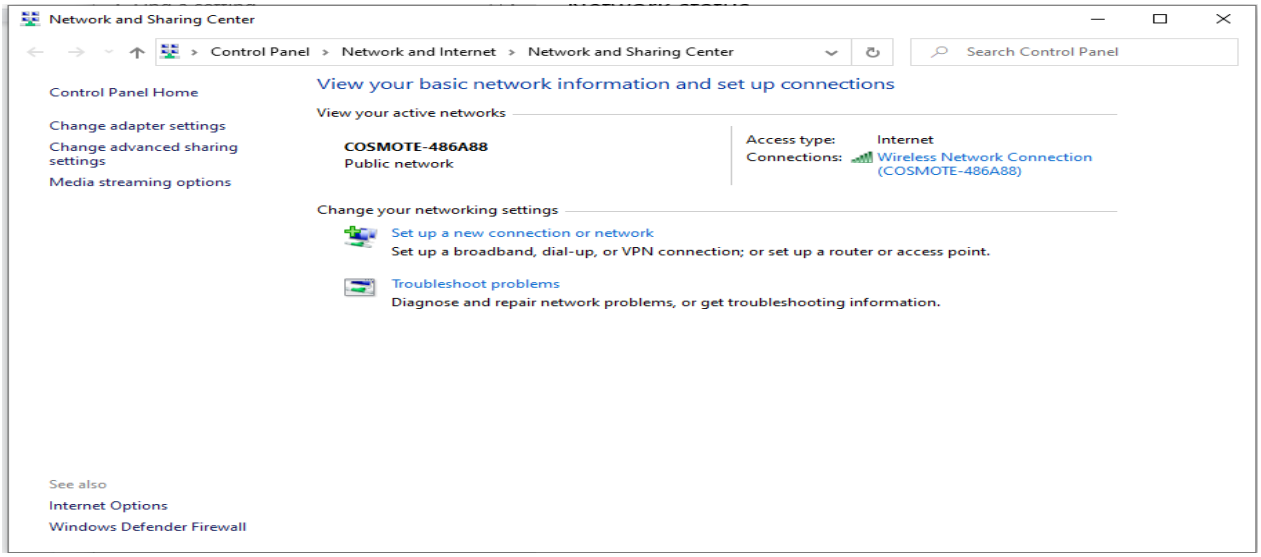
Name: TestWiFi
WiFi Band: Both
RADIUS Profile: FreeRADIUS

7.7 Προσθήκη ιδιωτικού κλειδιού & πιστοποιητικού CA στον supplicant

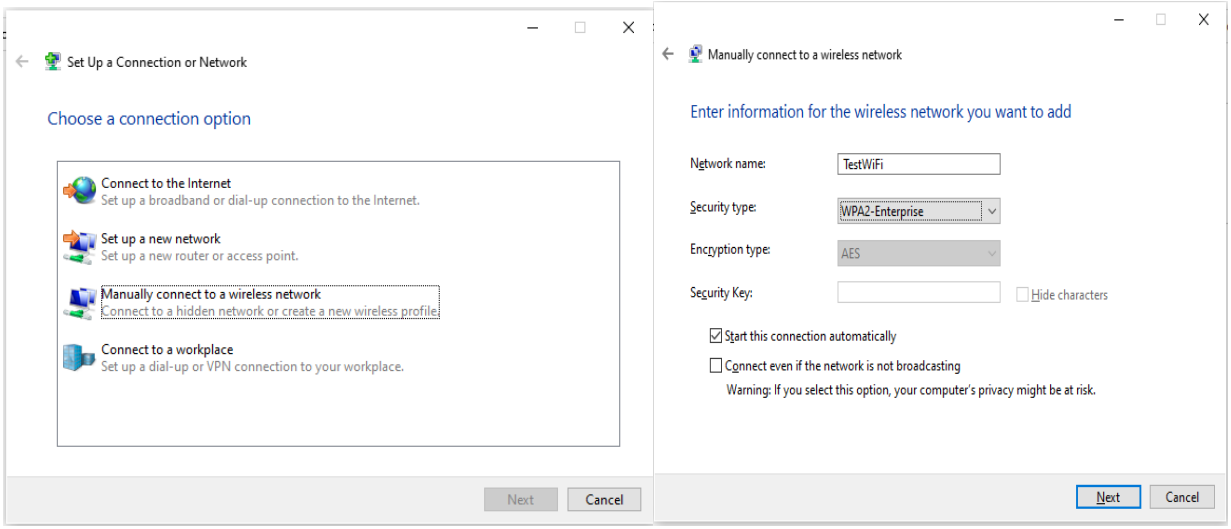
7.7.1 Windows 10

Για την ρύθμιση ασύρματης σύνδεσης eap-tls σε συσκευή με λειτουργικό Windows 10 εκτελέστηκαν τα παρακάτω βήματα:

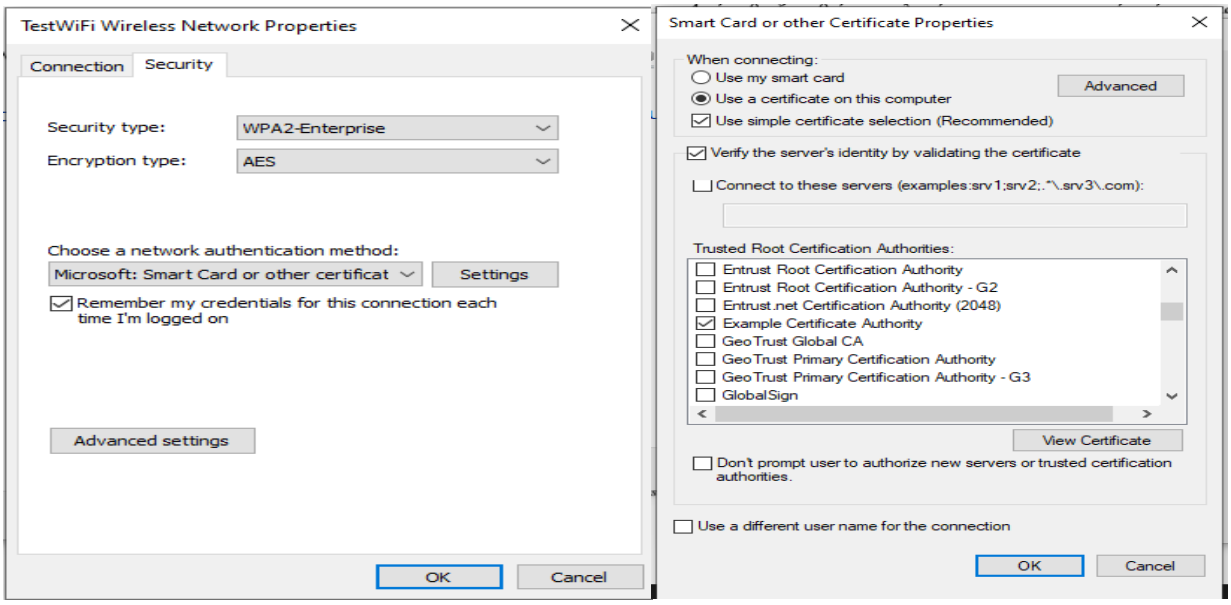
1. Εισαγωγή των πιστοποιητικών των CA και του χρήστη μέσω της εφαρμογής certmgr.msc.
2. Δημιουργία μιας νέας ασύρματης σύνδεσης μέσω του μενού του Πίνακα Ελέγχου.



Εικόνα 19: Windows 10 - Καρτέλα Network and Sharing Center



Εικόνα 20: Windows 10 - Καρτέλα Set Up a Network



Εικόνα 21: Windows 10 - Καρτέλα Wireless Network Properties

7.7.2 Android

Για την ρύθμιση ασύρματης σύνδεσης eap-tls σε συσκευή με λειτουργικό android 10 εκτελέστηκαν τα παρακάτω βήματα:

1. Αντιγραφή των root CA πιστοποιητικού και του πιστοποιητικού του χρήστη στην κάρτα SD της συσκευής.

2. Από το μενού WiFi → Πρόσθετες Ρυθμίσεις, επιλογή Εγκατάσταση Πιστοποιητικών και από εκεί επιλογή των πιστοποιητικών που βρίσκονται αποθηκευμένα στην κάρτα SD της συσκευής.

3. Από το μενού WiFi, επιλογή Προσθήκη Δικτύου.

4. Στην οθόνη που εμφανίζεται επιλογή των παρακάτω ρυθμίσεων:

Network SSID: Το SSID του δικτύου
Ασφάλεια: WPA2/WPA3-Enterprice
Μέθοδος EAP: TLS
Πιστοποιητικό CA: Το root CA που εγκαταστήσαμε στα βήματα 1 και 2
Πιστοποιητικό χρήστη: Το πιστοποιητικό χρήστη
Ταυτότητα: Οποιοδήποτε usename

5. Τέλος επιλογή Save για την σύνδεση στο ασύρματο δίκτυο.

7.8 Παραμετροποίηση του TPM

Για την υλοποίηση του TPM μπορεί να χρησιμοποιηθεί ένα μηχάνημα το οποίο διαθέτει ενσωματωμένο το TPM. Για την παραμετροποίηση του ώστε να συνδυαστεί με το πρωτόκολλο EAP-TLS μελετήθηκε ο κώδικας που φιλοξενείται στο GitHub.

Πάνω στη στοίβα λογισμικού tpm2-tss που ακολουθεί το TPM Software Stack των Trusted Computing Groups (TCG) (TSS 2.0) έχει υλοποιηθεί το tpm2-tss-engine, ο κώδικας του οποίου βρίσκεται στο GitHub και δημιουργεί στο TPM μία κρυπτογραφική μηχανή για το OpenSSL. Η υλοποίηση αυτή υποστηρίζει αποκρυπτογράφηση RSA και υπογραφές καθώς και υπογραφές ECDSA. Τα κλειδιά που χρησιμοποιούνται από αυτή την μηχανή βρίσκονται όλα κάτω από ένα κλειδί αποκρυπτογράφησης. Αυτό το κλειδί δημιουργείται σε κάθε επίκληση (αφού η δημιουργία κλειδιού ECC είναι ταχύτερη από αυτή του RSA). Επομένως, κανένα κλειδί SRK δεν χρειάζεται να χρησιμοποιηθεί εκ των προτέρων. Η τιμή αυθεντικοποίησης για την ιεραρχία αποθήκευσης, δηλαδή ο κωδικός πρόσβασης του κατόχου, θεωρείται ότι είναι σαφής (μηδενικού μήκους). Τα κλειδιά RSA δημιουργούνται με δυνατότητα υπογραφής καθώς και αποκρυπτογράφησης. Αυτό επιτρέπει τη χρήση όλων των κλειδιών RSA για οποιαδήποτε λειτουργία. Τα κλειδιά ECDSA δημιουργούνται ως κλειδιά ECDSA με δυνατότητα εκτέλεσης λειτουργιών υπογραφής.

Με την παρακάτω ακολουθία εντολών δημιουργείται ένα self-signed πιστοποιητικό χρησιμοποιώντας το κλειδί TPM. Η εντολή Openssl ορίζει το tpm2-tss ως μηχανή κρυπτογράφησης και δημιουργεί αυτο το πιστοποιητικό με βάση τις παρεχόμενες πληροφορίες διαμόρφωσης CSR [24].

```
$ tpm2tss-genkey -a rsa rsa.tss

$ openssl req -new -x509 -engine tpm2tss -key rsa.tss  -keyform engine -out
rsa.crt
```

Το tpm2-tss μπορεί να χρησιμοποιηθεί όπου χρησιμοποιείται το OpenSSL για τη δημιουργία ασφαλούς σύνδεσης καναλιού TLS [24].

```
./tpm2tss-genkey -a rsa rsa.tss

openssl req -new -x509 -engine tpm2tss -key rsa.tss  -keyform engine  -out
rsa.crt

openssl s_server -cert rsa.crt -key rsa.tss -keyform engine -engine tpm2tss -
accept 8443
```

Το πακέτο λογισμικού tpm2-openssl κάνει το TPM 2.0 προσβάσιμο μέσω του τυπικού OpenSSL API και των εργαλείων γραμμής εντολών, ώστε να μπορεί κανείς να προσθέσει υποστήριξη TPM σε (σχεδόν) οποιαδήποτε εφαρμογή βασίζεται στο OpenSSL 3.0. Στην περίπτωση της υλοποίησης αυτό βοηθάει στο να δοθεί πρόσβαση στο TPM μέσω της γραμμής εντολών του FreeRadius, ο οποίος χρησιμοποιεί το OpenSSL. Το tpm2-openssl υποστηρίζει τις παρακάτω λειτουργικότητες:

- Λειτουργίες συμμετρικής κρυπτογράφησης.
- Λειτουργίες ασύμμετρης κρυπτογράφησης.
- Δημιουργία τυχαίων αριθμών.
- Λειτουργίες κλειδιών.
- Λειτουργίες πιστοποιητικών ταυτότητας.

Για την περίπτωση της αυθεντικοποίησης σε ένα WiFi δίκτυο με την χρήση του πρωτοκόλλου EAP-TLS θα πρέπει να εγκατασταθεί και το πακέτο tpm2-pkcs11, του οποίου ο κώδικας βρίσκεται στο GitHub. Το PKCS#11 είναι ένα πρότυπο κρυπτογράφησης δημόσιου κλειδιού που ορίζει μια τυπική μέθοδο πρόσβασης σε κρυπτογραφικές υπηρεσίες από tokens/συσκευές όπως μονάδες ασφαλείας υλικού (hardware security modules-HSM), έξυπνες κάρτες κ.λπ. Στην περίπτωση μας εξετάζεται η σύνδεση μιας συσκευής με δυνατότητα Wi-Fi σε δίκτυο WPA2 Enterprise χρησιμοποιώντας το πρωτόκολλο EAP-TLS, όπου τα διαπιστευτήρια ελέγχου ταυτότητας διασφαλίζονται χρησιμοποιώντας ένα κλειδί που παράγεται από TPM 2.0 και είναι προσβάσιμο μέσω του προτύπου PKCS#11. Το WPA-Enterprise, που αναφέρεται επίσης ως λειτουργία WPA-802.1x, έχει σχεδιαστεί για εταιρικά δίκτυα και απαιτεί την ύπαρξη ενός RADIUS Server για τον έλεγχο ταυτότητας. Ο έλεγχος ταυτότητας των clients βασίζεται στο πρωτόκολλο EAP που περιλαμβάνει πολλούς τύπους σχημάτων ελέγχου ταυτότητας. Αυτό που χρησιμοποιείται σε αυτήν τη ρύθμιση είναι το EAP-TLS, που ορίζεται στο RFC 5216. Η παραμετροποίηση γίνεται στον supplicant και περιλαμβάνει τα παρακάτω βήματα [52]:

1ο Βήμα - Εγκατάσταση RADIUS Server CA στον supplicant

Τα πιστοποιητικά βρίσκονται στον κατάλογο πιστοποιητικών του RADIUS `certs`. Η εγκατάσταση του RADIUS Server CA γίνεται στη θέση:

```
/etc/pki/SSID/ca.pem
```

Η τοποθεσία της CA σε έναν Ubuntu Server, όπως είναι ο FreeRADIUS που έχει χρησιμοποιηθεί στην υλοποίηση είναι στην θέση:

```
/etc/freeradius/certs/ca.pem
```

2ο Βήμα - Δημιουργία του CSR (Certificate Signing Request)

Χρησιμοποιώντας το tpm2-pkcs11 ως κρυπτογραφική μηχανή για το openssl, δημιουργούμε το CSR στον Supplicant. Πρέπει να δημιουργηθεί ένα ιδιωτικό κλειδί στο σύστημα αποθήκευσης διαπιστευτηρίων του TPM 2.0 και το CSR προέρχεται από αυτό το κλειδί.

```
mkdir -p /etc/tpm2_pkcs11

export TPM2TOOLS_TCTI="device:/dev/tpmrm0"
export TPM2_PKCS11_TCTI="device:/dev/tpmrm0"

tpm2_ptool init
tpm2_ptool addtoken \
```

```
    --pid=1 \
    --sopin=sopin \
    --userpin=userpin \
    --label=label
tpm2_ptool addkey \
    --algorithm=rsa2048 \
    --label=label \
    --userpin=userpin
tpm2_ptool config \
    --key tcti \
    --value "device:/dev/tpmrm0" \
    --label label
TOKEN=`p11tool --list-token-urls | grep "token=label"`
export GNUTLS_PIN=userpin
export GNUTLS_SO_PIN=sopin
p11tool --login --list-all "${TOKEN}" --outfile p11tool.out
PRIVATE_KEY=`cat p11tool.out | grep private | awk '{ print $2 }'`
SUBJ="/C=FR/ST=Radius/L=Somewhere/O=Example
Inc./CN=testing/emailAddress=testing@test.com"
openssl req \
    -new \
    -engine pkcs11 \
    -keyform engine \
    -key "${PRIVATE_KEY};pin-value=userpin" \
    -subj "${SUBJ}" \
    -out client.csr
```

3ο Βήμα - Δημιουργία του πιστοποιητικού του client

Για να υπογραφεί το CSR και να παραχθεί ένα έγκυρο πιστοποιητικό του client για το σύστημα του supplicant, πρέπει να σταλεί το αρχείο CSR στον FreeRADIUS και να υπογραφεί χρησιμοποιώντας την CA που βρίσκεται στον κατάλογο `certs`. Από προεπιλογή, ο κωδικός πρόσβασης ιδιωτικού κλειδιού του πιστοποιητικού δοκιμής είναι “whatever”.

```
openssl ca \
    -batch \
    -keyfile ./ca.key \
    -cert ./ca.pem \
    -passin pass:whatever \
    -in client.csr \
    -out client.crt \
    -extensions xpclient_ext \
    -extfile xpextensions \
    -config client.cnf
```

Το πιστοποιητικό του client πρέπει να σταλεί στον Supplicant. Στη συνέχεια πρέπει να εγκατασταθεί στην θέση:

```
/etc/pki/SSID/client.crt.
```

4ο Βήμα - Παραμετροποίηση του wpa_supplicant

Στη συνέχεια πρέπει να δημιουργηθεί ένα αρχείο διαμόρφωσης του `wpa_supplicant`. Το χαρακτηριστικό `private_key` είναι ένα PKCS#11 URI που καθορίζει το ιδιωτικό κλειδί που είναι αποθηκευμένο στο TPM 2.0.

```
cat > wpa_supplicant.conf <<EOF
network={
    ssid="SSID"
    key_mgmt=WPA-EAP
    eap=TLS
    identity="testing"
    ca_cert="/etc/pki/SSID/ca.pem"
    client_cert="/etc/pki/SSID/client.crt"

private_key="pkcs11:model=Intel;manufacturer=Intel;serial=0000000000000000;to
ken=label;id=%32%62%37%30%65%62%36%32%66%33%32%62%31%63%65%37;object=0;type=p
rivate;pin-value=userpin"
}
EOF
```

Για να ξεκινήσει τη διαδικασία ελέγχου ταυτότητας, χρησιμοποιείται ο wpa_supplicant καθορίζοντας τη σωστή ασύρματη διεπαφή στο σύστημα του Supplicant.

```
wpa_supplicant -c wpa_supplicant.conf -i wlp1s0
```

5ο Βήμα - Διαμόρφωση του διαχειριστή δικτύου

Αρχικά καθορίζεται η τοποθεσία του PKCS11 Store που πρέπει να χρησιμοποιεί ο wpa_supplicant:

```
echo "TPM2_PKCS11_STORE=/etc/tpm2_pkcs11" >> /etc/sysconfig/wpa_supplicant
```

Επανεκκίνηση του wpa_supplicant.service με τη νέα διαμόρφωση:

```
systemctl restart wpa_supplicant.service
```

Προσθήκη της ακόλουθης διαμόρφωση σύνδεσης στο διαχειριστή δικτύου:

```
nmcli connection add type wifi ifname wlp1s0 con-name 'SSID' \
    802-11-wireless.ssid SSID \
    802-11-wireless-security.key-mgmt wpa-eap \
    802-1x.eap tls \
    802-1x.identity testing \
    802-1x.ca-cert /etc/pki/SSID/ca.pem \
    802-1x.client-cert /etc/pki/SSID/client.crt \
    802-1x.private-key' pkcs11:model=Intel;manufacturer=Intel;serial=00000000
00000000;token=label;id=%32%62%37%30%65%62%36%32%66%33%32%62%31%63%65%37;obje
ct=0;type=private;pin-value=userpin' \
    802-1x.private-key-password-flags not-required
```

Ενεργοποίηση της σύνδεσης:

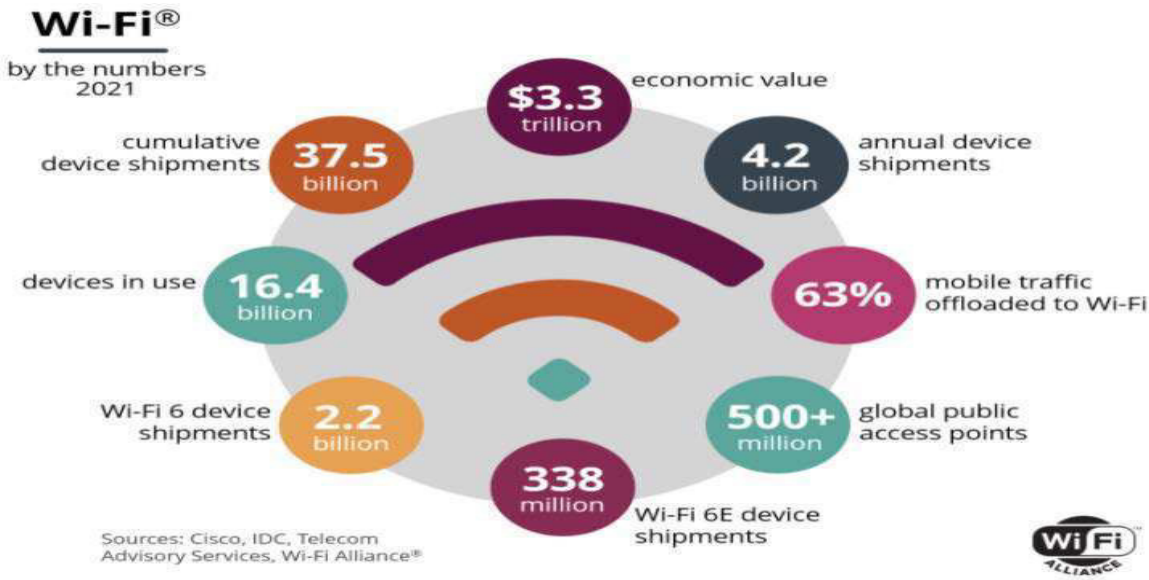
```
nmcli connection up SSID
```

8. ΥΙΟΘΕΤΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ WIFI

8.1 Η οικονομική αξία του WiFi

Τα WiFi δίκτυα αποτελούν μία από τις μεγαλύτερες επιτυχίες της εποχής της τεχνολογίας και θεωρούνται κλειδί για τη συνεχιζόμενη κοινωνική και οικονομική ανάπτυξη. Άτομα, οικογένειες, κυβερνήσεις και παγκόσμιοι οργανισμοί εξαρτώνται από το WiFi στην καθημερινότητα τους. Η δημιουργία WiFi δικτύων βοήθησε στον μετασχηματισμό της εκπαίδευσης, διεύρυνε τις δυνατότητες των παρόχων υγειονομικής περίθαλψης και βοήθησε στη δημιουργία νέων τεχνολογιών, βιομηχανιών και σταδιοδρομιών σε όλο τον κόσμο - ακόμη και στο διάστημα.

Εκτός από τα γνωστά κοινωνικά του οφέλη, το WiFi παρέχει σημαντικά οφέλη σε οικονομίες παγκοσμίως. Η παγκόσμια οικονομική αξία του WiFi το 2021 εκτιμάται σε 3,3 τρισεκατομμύρια δολάρια ΗΠΑ, σύμφωνα με μελέτη που ανατέθηκε από την WiFi Alliance [53]. Μέχρι το 2025 η αξία αυτή αναμένεται να αυξηθεί στα 4,9 τρισεκατομμύρια δολάρια.



Εικόνα 22: Το WiFi σε αριθμούς

Η οικονομική αξία του Wi-Fi για κάθε χώρα αναπτύχθηκε με την αξιολόγηση πολλών βασικών παραγόντων και τις παγκόσμιες εξελίξεις που επηρεάζουν τη βιομηχανία και που συμβάλλουν στην οικονομική αξία του WiFi για το 2021 και πέρα. Οι οικονομολόγοι συνδύασαν τους υπολογισμούς κάθε παράγοντα με επιπτώσεις συγκεκριμένες για κάθε χώρα. Μερικοί από τους παράγοντες που αξιολογήθηκαν ενδεικτικά ήταν:

- **Δωρεάν WiFi:** Οφέλη χρηστών για πρόσβαση σε δωρεάν δίκτυα WiFi σε δημόσιες τοποθεσίες, συμπεριλαμβανομένων και δημόσιων οργανισμών.
- **Επιχειρήσεις:** Εξοικονόμηση χρημάτων μέσω δικτύων WiFi που οδηγούν στην ψηφιοποίηση των επιχειρηματικών λειτουργιών, μείωση των καλωδίων των

υποδομών, χειρισμός περισσότερης κίνησης δεδομένων και ανάπτυξη καινοτόμων εφαρμογών.

- **Βιομηχανία γύρω από το WiFi**: Εταιρείες που φέρνουν συσκευές και εξοπλισμό WiFi στην αγορά και αυτές που παρέχουν υπηρεσίες σχετικές με το Wi-Fi, όπως ανάλυση cloud, προσωπική πρόσβαση Wi-Fi, και υπηρεσίες ροής.
- **Αναπτυσσόμενες οικονομίες**: Υψηλές τιμές κινητής τηλεφωνίας και χαμηλότερη διείσδυση ευρυζωνικών αποτελεσμάτων σε WiFi παρέχουν μεγάλη αξία σε πολλές αναπτυσσόμενες οικονομίες.
- **Νέες πηγές αξίας:** Η νέα τεχνολογία συμβάλλει στην αύξηση των εφαρμογών IoT, περισσότερος εφαρμογές που βασίζονται σε WiFi και μεγαλύτερη δυνατότητα εφαρμογής AR/VR.
- **Πανδημία κορωνοϊού**: Απρόσμενη αναστάτωση στην παγκόσμια οικονομία λόγω του COVID-19. Η πανδημία ανάγκασε τις οικονομίες να χρησιμοποιούν WiFi για να διατηρούν τις επιχειρήσεις και τις κρίσιμες λειτουργίες τους, αλλάζοντας τον τρόπο που λειτουργεί ο κόσμος και παραμένει συνδεδεμένος.

8.1.1 Το WiFi σε Επιχειρηματικά Περιβάλλοντα

Τα WiFi δίκτυα αποτελούν πλέον επιλογή ολοένα και περισσότερων επιχειρήσεων. Αυτό συμβαίνει γιατί υπάρχουν περισσότερες συσκευές που υποστηρίζουν την τεχνολογία WiFi, οι οποίες μπορούν να προσφέρουν βιομηχανικές προδιαγραφές προστασίας και απόδοσης που περιμένουν οι διαχειριστές επιχειρησιακών δικτύων.

Η νέα γενιά των WiFi δικτύων μπορεί να προσφέρει την υψηλότερη απόδοση που διατίθεται σε εταιρικά δίκτυα καθώς βελτιώνει τη χωρητικότητα και την απόδοση ολόκληρου του δικτύου, χρησιμοποιώντας χαρακτηριστικά που έχουν σχεδιαστεί για να διασφαλίζουν ότι κάθε συνδεδεμένη συσκευή να λειτουργεί στο βέλτιστο επίπεδο, συμπεριλαμβανομένων των παλαιών συσκευών. Άλλα χαρακτηριστικά που κάνουν πιο αποτελεσματική την χρήση του φάσματος έχουν ως αποτέλεσμα εξαιρετικά αποδοτικά δίκτυα που παρέχουν αυξημένη ταχύτητα και χωρητικότητα.

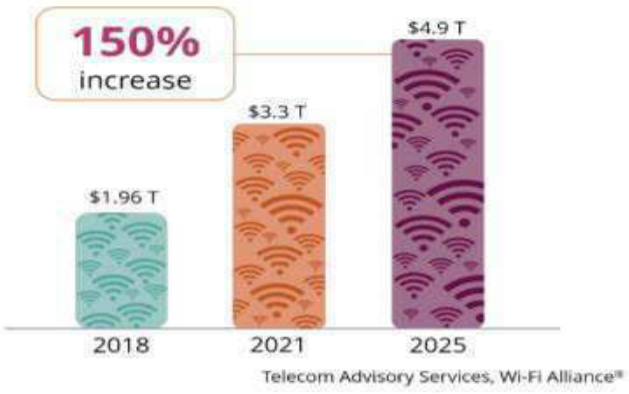
Τα εν λόγω δίκτυα είναι ικανά να υποστηρίξουν ένα εξελισσόμενο επιχειρηματικό περιβάλλον που χαρακτηρίζεται από αυξημένη κινητικότητα των εργαζομένων, ευέλικτους χώρους εργασίας και κατανεμημένες ομάδες που χρησιμοποιούν εργαλεία αποθήκευσης και συνεργασίας με βάση το cloud. Οι διαχειριστές δικτύου μπορούν να φιλοξενήσουν τις πρόσθετες συσκευές που φέρνουν οι εργαζόμενοι στο χώρο εργασίας και οι συσκευές που υποστηρίζουν αυτήν την τεχνολογία είναι έτοιμες να χειριστούν τις σημερινές αυξανόμενες απαιτήσεις συνδεσιμότητας και να υποστηρίξουν την αυξημένη ευελιξία και παραγωγικότητα ενός πιο κινητού εργατικού δυναμικού. Όλα αυτά τα χαρακτηριστικά σε συνδυασμό με δυνατούς μηχανισμούς αυθεντικοποίησης των χρηστών μπορούν να προσφέρουν ισχυρή προστασία των χρηστών και των δεδομένων που διακινούνται σε ένα τέτοιο δίκτυο.

Στον επιχειρηματικό κόσμο τεράστιο ρόλο έπαιξε και η έξαρση της πανδημίας του κορωνοϊού (COVID-19). Αρκετές μελέτες επικεντρώθηκαν στην εκτίμηση του μεριδίου

των εργαζομένων που θα μπορούσαν και μελλοντικά να εργάζονται από το σπίτι. Οι έρευνες έδειξαν [54] πως οι χώρες με πιο προηγμένα επίπεδα ψηφιοποίησης μπόρεσαν να στηρίξουν την τηλεργασία με αποτέλεσμα να συνεχίσει να λειτουργεί η οικονομία τους. Αυτό το καθεστώς υπάρχει μεγάλη πιθανότητα να γίνει η νέα πραγματικότητα στο μέλλον. Με μεγάλο ποσοστό λοιπόν εργαζομένων από το σπίτι τους είναι επόμενο πως οι επιχειρήσεις δεν θα έχουν την ανάγκη δημιουργίας μεγάλων ενσύρματων δικτύων στους χώρους αλλά θα μπορούν να επενδύσουν σε ασύρματες υποδομές που έχουν ευελιξία στην επεκτασιμότητα για κάλυψη μελλοντικών αναγκών.

8.1.2 Μελλοντικές προβλέψεις

Σύμφωνα με μελέτες [53] που έγιναν το 2018, υπήρχαν εκτιμήσεις πως η οικονομική αξία των WiFi δικτύων θα μεγάλωνε κατά 1,96 τρισεκατομμύριο δολάρια.



Εικόνα 23: Η Οικονομική αξία του WiFi

Τα αποτελέσματα ωστόσο καταδεικνύουν αύξηση σε οικονομική αξία κατά σχεδόν 3 τρισεκατομμύρια δολάρια, ή αλλιώς 150% ανάπτυξη, από το έτος 2018 έως το 2025, υπογραμμίζοντας ότι η τεχνολογία Wi-Fi είναι μία από τις κυρίαρχες οικονομικούς κινητήρες της ψηφιακής οικονομίας.

Συγκεκριμένα για την Ευρωπαϊκή Ένωση υπολογίζεται ότι η οικονομική αξία του WiFi για το 2021 υπολογίζονται σε 457,6 δισεκατομμύρια δολάρια και αναμένεται να αυξηθεί στα 637,2 δισεκατομμύρια δολάρια μέχρι του 2025. Η ανάπτυξη της αξίας των WiFi δικτύων τροφοδοτείται από την ενίσχυση της τεχνολογίας IoT, την αυξανόμενη υιοθέτηση των AR/VR τεχνολογιών και της αυξανόμενης σημασίας του δωρεάν Wi-Fi. Οι τιμές υποθέτουν ότι 500 MHz φάσματος είναι εγκεκριμένα για χρήση από το WiFi για το έτος 2021. Οι χώρες της Ευρωπαϊκής Ένωσης θα βιώσουν μεγαλύτερα οφέλη εάν διατεθεί περισσότερο φάσμα.

8.2 Πλεονεκτήματα ενός WiFi Δικτύου

Όπως εύκολα γίνεται αντιληπτό υπάρχουν πολλά πλεονεκτήματα από την εγκατάσταση ενός WiFi δικτύου σε επιχειρήσεις και δημόσιους οργανισμούς. Οι κύριοι άξονες σύγκρισης ανάμεσα σε ένα ασύρματο και ένα ενσύρματο δίκτυο είναι η ταχύτητα, η αξιοπιστία, η ασφάλεια, οι καθυστερήσεις και το κόστος εγκατάστασης.

Πίνακας 2: Σύγκριση WiFi και Ethernet

	Ethernet	WiFi
Ταχύτητα	Υψηλότερη ταχύτητα μεταφοράς δεδομένων	Χαμηλότερη ταχύτητα μεταφοράς δεδομένων
Αξιοπιστία	Σταθερή ταχύτητα	Η ταχύτητα εξαρτάται από εξωτερικούς παράγοντες και παρεμβολές
Ασφάλεια	Δεν απαιτείται πάντα κρυπτογράφηση των δεδομένων για ασφαλή επικοινωνία	Πρέπει να κρυπτογραφηθούν τα δεδομένα κατά την επικοινωνία
Καθυστερήσεις	Χαμηλότερες	Υψηλότερες
Κόστος Εγκατάστασης	Υψηλότερο - Απαιτείται υποδομή	Χαμηλότερο - Εύκολη εγκατάσταση

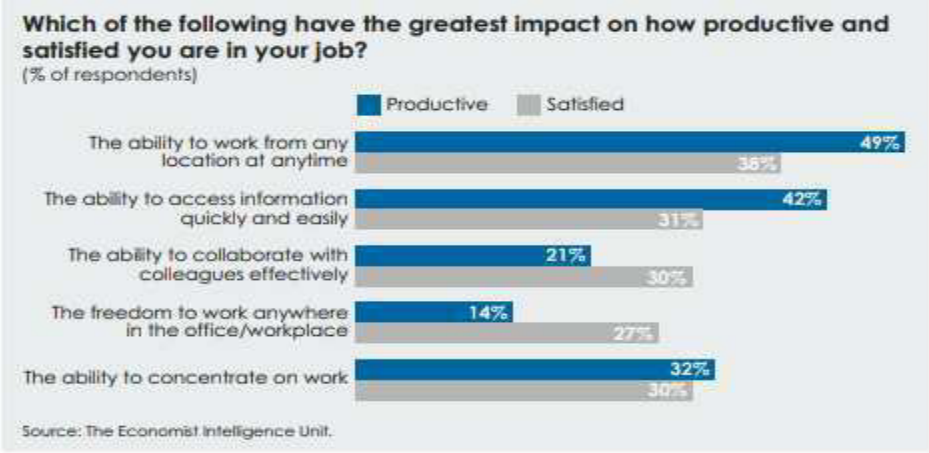
Πιο συγκεκριμένα η υιοθέτηση ενός ασύρματου δικτύου πρόσβασης μπορεί να έχει τα εξής πλεονεκτήματα:

- **Κόστος εγκατάστασης:** Σε γενικές γραμμές, το κόστος εγκατάστασης ενός ασύρματου δικτύου είναι σχετικά φθηνό, εκτός εάν το δίκτυό σας απαιτεί πρόσθετο εξοπλισμό, όπως ασύρματους επαναλήπτες ή δρομολογητή επαγγελματικής ποιότητας. Οι ασύρματοι επαναλήπτες αυξάνουν την ισχύ του σήματος και ένας δρομολογητής επαγγελματικής ποιότητας παρέχει πιο αξιόπιστη σύνδεση και βελτιωμένους ελέγχους ασφαλείας.
- **Εγκατάσταση:** Συνολικά, η εγκατάσταση ενός ασύρματου δικτύου είναι ταχύτερη και ευκολότερη επειδή απαιτεί λιγότερο εξοπλισμό. Επιπλέον, δεν χρειάζεται να αφιερωθεί χρόνο στη σύνδεση κάθε συσκευής στο δίκτυο χρησιμοποιώντας καλώδια Ethernet.
- **Κινητικότητα:** Τα ασύρματα δίκτυα επιτρέπουν στους υπαλλήλους ενός γραφείου να έχουν ευελιξία πρόσβασης στο δίκτυο από οποιαδήποτε τοποθεσία χρησιμοποιώντας οποιοδήποτε τύπο ασύρματης ενεργοποιημένης συσκευής. Δεν υπάρχουν προβλήματα με τα καλώδια και όλη η συνδεσιμότητα μπορεί να επιτευχθεί χωρίς τους περιορισμούς των φυσικών καλωδίων.

Στα οφέλη της εγκατάστασης ενός ασύρματου δικτύου έρχεται να προστεθεί και ο παράγοντας του κέρδους από την παραγωγικότητα του προσωπικού. Τα τελευταία δέκα χρόνια η πρακτική BYOD έχει κερδίσει έδαφος σε πολλές επιχειρήσεις. Οι κινητές συσκευές αυξάνουν την ανεξαρτησία των χρηστών και όλο και περισσότεροι εργοδότες επιτρέπουν την ασφαλή σύνδεση των εργαζομένων σε ένα ασφαλές εταιρικό δίκτυο. Με τα πλεονεκτήματα της τεχνολογίας WiFi οι εργαζόμενοι μπορούν να παραμένουν συνδεδεμένοι οπουδήποτε χωρίς να εξαρτώνται από έναν σταθερό υπολογιστή χωρίς να μπορούν να απομακρυνθούν από το γραφείο τους. Ο συνδυασμός ενός αξιόπιστου

ασύρματου δικτύου μα μία κινητή συσκευή κάνει το περιβάλλον εργασίας να είναι πιο ευέλικτο σε αλλαγές και λιγότερο εξαρτημένο από χρονικά και τοπικά περιθώρια.

Υπό αυτές τις συνθήκες οι εργαζόμενοι μπορούν να φέρνουν τις δικές τους έξυπνες συσκευές στην εργασία τους και μπορούν να εργαστούν με τρόπους που δεν υπήρχαν στο παρελθόν. Για παράδειγμα μπορούν να απαντούν σε e-mails και να αναθέτουν εργασίες ακόμα και όταν βρίσκονται εκτός γραφείου. Σύμφωνα με έρευνα του 2016 του Economist Intelligence Unit [50] στην οποία συμμετείχαν 1.865 εργαζόμενοι, όσοι ήταν συνδεδεμένοι στο διαδίκτυο μέσω κινητής συσκευής συνέβαλαν στην αύξηση της παραγωγικότητας για αυτήν την επιχείρηση κατά 16% και σε αύξηση της δημιουργικότητας των εργαζομένων κατά 18%. Εκτός από την παραγωγικότητα, διαπιστώθηκε ότι η εργασιακή ικανοποίηση αυξήθηκε κατά 23% και η πίστη στην εταιρεία αυξήθηκε κατά 21%.



Εικόνα 24: Επίδραση της ασύρματης πρόσβασης στην παραγωγικότητα των χρηστών

8.3 Εγκατάσταση ενός WiFi Δικτύου

Τα ασύρματα δίκτυα πρόσβασης μπορούν να υιοθετηθούν σε διάφορες δομές, όπως για παράδειγμα οικιακή χρήση, έξυπνες πόλεις, επιχειρήσεις και δημόσιοι οργανισμοί. Σε κάθε περίπτωση ωστόσο πρέπει να γίνει στάθμηση των αναγκών ώστε να βρεθεί το κατάλληλο μοντέλο δικτύου για κάθε σκοπό χρήσης.

8.3.1 Κριτήρια Επιλογής

Όταν υπάρχει ανάγκη επιλογής ανάμεσα στην εγκατάσταση ενός ασύρματου και ενός ενσύρματου δικτύου θα πρέπει να σταθμίσουμε ορισμένους παράγοντες και να ακολουθήσουμε συγκεκριμένη συλλογιστική, ώστε να πάρουμε την ορθότερη απόφαση για τον οργανισμό μας. Θα πρέπει λοιπόν να απαντήσουμε τα παρακάτω ερωτήματα ώστε να εξάγουμε τα σωστά συμπεράσματα [55]:

- **Ασφάλεια:** Ένας οργανισμός θα πρέπει να επενδύσει πολλά στην ασφάλεια του δικτύου της και των συσκευών που είναι συνδεδεμένες σε αυτό. Επιθέσεις μπορούν να πραγματοποιηθούν είτε σε ασύρματα είτε σε ενσύρματα

περιβάλλοντα. Ωστόσο στην πρώτη περίπτωση θεωρείται πιο εύκολη η πρόσβαση καθώς ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στα σήματα που μεταδίδονται. Θα πρέπει λοιπόν ο οργανισμός που έχει σκοπό να εγκαταστήσει ένα ασύρματο δίκτυο να επενδύσει στην ασφάλεια του δικτύου. Όπως αναφέρθηκε και σε προηγούμενα κεφάλαια ένας τρόπος είναι η ασφαλής αυθεντικοποίηση χρηστών και συσκευών με την χρήση αξιόπιστων πρωτοκόλλων, όπως το EAP-TPM που περιγράφηκε παραπάνω.

- **Σκοπος χρήσης:** Μετά την ασφάλεια, η επόμενη ερώτηση αφορά τον σκοπό χρήσης του δικτύου. Συγκεκριμένα, εάν το δίκτυο χρησιμοποιείται για τον έλεγχο ή την παρακολούθηση μιας διαδικασίας. Ο σκοπός χρήσης ενός δικτύου αποτελεί πρωταρχικό παράγοντα που επηρεάζει αν θα χρησιμοποιηθούν ενσύρματα ή ασύρματα μέσα σε αυτό.

- **Αξιοπιστία:** Το επίπεδο αξιοπιστίας που θέλουμε να πετύχουμε μέσα στο δίκτυο μας είναι ο επόμενος παράγοντας επιλογής και εξαρτάται από το είδος των συσκευών που σκοπεύουμε να χρησιμοποιήσουμε σε αυτό. Πολλές φορές οι ενσύρματες συσκευές θεωρούνται περισσότερο αξιόπιστες, ωστόσο με την κατάλληλη παραμετροποίηση ακόμα και ασύρματες συσκευές μπορούν να θεωρηθούν ασφαλείς μέσα σε ένα δίκτυο.

- **Καθυστερήσεις:** Γενικά, στα ασύρματα δίκτυα υπάρχει μεγαλύτερη πιθανότητα καθυστερήσεων συγκριτικά με τα ενσύρματα. Ωστόσο, υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν την καθυστέρηση κατά την επικοινωνία των δεδομένων. Για παράδειγμα η ταχύτητα μπορεί να επηρεαστεί από την ταχύτητα του επεξεργαστή των υπολογιστών, τη διαθέσιμη μνήμη, τον ρυθμό επικοινωνίας, τις αποστάσεις, το χρησιμοποιούμενο μέγεθος πακέτου δεδομένων και το πρωτόκολλο επικοινωνίας. Σε ορισμένες περιπτώσεις λοιπόν οι παράγοντες αυτοί μπορεί να μην επηρεάζουν την καθυστέρηση με κανέναν τρόπο.

- **Εύρος ζώνης:** Διαφορετικοί είναι οι παράγοντες που επηρεάζουν το εύρος ζώνης στα ενσύρματα και τα ασύρματα δίκτυα. Στην πρώτη περίπτωση το κανάλι επικοινωνίας είναι ο χαλκός ή η οπτική ίνα και το εύρος ζώνης επηρεάζεται από παράγοντες όπως η θερμοκρασία και η απόσταση, ενώ στην δεύτερη περίπτωση το κανάλι επικοινωνίας είναι ο κενός αέρας και επηρεάζεται από φαινόμενα όπως η θερμοκρασία, η υγρασία, η ατμοσφαιρική πίεση και οι παρεμβολές. Σημαντικό ρόλο λοιπόν για την επιλογή του δικτύου παίζει το μέρος που θέλουμε να το εγκαταστήσουμε και τα φαινόμενα που κάθε φόρα θα μπορούν να το επηρεάσουν.

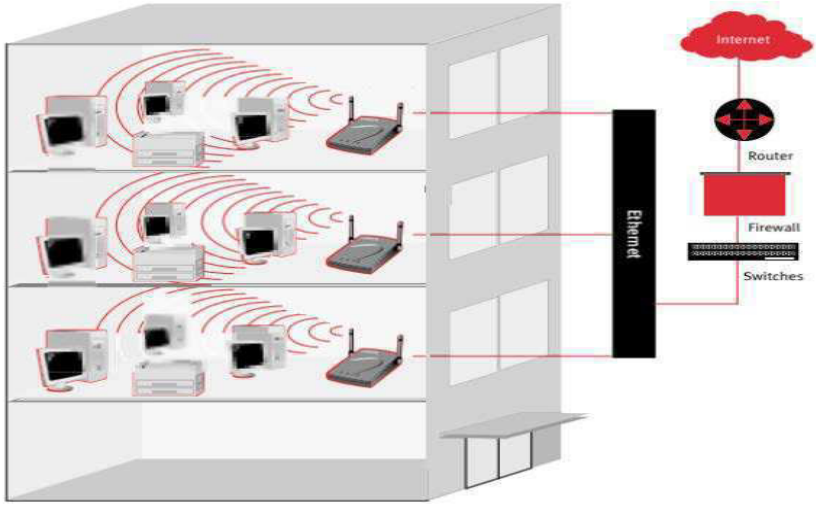
- **Οικονομικοί παράγοντες:** Στους οικονομικούς παράγοντες συγκαταλέγονται το κόστος των συσκευών, η κατανάλωση ενέργειας αλλά και το κόστος εγκατάστασης. Θεωρητικά οι συσκευές που υποστηρίζουν ασύρματη συνδεσιμότητα έχουν μεγαλύτερο κόστος αγοράς γιατί περιλαμβάνουν και ασύρματη κάρτα δικτύου. Ωστόσο στο κόστος αυτό θα πρέπει να συνυπολογιστεί και το κόστος κατανάλωσης ενέργειας της κάθε συσκευής. Όσον αφορά την

εγκατάσταση θα πρέπει να υπολογιστεί το κόστος εγκατάστασης κάθε περίπτωσης δικτύου και να απαντηθεί το ερώτημα αν πρόκειται για αρχική εγκατάσταση ή για επέκταση του υπάρχοντος δικτύου.

- **Τοποθεσία:** Άλλο ένα ερώτημα που θα πρέπει να απαντηθεί είναι η τοποθεσία στην οποία θα δημιουργηθεί ένα δίκτυο. Παίζει σημαντικό ρόλο στο κόστος κάθε φορά του δικτύου το αν είναι να αναπτυχθεί σε ένα επίπεδο ή αν θα εξυπηρετεί πολλούς ορόφους και εγκαταστάσεις που έχουν απόσταση μεταξύ τους. Όπως γίνεται εύκολα αντιληπτό στις περιπτώσεις των ενσύρματων δικτύων θα χρειαστούν πολλά καλώδια για την διασύνδεση ενώ για τα ασύρματα δίκτυα θα χρειαστούν ασύρματοι αναμεταδότες για την μετάδοση του σήματος σε μακρινές αποστάσεις.

8.3.2 Κόστος Εγκατάστασης

Η χρήση ενός ασύρματου δικτύου πρόσβασης σε ένα επιχειρηματικό περιβάλλον και κατ'επέκταση η δημιουργία ασφαλών μηχανισμών πρόσβασης σε αυτό δύναται να επιφέρουν σημαντικά οικονομικά οφέλη στην επιχείρηση. Τα οικονομικά οφέλη μεταφράζονται σε κέρδος που προκύπτει αφενός από την εγκατάσταση του δικτύου, αφετέρου από την πιθανή αύξηση της



Εικόνα 25: Παράδειγμα ασύρματου δικτύου πρόσβασης

παραγωγικότητας των εργαζομένων, όπως αναλύθηκε παραπάνω.Η κύρια διαφορά ενός ενσύρματου έναντι ενός ασύρματου δικτύου είναι η ανάγκη που υπάρχει στην πρώτη περίπτωση για τοποθέτηση δομημένης καλωδίωσης στον χώρο. Το πρόβλημα δεν έγκειται στο κόστος αγοράς των καλωδίων αλλά στο κόστος εγκατάστασης τους. Επιπλέον προκύπτει επιπλέον κόστος κάθε φορά που πρέπει να επεκταθεί το δίκτυο ή να συντηρηθεί η υπάρχουσα υποδομή.

Στον παρακάτω πίνακα φαίνεται ενδεικτικά το κόστος εγκατάστασης ενός ασύρματου δικτύου έναντι ενός ενσύρματου σε ένα μικρό εταιρικό περιβάλλον που απασχολεί 10 χρήστες (δεν συμπεριλαμβάνονται μηνιαία κόστη σύνδεσης στο internet και συντήρησης του εξοπλισμού).

Πίνακας 3: Σύγκριση κόστους εγκατάστασης WLAN και LAN

Δικτυακός Εξοπλισμός	Κόστος	Τεμάχια που απαιτούνται για LAN	Συνολικό κόστος για LAN	Τεμάχια που απαιτούνται για WLAN	Συνολικό κόστος για WLAN
Router Cisco 900 Series	500€	1	**500€**	1	**500€**
Switch Cisco 3560	1500€	1	**1500€**	1	**1500€**
AAA Server	2500€	0	**0€**	2	**5000€**
Cables cat6 SFTP 100m	40€	5	**200€**	1	**40€**
Access Points	100€	0	**0€**	2	**200€**
Desktop with wireless network card and TPM Module	400€	10	**4000€**	10	**4000€**
Installation Cost	-	-	**10000€**	-	**3000€**
Total Cost	**-**	**-**	**16200€**	**-**	**14240€**

Το κόστος εγκατάστασης φαίνεται να μην έχει μεγάλη διαφορά ανάμεσα στους δύο τύπους δικτύων, ωστόσο η επέκταση του δικτύου και η πιθανή μετακίνηση χρηστών κοστίζει πολύ περισσότερο σε ένα ενσύρματο δίκτυο.

Σε κάθε περίπτωση αυτό που γίνεται καταννοητό είναι ότι η υιοθέτηση ενός ασύρματου δικτύου πρόσβασης από μία εταιρία δεν έχει σημαντικό κόστος για αυτήν και μακροπρόθεσμα μπορεί να επιφέρει είτε άμεσα είτε έμμεσα οικονομικά οφέλη που μεταφράζονται σε χαμηλό κόστος εγκατάστασης ή και μελλοντικής επέκτασης στην πρώτη περίπτωση και σε αύξηση της παραγωγικότητας των εργαζομένων στην δεύτερη περίπτωση.

9. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία παρουσιάστηκε μία νέα προσέγγιση για την αυθεντικοποίηση χρηστών σε ασύρματα δίκτυα. Σε αυτή τη προσέγγιση συνδυάζεται το πρωτόκολλο EAP με το TPM, το οποίο μπορεί να χρησιμοποιηθεί για την δημιουργία και την αποθήκευση των πιστοποιητικών που χρειάζονται για την διαδικασία της αυθεντικοποίησης. Στις πρώτες υλοποιήσεις αυτού του πρωτοκόλλου παρουσιάστηκαν δυσκολίες ως προς τα πιστοποιητικά X.509, τα οποία θα έπρεπε να είναι τροποποιημένα με αποτέλεσμα να μην μπορούν να αναγνωριστούν κατά την διαδικασία της αυθεντικοποίησης. Τα προβλήματα αυτά επιλύθηκαν με τη χρήση λογισμικού, αποδεικνύοντας πως η χρήση του TPM είναι εύκολο να υιοθετηθεί κατά την διαδικασία αυθεντικοποίησης χρηστών με το πρωτόκολλο EAP-TLS.

Τα οφέλη που προκύπτουν από την χρήση του TPM είναι πολλά με τα κυριότερα να αφορούν την ασφάλεια των δεδομένων καθώς η αποθήκευση τους δεν γίνεται σε κάποιο εύκολα προσβάσιμο αρχείο του υπολογιστή αλλά μέσα στο TPM, με αποτέλεσμα να μην μπορεί να αποκτηθεί πρόσβαση σε αυτά.

Η ύπαρξη λοιπόν ενός τέτοιου συστήματος ελέγχου ταυτότητας θα καταστήσει τα WiFi δίκτυα τόσο δημοφιλή όσο και τα GSM. Όπως άλλωστε δείχνουν και πρόσφατες μελέτες τα ασύρματα δίκτυα πρόσβασης γίνονται ολοένα και πιο δημοφιλή και όλο και πιο πολλές επιχειρήσεις και δημόσιοι οργανισμοί τα υιοθετούν. Η χρήση ασφαλών πρωτοκόλλων αυθεντικοποίησης, όπως το EAP-TPM που προτάθηκε παραπάνω αλλά και το μικρό κόστος εγκατάστασης και επέκτασης των ασύρματων δικτύων φαίνεται να συμβάλλουν θετικά προς αυτή την κατεύθυνση. Ωστόσο τα κριτήρια επιλογής ανάμεσα σε ασύρματα και ενσύρματα δίκτυα παραμένουν εξατομικευμένα και η απόφαση στο τέλος εξαρτάται από τις προτεραιότητες που θέτει κάθε οργανισμός.

10. ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

Ως μελλοντικός ερευνητικός στόχος της παρούσας υλοποίησης προτείνεται η εφαρμογή αυτού του τρόπου αυθεντικοποίησης σε πραγματικά περιβάλλοντα και η διεξαγωγή μιας σειράς δοκιμών σε θέματα ασφάλειας και ταχύτητας του πρωτοκόλλου. Μετά από την παρέλευση δοκιμών θα διεξαχθούν συμπεράσματα ως προς την απόδοση αυτής της μεθόδου αυθεντικοποίησης, ώστε μελλοντικά να καταστεί δυνατή η προτυποποίηση του πρωτοκόλλου.

ΑΚΡΩΝΥΜΙΑ

AAA	Authentication Authorization Accounting
AR/VR	Augmented Reality/Virtual Reality
AVP	Attribute-Value Pairs
BYOD	Bring Your Own Device
CA	Certificate Authority
CHAP	Challenge Handshake Protocol
CRTM	Core Root of Trust
DSSS	Direct-Sequence Spread-Spectrum
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EK	Endorsement Key
FHSS	Frequency-Hopping Spread-Spectrum
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
LCP	Link Control Protocol
LEAP	Lightweight EAP
LLC	Link Local Control
MAC	Media Access Control
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAS	Network Authentication Server
NCP	Network Control Protocol
PAE	Port Access Entity
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent
POTP	Protected One-Time Password
PPP	Point to Point
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PWLAN	Public Wireless LAN
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest–Shamir–Adleman
RTM	Root of Trust for Reporting
SIM	Subscriber Identity Module
SSL	Secure Socket Layer
TBB	Trusted Boot Block

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSS	TCG Software Stack
TTLS	Tunneled Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
VSA	Vendor Specific Attributes
WEP	Wired Equivalent Privacy
WPA	Wireless Protected Access

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Gast M., 2017, “802.11 Wireless Networks”, 2nd ed., O'Reilly Media.

[2] Stallings W., 2017, “Cryptography and network security”, 4th ed., Boston, Mass: Pearson.

[3] Geier J., 2008, “Implementing 802.1X security solutions for wired and wireless networks”, Indianapolis, Wiley.

[4] Jyh-Cheng Chen and Yu-Ping Wang, "Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience," in IEEE Communications Magazine, vol. 43, no. 12, pp. supl.26-supl.32, Dec. 2005, doi: 10.1109/MCOM.2005.1561920.

[5] Iana.org, “Internet Assigned Numbers Authority”,[online] Available at: <http://www.iana.org/> [Accessed 17 May 2021].

[6] Kovačić, Salko & Đulić, Emina & Sehidic, Admir, “Improving the Security of Access to Network Resources Using the 802.1x Standard in Wired and Wireless Environments”, 2017.

[7] Madjid Nakhjiri & Mahsa Nakhjiri, 2009, “AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility”, Wiley.

[8] Arthur W., Challener D. and Goldman K., 2015, “A Practical Guide to TPM 2.0”, APress.

[9] Ezirim, Kenneth & Khoo, Wai & Koumantaris, George & Law, Raymond & Perera, Irippuge, 2012, “Trusted Platform Module – A Survey”.

[10] Trusted Computing Group. 2021, “Trusted Platform Module (TPM)” [online] Available at: <https://trustedcomputinggroup.org/work-groups/trusted-platform-module/> [Accessed 17 May 2021].

[11] ISO, “ISO/IEC11889-1:2015”, [online] Available at:<https://www.iso.org/standard/66510.html> [Accessed 17 May 2021].

[12] Trusted Platform Module Library Part 1: Architecture, Family “2.0”, Level 00 Revision 01.38 September 29, 2016.

[13] Johannes Winter, Kurt Dietrich, “A hijacker’s guide to communication interfaces of the trusted platform module”, Computers & Mathematics with Applications, Volume 65, Issue 5, 2013, Pages 748-761, ISSN 0898-1221.

[14] Mayes K. and Markantonakis K., 2017, “Smart Cards, Tokens, Security and Applications”, Springer.

[15] Sean W. Smith, 2005, Trusted Computing Platforms: Design and Applications, Springer.

[16] Jindal V., Verma A., & Bawa S., 2013, “Comparative Analysis of IEEE 802.11 Standards in Wireless Networking”.

[17] Holt Alan, Huang Chi-Yu, “802.11 Wireless Networks Security and Analysis”,2010, Springer.

[18] Choi M., Robles R.J., Hong C. & Kim T., 2008, “Wireless Network Security: Vulnerabilities, Threats and Countermeasures”.

[19] C. Latze, U. Ultes-Nitsche and F. Baumgartner, "Towards a zero configuration authentication scheme for 802.11 based networks", 33rd IEEE Conference on Local Computer Networks (LCN), 2008, pp. 367-373, doi: 10.1109/LCN.2008.4664192.

[20] C. Latze and U. Ultes-Nitsche, “A Proof-of-Concept Implementation of EAP-TLS with TPM support”, 7th Annual ISSA Conference,Johannesburg, South-Africa, July 2008.

[21] C. Latze, 2010, “Towards a secure and user-friendly authentication method for public wireless networks”, Logos Verlag.

[22] C. Latze, 2009, “EAP-TPM : A New Authentication Protocol for IEEE 802.11 Based Networks”.

[23] Raspberrypi.org, “Setting up a wireless LAN via the command line - Raspberry Pi Documentation”, [online] Available at: <https://www.raspberrypi.org/documentation/configuration/wireless/wireless-cli.md> [Accessed 17 May 2021].

[24] GitHub, “tpm2-software/tpm2-tss-engine”, [online] Available at: <https://github.com/tpm2 -software/tpm2-tss-engine> [Accessed 17 May 2021].

[25] Dierks T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[26] Trusted Computing Group, “IBM TrouSerS | Trusted Computing Group”, [online] Available at: <https://trustedcomputinggroup.org/resource/ibm-trousers/> [Accessed 17 May 2021].

[27] Y. Chen, A. Studer and A. Perrig, "Combining TLS and TPMs to Achieve Device and User Authentication for Wi-Fi and WiMAX Citywide Networks," 2008 IEEE Wireless Communications and Networking Conference, 2008, pp. 2804-2809, doi: 10.1109/WCNC.2008.491.

[28] Walt D., 2013, “FreeRADIUS - Manage your network resources with FreeRADIUS - Freeradius beginner's guide”, Shroff Publishers & Distr.

[29] Wiki.freeradius.org, “Getting Started” [online] Available at: <https://wiki.freeradius.org/guide/Getting%20Started> [Accessed 17 May 2021].

[30] “FreeRADIUS Technical Guide”, 2014, Network RADIUS SARL, [online] Available at: https://networkradius.com/doc/FreeRADIUS-Technical-Guide.pdf [Accessed 17 May 2021].

[31] Aziz N., Udzir N.I., & Mahmod R., 2014, “Extending TLS with Mutual Attestation for Platform Integrity Assurance”, J. Commun., vol. 9, 63-72.

[32] Trusted Computing Group, 2015, “TPM Keys for Platform Identity for TPM 1.2”, Specification Version 1.0, Revision 3.

[33] OpenSSL, “The Open Source toolkit for SSL/TLS.” [Online], Available at: <http://www.openssl.org> [Accessed 17 May 2021].

[34] Kun Li, Michael Maass, and Mike Ralph, 2012, “A Type-safe, TPM Backed TLS Infrastructure”, [Online], Available at: <https://www.cs.cmu.edu/~mmaass/tpm_tls/report.html> [Accessed 17 May 2021].

[35] Infineon, “Integration of TLS Functionality for OPTIGA™ TPM SLx 9670 TPM 2.0”, 2020, [Online], Available at: <https://www.infineon.com> [Accessed 17 May 2021].

[36] L. Zhou and Z. Zhang, "Trusted Channels with Password-Based Authentication and TPM-Based Attestation," 2010 International Conference on Communications and Mobile Computing, 2010, pp. 223-227, doi: 10.1109/CMC.2010.232.

[37] Kakei, Shohei & MOHRI, Masami & Shiraishi, Yoshiaki & Morii, Masakatu,2016, “SSL Client Authentication with TPM”, IEICE Transactions on Information and Systems, E99, D. 1052-1061. 10.1587/transinf.2015CYP0012.

[38] Kurose J. and Ross K., 2013, “Computer Networking - A Top Down Approach”, 6th edition, Pearson.

[39] Laura Chappell, 2012, “Wireshark Network Analysis - The Official Wireshark Certified Network Analyst Study Guide”, 2nd Edition, Chappell University.

[40] Mikrotik Help, “First Time Configuration”, [online] Available at: <https://help.mikrotik.com> [Accessed 22 May 2021].

[41] Mikrotik Documentation, 2020, “Manual:RADIUS Client”, [online] Available at: <https://help.mikrotik.com/> [Accessed 22 May 2021].

[42] Mikrotik Documentation, 2020, “Manual:Wireless EAP-TLS using RouterOS with FreeRADIUS”, [online] Available at: <https://help.mikrotik.com/> [Accessed 22 May 2021].

[43] Mikrotik Documentation, 2020, “Manual:Create Certificates”, [online] Available at: <https://help.mikrotik.com/> [Accessed 22 May 2021].

[44] UniFy Help and Support Center, “Getting started with UniFi”, [online] Available at: <https://help.ui.com> [Accessed 22 May 2021].

[45] GitHub, “tmpk - TPM2 key and storage management toolkit”, [online] Available at: <https://github.com/folbricht/tpmk/blob/master/README.md> [Accessed 22 May 2021].

[46] TechExpert Tips, “FreeRadius Installation with MySQL Integration on Ubuntu Linux”, [online]Available at:<https://techexpert.tips/freeradius/freeradius-installation-mysql-integration-ubuntu> [Accessed 22 May 2021].

[47] VPNServer, “Setup and Configuration of FreeRADIUS + MySQL on Ubuntu 14.04 64Bit”, [online] Available at:<https://www.vpsserver.com/community/tutorials/10/setup-and-configuration -of-freeradius-mysql-on-ubuntu-14-04-64bit/> [Accessed 22 May 2021].

[48] Digital Ocean, Etel Sverdlov, 2012 “How To Set Up Master Slave Replication in MySQL”, [online] Available at:<https://www.digitalocean.com/community/tutorials/how-to-set-up-master-slave-replication-in-mysql> [Accessed 22 May 2021].

[49] “The raddb/ directory”, [online] Available at: https://networkradius.com/doc/3.0.10/raddb/home.html [Accessed 17 May 2021].

[50] “Mobility, performance and engagement. How CIOs can contribute to business performance by shaping the employee experience”, 2016, A report by The Economist Intelligence Unit.

[51] GitHub, “tpm2-software/tpm2-tss”, [online] Available at: <https://github.com/tpm2-software/tpm2-tss> [Accessed 23 Sep 2021].

[52] GitHub, “tpm2-software/tpm2-pkcs11”, [online] Available at: <https://github.com/tpm2-software/tpm2-pkcs11/blob/master/docs/EAP-TLS.md> [Accessed 23 Sep 2021].

[53] WiFi Alliance, “Global Economic Value of Wi-Fi 2021 – 2025”, September 2021 [online] Available at: <https://www.wi-fi.org/discover-wi-fi/value-of-wi-fi> [Accessed 30 Sep 2021].

[54] Katz, R; Jung, J. and Callorda, F. (2020e). The economic value of Wi-Fi: a global view (2021-2025). New York: Telecom Advisory Services.

[55] Michael J. Bequette, Matthew K. Giunta, White Papper, “Wired or Wireless? A Practical Approach to Making the Right Selection.”