ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΠΟΤΙΜΗΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ VoIP, VoLTE, VoWiFi και STIR/SHAKEN

Δημήτρης Γεωργιλάκης

Επιβλέπων Καθηγητής:
Ξενάκης Χρήστος

ΠΕΙΡΑΙΑΣ

05 2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Security Assessment on VoIP, VoLTE, VoWiFi and STIR/SHAKEN protocols

Δημήτρης Γεωργιλάκης
Α.Μ.: MTE - 1906

ΠΕΡΙΛΗΨΗ

Καθώς οι άνθρωποι εξελίσσονται και μαζί με αυτούς γεννούνται νέες ανάγκες, η τεχνολογία δεν έχει να κάνει άλλο παρά να εξελιχθεί μαζί με αυτούς. Πλέον, σχεδόν καταργήσαμε τα παλιά δίκτυα επικοινωνίας (circuit switched) με απώτερο σκοπό την μετάβαση σε μια τεχνολογία που θα είναι αρκετά πιο γρήγορη στις υπηρεσίες της, εύκολα διαχειρίσιμη, και συνεχώς διαθέσιμη ανεξαρτήτου τοποθεσίας. Έτσι η μετάβαση έγινε στα δίκτυα packet switched τα οποία βασίζονται στο πρωτόκολλο IP, την τεχνολογία του Ίντερνετ. Συνεπώς, δίκτυα όπως τα 2G και 3G έχουν αρχίσει και μειώνονται σε πολλές χώρες, ενώ δίκτυα όπως το 4G και 5G έχουν εδραιωθεί ως βασικές τεχνολογίες φωνής και data. Η παροχή υπηρεσίας φωνής στις τεχνολογίες 4G και 5G βασίζεται στην εδραιωμένη πλέον τεχνολογία VoIP, βάση της οποίας γεννήθηκαν οι τεχνολογίες VoWiFi και VoLTE.

Στην παρούσα διπλωματική θα κάνουμε μια ιστορική αναδρομή στις υπηρεσίες circuit switched και packet switched καθώς και στα πρωτόκολλα τους. Εν συνεχεία θα αναλυθεί η αρχιτεκτονική δομή αλλά και τα πρωτόκολλα των τεχνολογιών VoIP, VoLTE και VoWiFi καθώς και οι ευπάθειες τους. Προχωρώντας στα επόμενα μέρη θα πραγματοποιήσουμε διάφορες επιθέσεις και θα παρατηρήσουμε τις επιδράσεις αυτών. Τελειώνοντας την διπλωματική, θα προταθούν κάποιες λύσεις που θα μειώνουν αλλά και θα αντιμετωπίζουν ολοκληρωτικά τις αδυναμίες αυτές.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: VoIP, VoLTE, VoWiFi, scapy, DOS, Vulnerabilities

ABSTRACT

As people's needs evolving, so as technology needs to be evolved. Circuit-switched based networks have become obsolete in order to design new technologies that will be faster, always available and easy to use. Such kind of technology is Packet switched network that is based on IP protocol, the protocol of Internet. Thus, networks like 2G or 3G have become obsolete in many countries, whereas 4G or 5G are the main networks for data and voice. VoLTE and VoWiFi are the main voice services of these two technologies which are based on VoIP technology.

The purpose of this thesis is to analyze the vulnerabilities of these 3 voice technologies, VoIP, VoLTE and VoWiFi. We will present a historic background of the circuit and packet switched networks along with their protocols. Moreover, we will proceed to the analysis of their architectural structure and their used protocols, but also proceed to a vulnerability assessment. On the next parts, we will launch some attacks and observe their impact. Finally, we will propose some mitigations that will help to avoid or reduce the impact of such attacks.

KEYWORDS: VoIP, VoLTE, VoWiFi, scapy, DOS, Vulnerabilities

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω την οικογένεια μου, την γυναίκα μου καθώς και τον καθηγητή μου μαζί με την επιβλέπουσα βοηθό του, αλλά και όλους τους φίλους, συναδέλφους και συμφοιτητές για την πραγματοποίηση και ευχάριστη ολοκλήρωση αυτού του μεταπτυχιακού.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. Εισαγωγή

Η υπηρεσία φωνής είναι ένα πολύτιμο και απαραίτητο πλέον «αγαθό», της καθημερινότητας μας και αυτό φάνηκε από τα τέλη του 19^{ου} αιώνα. Καθώς εξελίσσονται οι ανάγκες των ανθρώπων έτσι εξελίσσεται και η τεχνολογία. Μετά την εμφάνιση της ενσύρματης τηλεφωνίας από πόλη σε πόλη, προχωρήσαμε από χώρα σε χώρα και έπειτα από ήπειρο σε ήπειρο, καταργώντας έτσι τα σύνορα ως εμπόδιο στην επικοινωνία των ανθρώπων.

Οι ανάγκες όμως μεγάλωσαν και έτσι προέκυψε η ανάγκη για την ασύρματη και κινητή επικοινωνία. Συνεπώς, τα δίκτυα στα οποία βασιζόταν η ενσύρματη υπηρεσία φωνής, packet-switched, άνοιξαν τον δρόμο στην υλοποίηση της υπηρεσίας φωνής μέσω των κεραιών κινητής τηλεφωνίας. Αφού ολοκληρώθηκε αυτή η «συνεργασία» τα δίκτυα 1G, 2G και 3G γεννήθηκαν. Καθώς όμως αυξάνονταν οι απαιτήσεις των χρηστών για μεγαλύτερες ταχύτητες, καθώς τα δίκτυα 2G και 3G μπορούσαν και παρείχαν υπηρεσίες data, η ανάγκη για μια ολοκληρωτική αλλαγή έκανε την εμφάνιση της. Εμφανίστηκε όταν οι περισσότεροι πάροχοι τηλεφωνίας μεταβίβασαν την ενσύρματη υπηρεσία φωνής στα δίκτυα packet-switched δηλαδή στα δίκτυα που γίνεται η χρήση του πρωτοκόλλου IP. Έτσι οι τεχνολογίες VoIP, VoLTE και VoWiFi γεννήθηκαν. Η πρώτη τεχνολογία που εμφανίστηκε ήταν η VoIP, η οποία χρησιμοποιεί το IP πρωτόκολλο, εντάσσοντας έτσι πολλές ευκολίες αλλά και λειτουργίες στην χρήση της. Τα δίκτυα 4G και 5G εγκαταστάθηκαν στα packet switched δίκτυα, βασίζοντας τις υπηρεσίες φωνής τους (VoLTE και VoWiFi) πάνω στην τεχνολογία VoIP.

Οι τεχνολογίες VoLTE και VoWiFi παρέχουν την υπηρεσία φωνής με μεγαλύτερη πλέον διαθεσιμότητα αλλά και ευκολία στην χρήση, καθώς και την δυνατότητα να συνεργάζονται με άλλες τεχνολογίες.

2. Ιστορική Αναδρομή

Στα τέλη της δεκαετίας του ‘70 στο Τόκιο της Ιαπωνίας, το πρώτο επίσημο δίκτυο κινητής τηλεφωνίας (1G), μπήκε σε λειτουργία από την Nippon Telegraph and Telephone (NTT), καταφέρνοντας μέσα σε λίγα χρόνια να εξαπλωθεί, δίνοντας υπηρεσία ασύρματης κινητής επικοινωνίας σε όλη την χώρα. Αυτό σήμανε και την απαρχή της ασύρματης κινητής επικοινωνίας.

Έτσι, μετά την τεράστια απήχηση του 1G μέχρι και τις αρχές του ’90, τα δίκτυα κινητής τηλεφωνίας χρειάζονταν να εξελιχθούν ώστε να μπορούν να καλύπτουν τις ανάγκες του τότε, απαιτητικού κοινού. Το 1991, το εξελιγμένο 2G έκανε την εμφάνιση του, χρησιμοποιώντας νέες τεχνολογίες με επίκεντρο, την εναλλαγή του δικτύου από αναλογικό σε ψηφιακό, κάνοντας το χρήσιμο μέχρι και τα μέσα του 2010 στο ευρύ κοινό. Ακολούθησαν οι επόμενης γενιάς τεχνολογίες, όπως το 3G, το 4G και πλέον το 5G.

Με την δημιουργία του 2G ως επόμενης γενιάς δίκτυο κινητής επικοινωνίας, έπρεπε να αναπτυχθεί και ένα πρότυπο δικτύου, το οποίο να μπορεί να χρησιμοποιείται από τις διάφορες συσκευές επικοινωνίας. Έτσι, η ETSI ανέπτυξε το GSM πρωτόκολλο κινητής, το οποίο ξεκίνησε να λειτουργεί το 1991, φτάνοντας τους 1.5 δισεκατομμύρια χρήστες παγκοσμίως, μέχρι και το 2005. Με το πέρας του καιρού, το GSM δίκτυο κινητής γινόταν ευρέως γνωστό σε όλο και περισσότερους συνδρομητές, με αποτέλεσμα να αναπτυχθούν νέες υπηρεσίες για να καλύψουν νέες ανάγκες. Το 1995 εμφανίστηκαν τα πρώτα SMS, το Fax, η αναμονή και η προώθηση κλήσης, καθώς και η χαμηλής ταχύτητας, μεταφορά δεδομένων.

Το GPRS πρωτόκολλο ήρθε να αντικαταστήσει το GSM δίκτυο, στο πλέον εξελιγμένο, 2.5G, δίκτυο κινητής επικοινωνίας, κάνοντας ένα μεγάλο άλμα, αφού χρησιμοποιεί δίκτυο packet-switched εν αντιθέσει με το circuit-switch δίκτυο του GSM, κάνοντας το ικανό να μπορεί να υποστηρίξει μεγαλύτερες ταχύτητες στο Internet και με μικρότερες χρεώσεις. Υποστηρίζει υπηρεσίες όπως MMS[1] και WAP[2].

Τα επόμενης γενιάς δίκτυα κινητής επικοινωνίας (3G, 4G, 5G), αναπτύχθηκαν πιο γρήγορα από τους προκατόχους τους, καθώς η ανάγκη για μεγαλύτερο όγκο δεδομένων σε μεγαλύτερες ταχύτητες και σε λιγότερο χρόνο, ήταν μεγάλη.

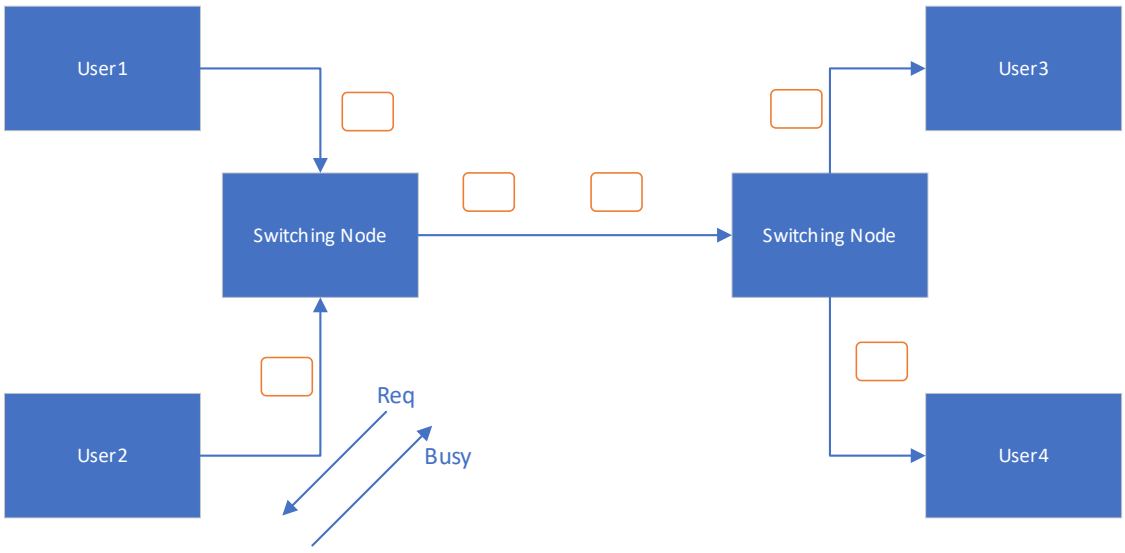
Το 3G έκανε την πρώτη του εμφάνιση ως εμπορικό προϊόν το 2002 φτάνοντας ταχύτητες, έως και σήμερα, ~22Mbit/s σύμφωνα με την τεχνολογική υποδομή και το πρωτόκολλο που χρησιμοποιεί ο εκάστοτε πάροχος (HSPA, HSPA+)[4].

Το 2009 το 4G (LTE) έκανε το επίσημο ντεμπούτο του στην Νότια Κορέα και μέχρι και σήμερα είναι το κύριο πρωτόκολλο κινητής επικοινωνίας στις περισσότερες συσκευές του κόσμου, φτάνοντας ταχύτητες έως και τα 300Mbit/s. Υποστηρίζει τεχνολογίες όπως VoLTE.

Το 5G είναι και το τελευταίας γενιάς, πρωτόκολλο κινητής επικοινωνίας, το οποίο μπορεί να φτάσει και ταχύτητες έως και 10Gbit/s. Έχει πολύ μικρότερη κάλυψη σε σχέση με το 4G αλλά μπορεί να φτάσει πολύ μεγαλύτερες ταχύτητες.

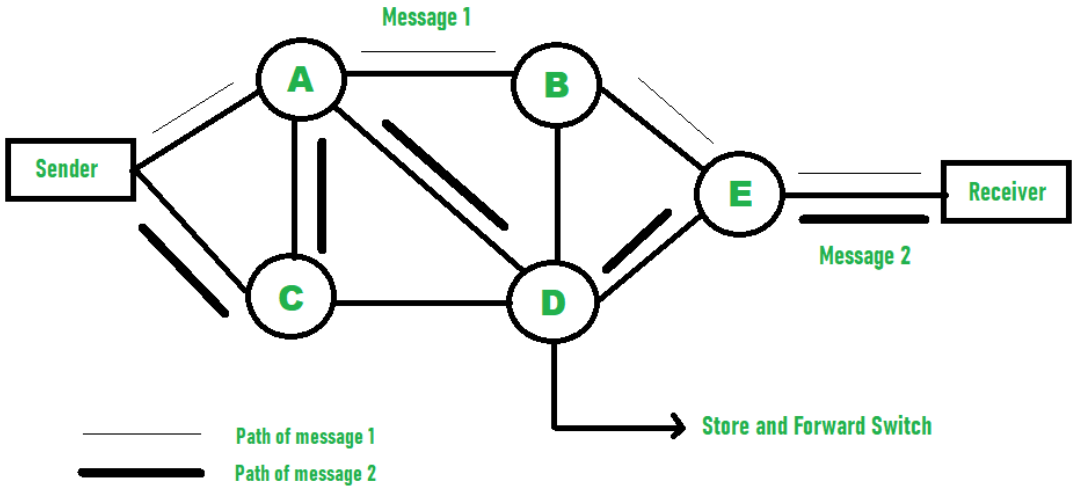
Η ραγδαία ανάπτυξη της τεχνολογίας, οι απαιτήσεις, οι ανάγκες των καταναλωτών για εύκολη και άμεση πρόσβαση σε διάφορες υπηρεσίες, καθώς και τα οικονομικά συμφέροντα των εταιριών, έχουν δημιουργήσει την ανάγκη μιας οντότητας στην οποία όλα θα μπορούν να είναι διαθέσιμα, αρκεί να υπάρχει σύνδεση στο διαδίκτυο. Για να γίνει αυτό όμως, πρέπει υπηρεσίες όπως η κλασσική τηλεφωνία PSTN-ISDN, η επίγεια τηλεόραση, και πολλές άλλες, να μπορέσουν να μετατραπούν στην ψηφιακή τους μορφή, ώστε να είναι διαθέσιμες μέσω του διαδικτύου. Η ανάγκη αυτή, έχει οδηγήσει τις εταιρίες να αφήνουν πίσω τους τεχνολογίες όπως PSTN, ISDN, FAX, SDH[4], μισθωμένα κυκλώματα κ.α. και να μεταφέρουν αυτές τις υπηρεσίες, αλλάζοντας προφανώς την τεχνολογία τους κάτω από την ομπρέλα του IP δικτύου (packet-switching). Τεχνολογίες που βασίζονται σε παλιάς τεχνολογίας κυκλώματα, όπως τα αναλογικά (Circuit switching) έχουν φτάσει στο τέλος τους. Έτσι οι εταιρίες τηλεπικοινωνίων, κατανοώντας πλέον τις ανάγκες των καταναλωτών για την άμεση και εύκολη πρόσβαση στις υπηρεσίες τους, αναβάθμισαν την τεχνολογία και την υποδομή τους και διέθεσαν τις υπηρεσίες τους μέσω του διαδικτύου.

Τα αναλογικά κυκλώματα ήταν η πρώτη τεχνολογία που χρησιμοποιήθηκε στις τηλεπικοινωνίες, για την μεταφορά του αναλογικού σήματος. Η τεχνολογία που χρησιμοποιούσαν για να μεταφέρουν την φωνή μέσα από το μέσο, ήταν η πολυπλεξία του σήματος, καθώς διαιρούσε τη χωρητικότητα του τηλεπικοινωνιακού καναλιού σε λογικά κανάλια και συνήθως οι τύποι που λάμβαναν χώρα ήταν 1) Frequency Division Multiplexing (FDM), 2) Time Division Multiplexing (TDM) ή 3) Code Division Multiplexing (CDM)[5]. Το πρόβλημα στην συγκεκριμένη τεχνολογία ήταν ότι η διανομή της χωρητικότητας του καναλιού (bandwidth) ήταν μη αποτελεσματική καθώς αν το κανάλι που χρησιμοποιείται βρίσκεται σε κατάσταση ηρεμίας (με λίγα δεδομένα) η χωρητικότητα του καναλιού είναι σταθερή βάση της μέγιστης τιμής που έχει συμφωνηθεί. Έτσι αν δεν υπάρχουν διαθέσιμα κανάλια για να σταλεί η νέα σηματοδοσία αιτήματος κλήσης, η κλήση αυτή είτε μπορεί να έχει μεγάλη καθυστέρηση είτε και να μην καταφέρει να πραγματοποιηθεί. Υπηρεσίες κινητής 1G, 2G, 3G, σταθερής PSTN, ISDN, καθώς και υπηρεσίες ίντερνετ όπως SDH, SONET βασίζονται σε αυτή την τεχνολογία.



Εικόνα 1: Δομή Circuit-switched

Η νεότερη τεχνολογία, packet-switching, είναι και η βάση του IP πρωτοκόλλου. Τα δεδομένα σπάνε σε μικρά πακέτα και μεταφέρονται στον κοντινότερο εξυπηρετητή (router) και αυτό με την σειρά του στον επόμενο, μέχρι να φτάσουν στον τελικό προορισμό τους. Στην συγκεκριμένη τεχνολογία, το μέσο μετάδοσης μπορεί να μοιράζεται το συνολικό του bandwidth ανάμεσα σε διάφορα τερματικά, καθώς αρκετοί συνδρομητές την ίδια στιγμή μπορεί να μην κάνουν χρήση του διαδικτύου, κάνοντας έτσι πιο αποτελεσματική, γρήγορη και σίγουρη την μετάδοση των δεδομένων. Η τεχνολογία αυτή μας φέρνει μεγαλύτερες ταχύτητες και περισσότερη ευκολία στην πρόσβαση των υπηρεσιών. Υπηρεσίες όπως 4G, VoIP, VoLTE, VoWiFi κάνουν χρήση αυτής της τεχνολογίας.



Εικόνα 2: Δομή packet-switching δικτύου

Καθώς το μεγαλύτερο ποσοστό των τηλεπικοινωνιακών εταιριών έχουν μεταβεί στον ψηφιακό κόσμο των υπηρεσιών φωνής, η δυνατότητα χρήσης της υπηρεσίας σε συνδυασμό με τα χαμηλά κόστη, την άμεση διαθεσιμότητα και την ευκολία χρήσης, έχει αυξηθεί δραματικά. Έτσι νέα πρωτόκολλα και υπηρεσίες δημιουργήθηκαν, ώστε να εξυπηρετήσουν τις προαναφερθείσες ανάγκες.

Το πρωτόκολλο VoIP (Voice over IP), αποτελεί μια ομάδα διάφορων πρωτοκόλλων-τεχνολογιών προσφέροντας υπηρεσία φωνής σε πραγματικό χρόνο μαζί με άλλες multimedia και μη υπηρεσίες, σε αρκετά χαμηλό κόστος έως και μηδενικό.

Το VoIP γίνεται μια ελκυστική επιλογή επικοινωνίας για τους καταναλωτές καθώς δίνει την δυνατότητα στον χρήστη να χρησιμοποιήσει την οικιακή του ή εταιρική του τηλεφωνική σύνδεση σε διάφορες συσκευές, οποιαδήποτε στιγμή θέλει, πραγματοποιώντας κλήσεις με μηδενικό ή ελάχιστο κόστος. Δεδομένου των χαμηλών συνδρομητικών τελών στις συνδέσεις Ίντερνετ από τους παρόχους, η χρήση του VoIP έχει αποκτήσει μεγάλη δημοτικότητα τόσο στους εταιρικούς όσο και στους οικιακούς χρήστες. Παρόλα αυτά, όσο η χρήση του VoIP πρωτοκόλλου αυξάνεται, τόσο αυξάνεται και ο κίνδυνος για πιθανές απειλές. Ενώ οι ευπάθειες του VoIP είναι συνήθως παρόμοιες με αυτές που οι χρήστες αντιμετωπίζουν στο διαδίκτυο, νέες απειλές, απάτες και επιθέσεις γεννιούνται για την IP τηλεφωνία.

Όπως προαναφέραμε, μετά την μετάβαση των υπηρεσιών φωνής των τηλεπικοινωνιακών παρόχων σε δίκτυα IP (packet switching), η ανάγκη για καλύτερη ποιότητα φωνής, με χαμηλότερο κόστος και για τις δύο πλευρές (πελάτης – πάροχος) εμφανίστηκε και στις υπηρεσίες κινητής τηλεφωνίας. Με την άφιξη του LTE 4G, (η πρώτη γενιά κινητής που βασίζεται σε packet switching τεχνολογία), υπηρεσίες όπως η VoLTE και VoWiFi εμφανίστηκαν, ώστε να αναβαθμίσουν την ποιότητα και ευκολία της υπηρεσίας φωνής.

Το VoLTE είναι μια τεχνολογία που μεταφέρει πακέτα φωνής πάνω από το IP πρωτόκολλο μέσω του packet switched δικτύου, κάνοντας έτσι την ποιότητα της κλήσης πολύ καλύτερη σε σχέση με τις παλιές υπηρεσίες φωνής. Για την διευκόλυνση της επικοινωνίας, κάθε φωνητική κλήση μέσω VoLTE διατηρεί ένα session σηματοδοσίας, όπως ακριβώς κάνει και το VoIP πρωτόκολλο. Η δυνατότητα στον χρήστη να μπορεί να ανοίξει μια σύνδεση στο Ίντερνετ μέσω της υπηρεσίας LTE (mobile data), την ώρα που βρίσκεται σε κλήση από το ίδιο τερματικό, προσφέρει ένα μεγάλο πλεονέκτημα.

Το VoWiFi, χρησιμοποιεί την τεχνολογία του Wi-Fi (802.11) ώστε να μεταφέρει πακέτα φωνής VoIP, στον IMS[6] server του παρόχου. Το πρωτόκολλο αυτό δίνει την δυνατότητα στον χρήστη να μπορεί να πραγματοποιεί κλήσεις μέσω του τερματικού κινητής τηλεφωνίας (π.χ κινητό), χρησιμοποιώντας το δίκτυο Wi-Fi, όπου αυτό είναι διαθέσιμο, «ακολουθώντας» έτσι στο χρήστη, ακόμα και όταν η επικοινωνία του τερματικού με την κεραία της κινητής, είναι αδύνατη.

3. Τεχνολογία VoIP

Όπως προαναφέραμε, η τεχνολογία την σταθερής τηλεπικοινωνίας ξεκίνησε και υλοποιήθηκε πάνω από τα δίκτυα μεταγωγής (circuit switch), τα πολύ γνωστά σε όλους μας PSTN/ISDN. Με τα δίκτυα μεταγωγής, ο χρήστης μπορούσε να πραγματοποιήσει κλήσεις όπου ήθελε ανά τον κόσμο, με τις ανάλογες χρεώσεις βάση τιμοκαταλόγου. Μάλιστα, προτού οι πάροχοι μεταβούν στην νεότερη τεχνολογία των δικτύων μεταγωγής, δηλαδή τα ψηφιακά κέντρα, τα αναλογικά κέντρα είχαν μεγάλο κόστος προς τον πελάτη καθώς χρέωναν τον συνδρομητή σύμφωνα με τον χρόνο που κρατούσε το κύκλωμα ενεργό, ακόμα δηλαδή και αν η κλήση δεν ολοκληρωνόταν.

Voice over IP (VoIP) ονομάζεται η τεχνολογία που προσφέρει την δυνατότητα φωνητικής επικοινωνίας μεταξύ πολλαπλών τερματικών, καθώς χρησιμοποιεί το δίκτυο IP, εν αντιθέσει με τα παλιά τηλεφωνικά δίκτυα PSTN/ISDN τα οποία χρέωναν τον χρήστη βάση του χρόνου της ομιλίας και των κωδικών περιοχών και χωρών.
Το 1974 πραγματοποιήθηκε η πρώτη δοκιμή δικτυακής υπηρεσίας φωνής μέσω την τεχνολογίας NVP (Network Voice Protocol), που έτρεξε πάνω σε δίκτυο ARPANET και στέφθηκε με επιτυχία δίνοντας ελπίδες για την εξέλιξη της ιδέας αυτής. Το 1995 το Internet Phone (iphone) πραγματοποιεί μια κλήση σε πραγματικό χρόνο μέσα από το Internet, ενώ μέχρι και το 2000 έχουν αναπτυχθεί τα περισσότερα πρωτόκολλα στα τα οποία βασίζεται το VoIP (SIP, RTP)
Η τεχνολογία VoIP για να είναι λειτουργική και υλοποιήσιμη, χρειάζεται τερματικά ικανά να υποστηρίζουν το πρωτόκολλο IP, όπως συσκευές τηλεφώνου VoIP ή λογισμικά (softphones) που τρέχουν σε διάφορες συσκευές με εγκατεστημένο λειτουργικό σύστημα. Οι κλήσεις μπορούν να πραγματοποιηθούν πάνω από ένα τοπικό δίκτυο (LAN) ή πάνω από το Internet.

3.1. SIP

Το SIP πρωτόκολλο (Session Initiation Protocol) είναι υπεύθυνο για την αρχικοποίηση και της διαχείρισής μιας VoIP τηλεφωνικής συνεδρίας.

Το κλασσικό τηλεφωνικό μοντέλο POTS[7], το οποίο είναι ενεργό ακόμα σε αρκετές χώρες στον κόσμο, βασίζεται στην υποδομή των ψηφιακών τηλεφωνικών κέντρων των παρόχων τηλεφωνίας, τα οποία περνούν την φωνή μετατρέποντας την πρώτα σε συνεχές ρεύμα, μέσα από ζεύγη καλωδίων χαλκού. Προφανώς αυτό δεν μπορεί να προσφέρει διαθεσιμότητα, ευκολία, αλλά και ευελιξία στον χρήστη καθώς η υπηρεσία θα καταλήγει πάντα σε μια σταθερή και στατική υποδομή. Ο χρήστης αδυνατεί να τροποποιήσει την υπηρεσία σύμφωνα με τις ανάγκες του, παρά μόνο κατόπιν αιτήσεως του στον πάροχο και αυτό σε συγκεκριμένες περιπτώσεις. Τέλος, προβλήματα ποιότητας και αξιοπιστίας λόγω των φυσικών περιορισμών του χαλκού καθιστούν την κλασσική τηλεφωνία δύσχρηστη.

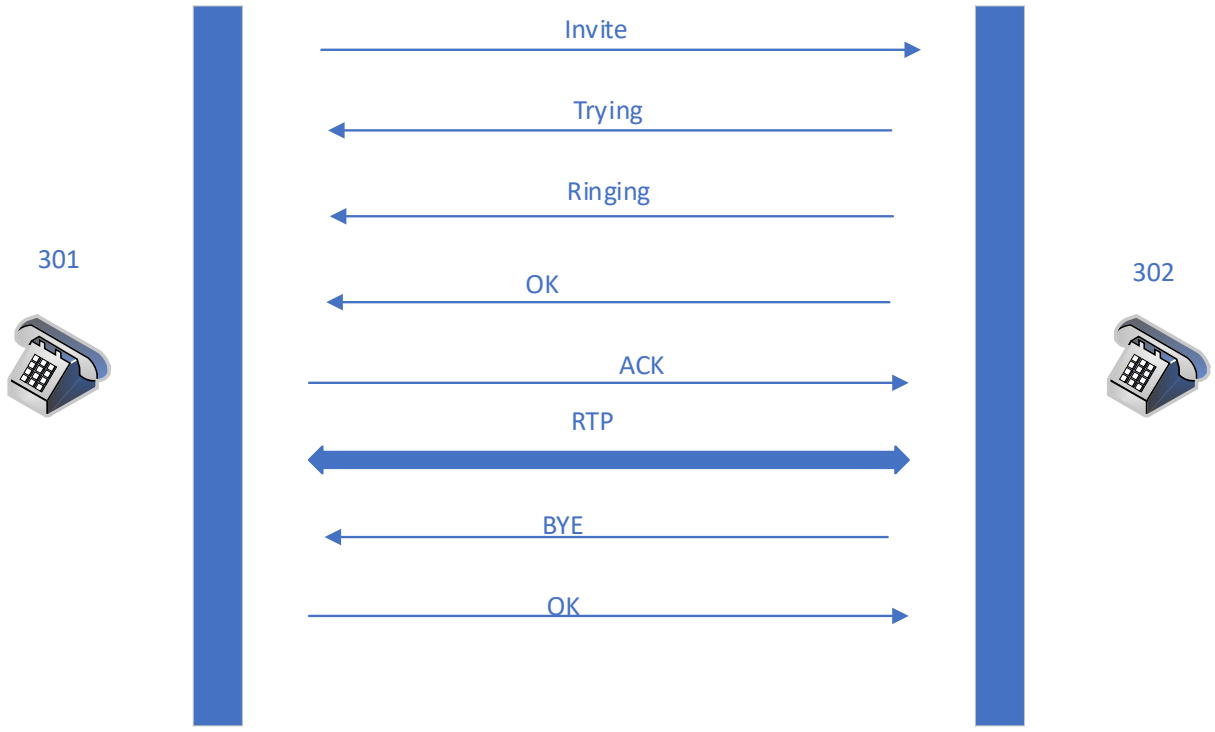
Το πρωτόκολλο SIP λειτουργεί στο application-layer του OSI model[8] και μπορεί να εγκαθιδρύσει, τροποποιήσει, διαχειριστεί και να τερματίσει τηλεφωνικές συνεδρίες με διάφορα χαρακτηριστικά, όπως απλές τηλεφωνικές κλήσεις, τηλεφωνικές κλήσεις με παραπάνω από δύο συνομιλητές, αυτοματοποιημένες διαδικασίες σε VoIP τηλεφωνικά κέντρα και video meetings. Ο χρήστης πλέον, μπορεί να διαχειριστεί τον τηλεφωνικό του αριθμό οπουδήποτε και αν βρίσκεται, εν αντιθέσει με την τεχνολογία PSTN/ISDN, αρκεί το τερματικό του (VoIP συσκευή, laptop, mobile, software) να είναι ικανό να υποστηρίξει το SIP πρωτόκολλο.

Το SIP αποτελείται από 5 πυλώνες:

- **Τον εξοπλισμό του χρήστη**: Τι εξοπλισμό χρησιμοποιεί ο χρήστης για την επικοινωνία
- **Την διαθεσιμότητα του χρήστη**: Αν ο χρήστης έχει τον κατάλληλο εξοπλισμό και την δυνατότητα για επικοινωνία
- **Τους πόρους του χρήστη:** Τι πόρους και ποιες παραμέτρους θα χρησιμοποιήσει ο χρήστης και το τερματικό του
- **Την εγκαθίδρυση της επικοινωνίας:** Την εκκίνηση της επικοινωνίας κατόπιν κοινής συμφωνίας για τις παραμέτρους που θα χρησιμοποιηθούν από τα τερματικά
- **Την διαχείριση της επικοινωνίας:** Την κατάλληλη παραμετροποίηση και έλεγχο των πρωτοκόλλων και των εξυπηρετητών για την σωστή επικοινωνία.

Μπορούμε να συμπεράνουμε λοιπόν, πως το SIP δεν είναι ένα ανεξάρτητο πρωτόκολλο επικοινωνίας ώστε να πραγματοποιήσει μια κλήση. Είναι ένα κομμάτι από ένα σύνολο πρωτοκόλλων που αλληλεξαρτώνται για να ολοκληρώσουν την δομή της VoIP τεχνολογίας. Τέτοια πρωτόκολλα είναι το RTP (Real-Time Protocol) το οποίο είναι υπεύθυνο για την μεταφορά των δεδομένων σε πραγματικό χρόνο, το RSTP (Real-Time streaming protocol) το οποίο διαχειρίζεται τον τρόπο παράδοσης των δεδομένων, το (Session Description Protocol) το οποίο διαχειρίζεται τις παραμέτρους που ανταλλάσσονται μεταξύ των τερματικών ώστε να προβούν σε μια κοινή συμφωνία και να ξεκινήσει η συνεδρία. Συνεπώς το SIP, για να προσφέρει στον τελικό χρήστη μια ολοκληρωμένη επικοινωνία, βασίζεται και σε άλλα πρωτόκολλα. Επιπλέον το SIP μπορεί να μεταφερθεί μέσω του πρωτοκόλλου TCP ή UDP ανάλογα με τις ανάγκες του κάθε χρήστη.

Η SIP trunk, μια εικονική αναλογική τηλεφωνική γραμμή που χρησιμοποιεί το SIP πρωτόκολλο, καταχωρείται στις ρυθμίσεις του SIP τερματικού και μέσω της διασύνδεσής στο διαδίκτυο, δίνει υπηρεσίες τηλεφωνίας, οπουδήποτε και αν βρίσκεται ο χρήστης, κάνοντας έτσι την VoIP τεχνολογία ιδανική.

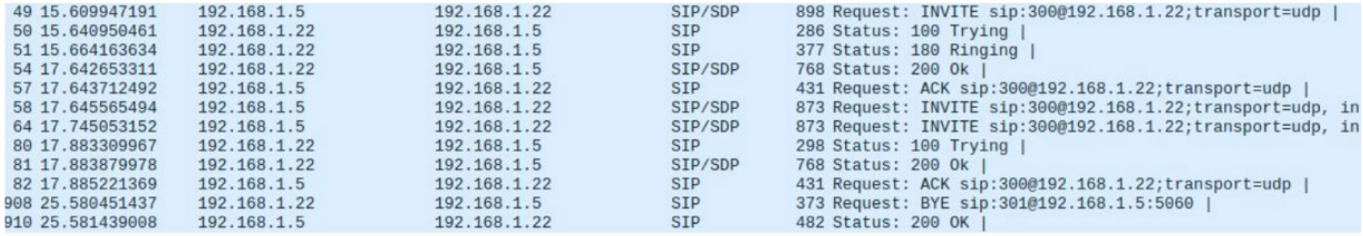


Εικόνα 3: Παράδειγμα VoIP επικοινωνίας δύο τερματικών

3.1.1. Οντότητες SIP

Το SIP αποτελείται από 4 οντότητες όπου ο η καθεμία συμμετέχει στην επικοινωνία μεταξύ των τερματικών είτε σαν client (η οντότητα που ξεκινάει την κλήση) είτε σαν server (η οντότητα που απαντάει στα αιτήματα). Κάθε τερματικό μπορεί να έχει σαν αρμοδιότητα παραπάνω από μια οντότητα.

- **User Agent (UA):** Εκκινεί και τερματίζει την συνεδρία ανταλλάζοντας SIP requests και responses. UA είναι οι συσκευές όπως IP τηλέφωνα, κινητά ακόμα και softphones, δηλαδή λογισμικά που βασίζονται στο SIP πρωτόκολλο
- **Proxy Server:** Ένα ενδιάμεσο τερματικό που λειτουργεί σαν server και σαν client. Σκοπός του είναι να κατασκευάζει SIP αιτήματα (requests) εκ μέρους άλλων clients. Τα αιτήματα αυτά εξυπηρετούνται είτε εσωτερικά στον server είτε προωθούνται σε άλλους Servers. Ο proxy server είτε λαμβάνει τα μηνύματα των agents και τα προωθεί, ή αν είναι απαραίτητο τροποποιεί τα request μηνύματα προτού τα προωθήσει.
- **Redirect Server:** Σκοπός αυτής της οντότητας είναι να παράγει και να αποστέλλει απαντήσεις με κωδικό 3xx στα requests που λαμβάνει, ενημερώνοντας έτσι τον χρήστη, τις διευθύνσεις που ζητάει για την πραγματοποίηση της συνεδρίας.
- **Registar:** Η οντότητα που δέχεται τα REGISTER αιτήματα, με σκοπό να ανανεώσει την βάση δεδομένων της, με τα στοιχεία του χρήστη που στέλνει το αίτημα.



Εικόνα 4: Packet capture μια τυχαίας κλήσης μεταξύ δύο τερματικών

3.1.2. SIP Μηνύματα

Τα SIP μηνύματα μπορούν να χωριστούν σε δύο βασικές κατηγορίες:

Αιτήματα (Requests) και Απαντήσεις (Responses).

Όπως προαναφέραμε τα SIP αιτήματα αποστέλλονται από τους clients προς τους servers και οι απαντήσεις από τον server προς τους clients.

3.1.3. SIP Request

Τα SIP Request, αποτελούνται από τα ακόλουθα μηνύματα:

- INVITE: αρχικοποιείται η κλήση μεταξύ των τερματικών
- ACK: επιβεβαιώνει την τελική απάντηση από το INVITE μήνυμα
- BYE: τερματίζει την κλήση
- CANCEL: ακυρώνει τον κωδωνισμό και την αναζήτηση του απέναντι χρήστη
- OPTIONS: ρωτάει τις δυνατότητες και τους όρους του απέναντι τερματικού
- REGISTER: καταχωρεί τον client στο Location Service
- INFO: στέλνει διάφορες πληροφορίες κατά την διάρκεια της συνεδρίας χωρίς να επηρεάζει την υπάρχουσα κλήση

3.1.4. SIP RESPONSE

Μετά την παραλαβή του Request μηνύματος, ο παραλήπτης απαντά με ένα SIP Response μήνυμα, που υποδηλώνει την κατάσταση του server . Η απάντηση ξεκινάει με τον αριθμό του SIP version που χρησιμοποιείται, ακολουθώντας έναν τριψήφιο κωδικό απάντησης (response code) και ένα επεξηγηματικό πεδίο για το status code.

Τα status codes περιλαμβάνουν:

- 1xx: πληροφοριακή απάντηση για την συνέχιση της διαδικασίας του αιτήματος. Πχ 100 trying and 180 ringing.
- 2xx: απάντηση ότι το αίτημα ολοκληρώθηκε επιτυχώς
- 3xx: είναι απάντηση από τους ενδιάμεσους servers (redirect) στο request Invite
- 4xx: client error. Είτε η το αίτημα είναι λάθος γραμμένο, είτε ο server δεν μπορεί να ολοκληρώσει το αίτημα
- 5xx: είναι απάντηση στο αίτημα που έγινε, πως δεν μπορεί να ολοκληρωθεί λόγω προβλήματος στον server

- 6xx: είναι γενικό μήνυμα ώστε να ενημερώσει πως το αίτημα δεν μπορεί να εξυπηρετηθεί από κανέναν server.

3.2. RTP

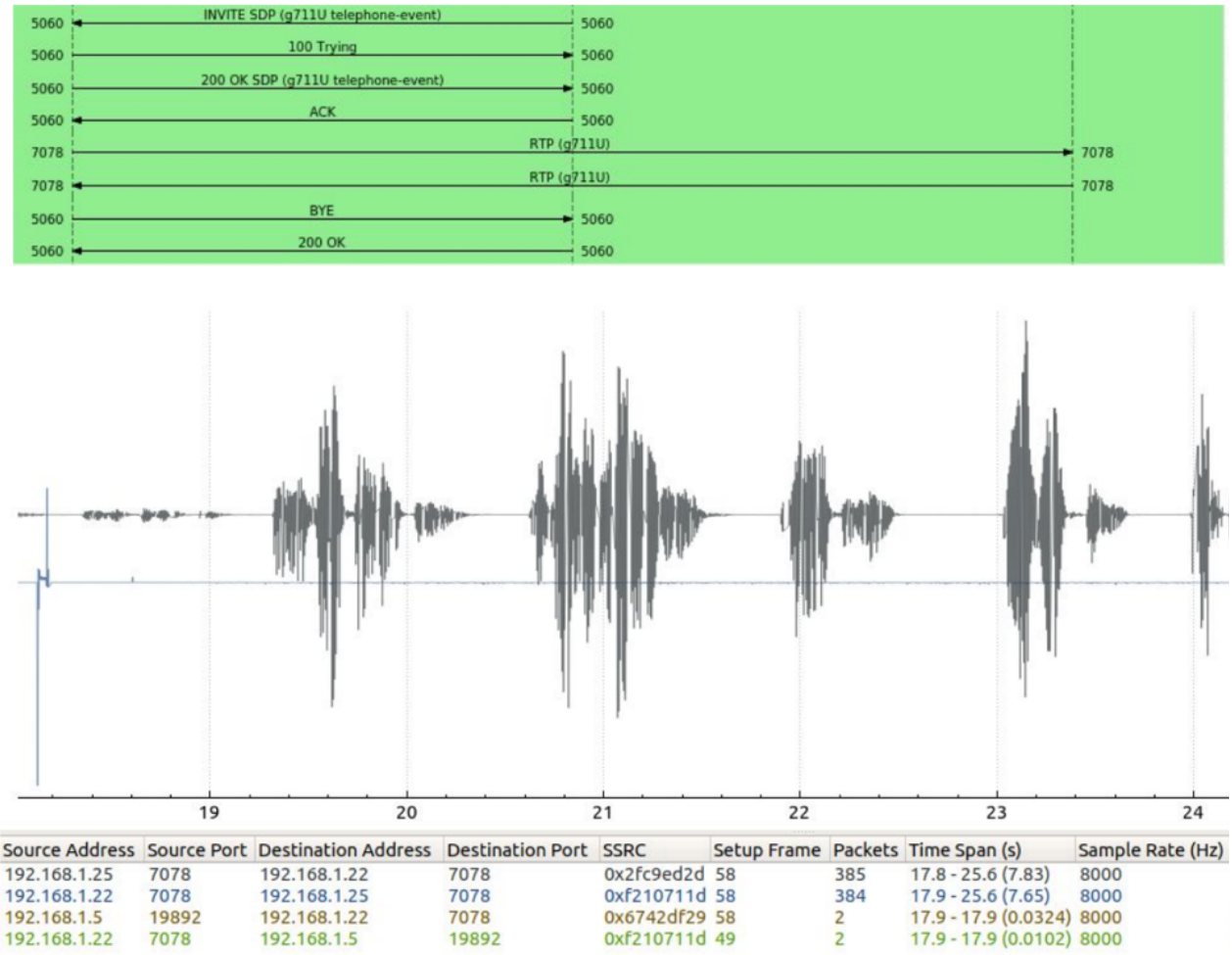
Το RTP πρωτόκολλο (Real-Time Transport Protocol) είναι υπεύθυνο για την μεταφορά των πακέτων video και φωνής σε πραγματικό χρόνο. Οι υπηρεσίες που προσφέρει και απαρτίζουν το πρωτόκολλο είναι η αναγνώριση του τύπου του πακέτου, η κατοχύρωση του αριθμού του πακέτου βάση σειράς, η χρονική στιγμή που το πακέτο μπήκε στο μέσο, καθώς και ο έλεγχος για την παράδοση των πακέτων. Το RTP υποστηρίζει μεταφορά δεδομένων σε πολλαπλούς προορισμούς χρησιμοποιώντας την μετάδοση μέσω multicast πακέτων, ενώ το πρωτόκολλο που χρησιμοποιεί για την μεταφορά των πακέτων σε πραγματικό χρόνο είναι το UDP[9]. Συνεπώς το RTP δεν έχει κάποιο μηχανισμό και δεν εγγυάται, για τον έλεγχο της επιτυχούς μεταφοράς των δεδομένων στον προορισμό τους την σωστή χρονική στιγμή ή με την σωστή σειρά, για αυτό και βασίζεται σε πρωτόκολλα χαμηλότερου στρώματος για την δουλειά αυτή.

Στην παρακάτω εικόνα (Εικόνα 5) παρατηρούμε ότι τα πακέτα φωνής που διαβάσαμε με την βοήθεια του Wireshark, κατά την διάρκεια μίας κλήσης μεταξύ δύο τερματικών, βασίζονται στο RTP πρωτόκολλο.

66 17.790191286	192.168.1.25	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2FC9ED2D, Seq=1,
69 17.811682697	192.168.1.25	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2FC9ED2D, Seq=2,
70 17.820811926	192.168.1.25	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2FC9ED2D, Seq=3,
76 17.862873007	192.168.1.25	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2FC9ED2D, Seq=4,
77 17.865448210	192.168.1.22	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xF210711D, Seq=0,
78 17.870624806	192.168.1.5	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6742DF29, Seq=32
79 17.875621930	192.168.1.22	192.168.1.5	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xF210711D, Seq=1,
83 17.890572705	192.168.1.5	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6742DF29, Seq=32
84 17.903032127	192.168.1.5	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x6742DF29, Seq=32
85 17.906063250	192.168.1.22	192.168.1.25	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xF210711D, Seq=2,
86 17.925332199	192.168.1.22	192.168.1.25	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xF210711D, Seq=3,
87 17.930803924	192.168.1.25	192.168.1.22	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x2FC9ED2D, Seq=8,
88 17.935534049	192.168.1.22	192.168.1.25	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xF210711D, Seq=4,

Εικόνα 5: Packet capture από RTP πακέτα

Επιπλέον, βάζοντας τα RTP πακέτα που έχουμε συλλάβει, στο RTP player του Wireshark, μπορούμε να ακούσουμε την συνομιλία, όπως φαίνεται στην Εικόνα 6.



Εικόνα 6: Wireshark Player για πακέτα RTP

3.3. SDP

Το πρωτόκολλο SDP (Session Description Protocol), όπως χαρακτηρίζει και το όνομα του, είναι υπεύθυνο να ενημερώσει το καλούντα για τις παραμέτρους της κλήσης που έχει θέσει ο καλών πριν προχωρήσουν στην πραγματοποίηση της κλήσης. Οι παράμετροι που περιλαμβάνονται στο μήνυμα είναι συνήθως πληροφορίες όπως οι codecs που χρησιμοποιούνται, IP address και πόρτες, καθώς και ο τύπος της κλήσης (voice ή video). Τις παραμέτρους αυτές μπορούμε να τις βρούμε στα μηνύματα INVITE.

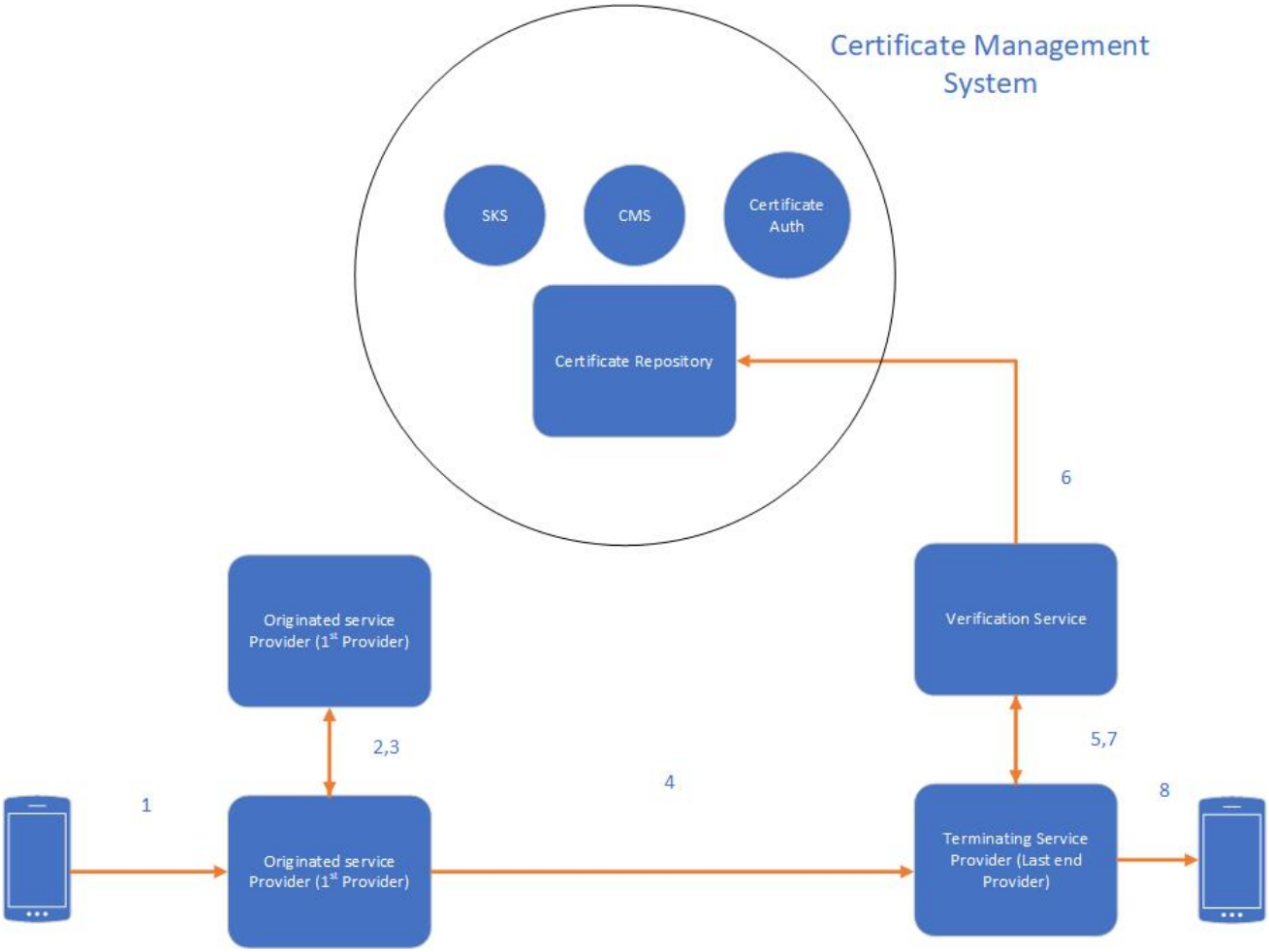
3.4. STIR/SHAKEN Protocols

Πρόσφατες έρευνες που αφορούσαν τις τηλεφωνικές απάτες που έχουν γίνει τα τελευταία χρόνια στην Αμερική, αναφέρουν πως μέχρι και το 2020 έχουν καταγραφεί πάνω από 5.5 δισεκατομμύρια κλήσεις απάτης και robocalls (αυτοματοποιημένες κλήσεις με εγγεγραμμένα μηνύματα), με αποτέλεσμα να αποσπάσουν περίπου κοντά στα 429 εκατομμύρια δολάρια. Οι κακόβουλοι χρήστες προσπαθούν πρώτα να αποπλανήσουν τα θύματα τους με τέτοιο τρόπο ώστε ο αριθμός από τον οποίο καλούν, να φαίνεται ως κάποιος άλλος. Παραδείγματος χάρη, κλήσεις που πραγματοποιούνται από άλλες χώρες, φαίνονται ότι γίνονται από την χώρα του καλούντα ώστε να κάνουν το θύμα πιο άνετο στο να απαντήσει την κλήση. Έχει παρατηρηθεί επίσης, πως οι κακόβουλοι χρήστες μέσα από social engineering μπορούν να καταφέρουν να αποσπάσουν προσωπικές πληροφορίες από τον χρήστη, όπως την χώρα στην οποία μένει, την περιοχή, την διεύθυνση ώστε να μπορέσουν να καλέσουν ακόμα από ένα εικονικά «γειτονικό» αριθμό. Παράδειγμα αν το θύμα είναι συνδρομητής με αριθμό 210-22xxxxx, τότε η κλήση που θα κάνει ο κακόβουλο χρήστης, μπορεί να είναι από τον αριθμό 210-22xxyyy. Η κλήση που θα πραγματοποιηθεί είναι συνήθως ένα αυτόματο ηχογραφημένο μήνυμα το οποίο αποσκοπεί στην αποπλάνηση του θύματος έναντι κάποιο ποσού, μιμούμενο ακόμα και κυβερνητικές οργανώσεις ή υπηρεσίες. Αυτού του τύπου η απάτη/επίθεση μπορεί να χρησιμοποιήσει οποιονδήποτε αριθμό από τυχαίους συνδρομητές (εκτός αν η επίθεση είναι στοχευμένη) μειώνοντας έτσι την λειτουργικότητα της τεχνολογίας VoIP.

Εταιρίες και τηλεπικοινωνιακοί φορείς, παρατηρώντας το σημαντικό αυτό πρόβλημα αλλά και την αρνητική επίδραση που έχει ανά τον κόσμο, αποφάσισαν πως πρέπει να βρεθεί μια λύση. Το FCC (Federal Communications Commission), μια ανεξάρτητη επιτροπή τηλεπικοινωνιών ανέπτυξε τους μηχανισμούς STIR/SHAKEN που θα αντιμετωπίσουν αυτού του είδους τις επιθέσεις.

Το STIR/SHAKEN είναι μια σύνθεση από πρωτόκολλα και διαδικασίες, που έχουν ως σκοπό την αντιμετώπιση των spoofed κλήσεων (κλήσεις ψεύτικο caller-id) αλλά και την επιβεβαίωση της αυθεντικότητας του αριθμού πριν την πραγματοποίηση της κλήσης. Το STIR/SHAKEN εφαρμόζει ένα κρυπτογραφημένο μηχανισμό αυθεντικοποίησης και επιβεβαίωσης, με σκοπό την κατοχύρωση της εμπιστοσύνης μεταξύ του καλών και καλούντα χρήστη. Βασίζονται σε ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές. Το STIR προσφέρει την δυνατότητα στο SIP πρωτόκολλο να αυθεντικοποιήσει τον αριθμό

τηλεφώνου (Caller-ID), ενώ το SHAKEN ορίζει την αρχιτεκτονική υποδομή στο δίκτυο τηλεφωνίας στην οποία θα υλοποιηθεί το STIR, καθώς τον μηχανισμό που θα επιβεβαιώσει τον αριθμό.



Εικόνα 7: Διαδικασία κλήσης με STIR/SHAKEN

3.4.1. STIR/SHAKEN

STIR (Secure Telephony Identity Revisited) είναι ένα το πρότυπο το οποίο είναι υπεύθυνο στο να «σκιαγραφήσει» τα πρωτόκολλα που θα χρειαστούν ώστε να δημιουργηθεί ένα ψηφιακό πιστοποιητικό για μια VoIP κλήση, διασφαλίζοντας έτσι την αυθεντικότητα του αριθμού κλήσης. Κάθε πάροχος αποκτά τα ψηφιακά πιστοποιητικά μέσα από μια έμπιστη αρχή έκδοσης πιστοποιητικών (Certificate Authority). Τα ψηφιακά πιστοποιητικά

χρησιμοποιούν δεδομένα από το SIP πρωτόκολλο ώστε να πιστοποιήσουν την ταυτότητα του καλών καθώς και την αυθεντικότητα της κλήσης. Με αυτό τον τρόπο ο πάροχος που θα δεχθεί το πακέτο SIP, θα προσθέσει δεδομένα στο header του SIP, με σκοπό να υποδείξει αν είναι σίγουρος ότι η κλήση προέρχεται από κάποιον ταυτοποιημένο συνδρομητή και αν αυτός ο συνδρομητής καλεί με τον σωστό αριθμό.

Ο πρώτος φορέας που θα δρομολογήσει την κλήση, είναι υπεύθυνος ώστε να αυθεντικοποιήσει την κλήση, πιστοποιώντας τους χρήστες με έναν από τους εξής τρείς τρόπους:

- A-Attestation: Ο πάροχος επικυρώνει την ταυτότητα του καλών αλλά και τον τηλεφωνικό αριθμό που χρησιμοποιεί
- B-Attestation: Ο πάροχος επικυρώνει την ταυτότητα του καλών αλλά όχι και τον τηλεφωνικό αριθμό που χρησιμοποιεί
- C-Attestation: Ο πάροχος είναι ο φορέας εισόδου των πακέτων φωνής που έλαβε μέσω δικτύου από μια υποδομή που δεν υποστηρίζει το το STIR/SHAKEN. Αυτό σημαίνει πως η κλήση δεν ξεκίνησε από εκείνον, απλά την δρομολογεί. Την δρομολογεί όμως αφού πρώτα ελέγξει μέσω άλλου μηχανισμού αν η κλήση είναι επιβεβαιωμένη ότι ήρθε από κάποιο άλλο έμπιστο φορέα. Σε περίπτωση που δεν είναι, η κλήση απορρίπτεται.

Ο πάροχος αφού παράξει ένα JSON token το οποίο αποτελείται από τον αριθμό του καλών, τον αριθμό του συνδρομητή που καλείται, το επίπεδο του attestation, την ακριβή ώρα και ένα αναγνωριστικό, το προσθέτει στο SIP header σε ένα νέο identity πεδίο, αφού πρώτα το κωδικοποιήσει σε μορφή base64. Έτσι κάθε πάροχος που θα λαμβάνει το πακέτο θα το δρομολογεί μέχρι να φτάσει στον προορισμό του, αφού πρώτα περάσει μέσα από υπηρεσίες επιβεβαίωσης της αυθεντικότητας. Ύστερα, η υπηρεσία αυτή αποκτά το ψηφιακό πιστοποιητικό του παρόχου από όπου ξεκίνησε η κλήση, μέσα από την κοινή «αποθήκη» ψηφιακών πιστοποιητικών, ξεκινώντας την διαδικασία επιβεβαίωσης της αυθεντικότητας.

3.4.2. Αναλυση στην λειτουργία STIR/SHAKEN

Λειτουργία επιβεβαίωσης των κλήσεων

1. Ο πάροχος λαμβάνει το SIP Invite μήνυμα και προσθέτει τον Attestation βαθμό:

Αφού λάβει ο πάροχος το πακέτο INVITE κάνει τον έλεγχο ώστε να επιβεβαιώσει τον αριθμό που καλεί ο χρήστης, προτού προωθήσει το πακέτο στον τελικό χρήστη, δηλαδή τον καλούντα

2. Ο βαθμός Attestation προστίθεται:

Ο πάροχος αφού κάνει τον απαραίτητο έλεγχο για την αυθεντικότητα του καλών αλλά και του αριθμού που αποστέλλει, όπως αναλύσαμε παραπάνω, κρίνει αναλόγως και τοποθετεί τον βαθμό εμπιστευτικότητας.

3. Ο πάροχος που λαμβάνει την κλήση πρώτος δημιουργεί το Identity header:

Ο πάροχος βλέπει τον αριθμό κλήσης και επιβεβαιώνει τον χρήστη. Για να κατοχυρώσει την επιβεβαίωση του, τοποθετεί ένα κρυπτογραφημένο ψηφιακό πιστοποιητικό στο SIP πακέτο, το οποίο περιλαμβάνει τις τιμές που αναφέρθηκαν παραπάνω

4. Ο τελευταίος πάροχος, δηλαδή αυτός που θα στείλει την κλήση στο τερματικό του καλούντα, αφού λάβει το πακέτο SIP αποκρυπτογραφεί το πιστοποιητικό, διαβάζει τις λεπτομέρειες του πακέτου, μαζί με το Attestation βαθμό ώστε να κρίνει αν είναι όλα σωστά

5. Αποστολή του πακέτου στην υπηρεσία επαλήθευσης για την αυθεντικότητα του χρήστη

6. Η υπηρεσία επαλήθευσης, ελέγχει το ψηφιακό πιστοποιητικό, περνώντας το πρώτα από διάφορες βάσεις δεδομένων

7. Αφού ολοκληρωθεί η διαδικασίας επιβεβαίωσης , τότε το πακέτο στέλνεται στον προορισμό του.

3.4.3. Ανάλυση της διαδικασίας παραγωγής, επιβεβαίωσης και χρήσης ψηφιακών πιστοποιητικών

Οι πάροχοι διαχειρίζονται τα private κλειδιά και τα ψηφιακά πιστοποιητικά μέσα από το CMS (Certificate Management Solution), τα οποίο μπορεί να είναι είτε μια λύση cloud είτε μια λύση εγκατεστημένη στην υπάρχουσα υποδομή του παρόχου.

Το CMS δημιουργεί ένα ζευγάρι από private και public κλειδιά. Με το private κλειδί ο πάροχος συντάσσει μια ψηφιακή υπογραφή, δηλώνοντας την αυθεντικότητα των δεδομένων που αποστέλλει, ενώ με το public κλειδί μπορεί να επιβεβαιώσει αυτή την υπογραφή που έχει τοποθετηθεί σε άλλα δεδομένα από άλλους παρόχους. Συνεπώς, πρέπει μόνο ο πάροχος που έχει το private κλειδί να έχει πρόσβαση σε αυτό και κανένας άλλος. Το SKS (secure key store) είναι το σημείο όπου τοποθετείται το κλειδί αυτό, ώστε να αποτραπεί τυχόν κλοπή.

Όσο αφορά τα public κλειδιά, τα οποία είναι διαθέσιμα στο CMS πρέπει με κάποιο τρόπο να υποδηλώνουν τον ιδιοκτήτη τους, αλλιώς ο κάθε κακόβουλος χρήστης θα μπορούσε να δηλώσει πως του ανήκει. Σκοπός λοιπόν όπως αναφέραμε και προηγουμένως, είναι να στηθεί μια αλυσίδα εμπιστοσύνης και για αυτό το CMS διαθέτει τα public κλειδιά σε πιστοποιητικά, δηλαδή εγγραφές που περιλαμβάνουν το public κλειδί αλλά και πληροφορίες για τον ιδιοκτήτη. Για να αποκτηθεί το πιστοποιητικό, το CMS στέλνει το public κλειδί σε μια αρχή έκδοσης πιστοποιητικών, η οποία στέλνει το πιστοποιητικό υπογεγραμμένο, με τις πληροφορίες του ιδιοκτήτη και το public κλειδί. Ύστερα το CMS το αποθηκεύει στον ίδιο χώρο με τα υπόλοιπα υπογεγραμμένα πιστοποιητικά, το οποίο μπορεί να το προσπελάσει οποιοσδήποτε πάροχος.

Τα ιδιωτικά κλειδιά θα πρέπει να μένουν πάντα ασφαλή και να είναι προσβάσιμα μόνο από τον ιδιοκτήτη. Έτσι οι πάροχοι για να διασφαλίσουν τα ιδιωτικά τα κλειδιά τους τα κρυπτογραφούν με ένα άλλο κλειδί. Η μέθοδος που χρησιμοποιείται κυρίως στα STIR/SHAKEN είναι η envelope encryption.

Με τη μέθοδο αυτή κρυπτογραφείται το ιδιωτικό κλειδί με ένα άλλο κλειδί data key το οποίο με την σειρά του κρυπτογραφείται με ένα τρίτο κλειδί , το master key. Τέλος όλα τα κλειδιά αποθηκεύονται στο SKS. Το master key αποθηκεύεται σε μια μονάδα κατασκευασμένη μόνο για κρυπτογραφικές διαδικασίες, τελείως απομονωμένη από την υπόλοιπη υποδομή. Σε αυτή τη υποδομή ολοκληρώνονται και οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης.

Όταν έρθει η στιγμή για την υπηρεσία αυθεντικοποίησης να υπογράψει μια κλήση, χρειάζεται το ιδιωτικό κλειδί. Συνεπώς, η υπηρεσία συνδέεται μέσω TLS σύνδεσης, στο SKS μεταφέροντας το κρυπτογραφημένο data key με σκοπό να το αποκρυπτογραφήσει το master key. Μετά την αποκρυπτογράφηση του data key, το κλειδί μεταφέρεται σε αναγνώσιμη μορφή μέσα από το ίδιο TLS session στην υπηρεσία αυθεντικοποίησης. Το data key αποκρυπτογραφεί το ιδιωτικό κλειδί ώστε να μπορέσει η υπηρεσία να υπογράψει με το ιδιωτικό κλειδί την κλήση. Μετά την ολοκλήρωση της διαδικασίας ψηφιακής υπογραφής, τα κλειδιά δεν αποθηκεύονται κάπου και έτσι καταστρέφονται.

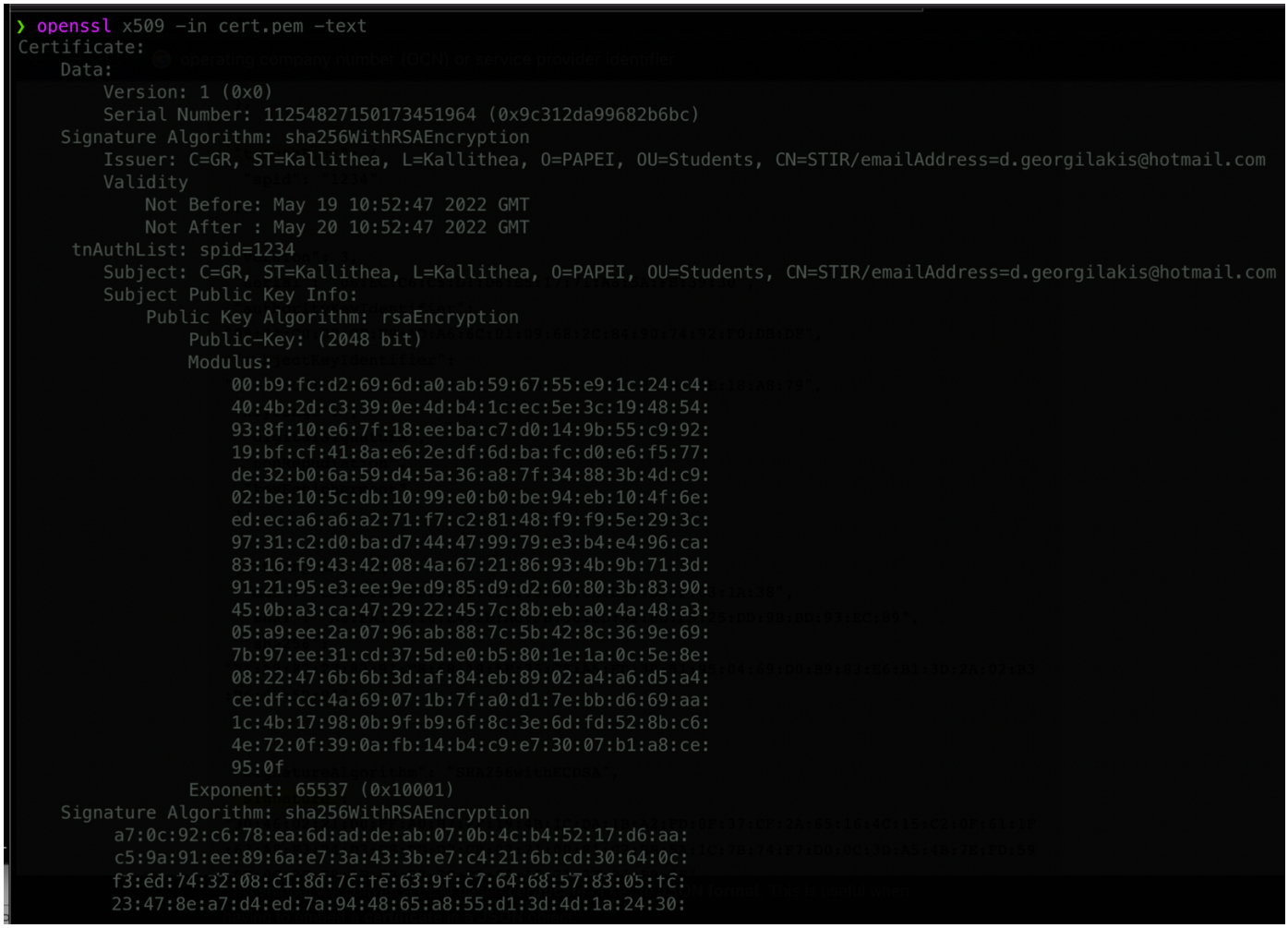
Σύμφωνα με τους κανόνες ασφάλειας, κανένας πάροχος δεν μπορεί να ζητήσει ή να αιτηθεί πιστοποιητικά χωρίς να πληροί τους βασικούς κανόνες που θέτονται από τον PA (Policy Administrator). Αυτό σταματά τους κακόβουλους χρήστες από το να υπογράφουν τις

κλήσεις (σε περίπτωση που έχουν ζητήσει πιστοποιητικό από την αρχή). Ο PA πρέπει πάντα να είναι μια οντότητα εμπιστοσύνης. Για να μπορέσει ο PA να εγκρίνει στους παρόχους τα αιτήματα των πιστοποιητικών, θα πρέπει ο πάροχος να ζητήσει ένα *service code token*, που περιλαμβάνει το OCN[15] ή SPID[16] του παρόχου. Αν ο PA πιστοποιήσει την ταυτότητα του παρόχου, και το αίτημα του εγκριθεί, τότε επιστρέφει το token με το SPID. Έτσι ο πάροχος είναι ικανός πλέον, να ζητήσει πιστοποιητικά.

Συνοπτικά μπορούμε να αναφέρουμε τα εξής:

- STI-AS (STI- Authentication Server): Είναι υπεύθυνος στο να υπογράφει τα αιτήματα, έχοντας πρόσβαση στο SKS
- STI-VS (STI-Verification Server): είναι υπεύθυνος στο επιβεβαιώνει τα αιτήματα διαβάζοντας τα δημόσια κλειδιά των παρόχων.
- Authenticator: Είναι η οντότητα που αποτελείται από τα STI-AS και STI-VS και εφαρμόζει τις διαδικασίες υπογραφής για να δημιουργήσει και επιβεβαιώσει τις ψηφιακές υπογραφές.
- SKS (Secure Key Store): Είναι η οντότητα που τα ιδιωτικά κλειδιά των παρόχων είναι αποθηκευμένα και καλείται να τα προμηθεύσει σε αυτούς, όταν έρθει η ώρα της υπογραφής μια κλήσης.
- STI-CR (Certificate Repository): Είναι ο server που περιέχει όλα τα ψηφιακά πιστοποιητικά και είναι διαθέσιμος σε όλους τους παρόχους μέσω του διαδικτύου. όπως αναφέραμε πρέπει τα δημόσια κλειδιά να είναι ασφαλή οπότε η διαδικασία προσπέλασης γίνεται μέσω TLS.
- SP-KMS (Key Management Server): Ο KMS server είναι υπεύθυνος στο να ζητάει τα *service code token* όπως προαναφέραμε, από τον AP. Στην συνέχεια ζητάει το ψηφιακό πιστοποιητικό, καθότι έχει γίνει η ταυτοποιήση στο προηγούμενο βήμα και στην συνέχεια παράγει το ιδιωτικό και δημόσιο κλειδί του. Το ιδιωτικό στέλνεται στον SKS, ενώ το δημόσιο στον STI-CR

Για να γίνει το αίτημα ενός πιστοποιητικού, ο πάροχος πρέπει να κατασκευάσει ένα Certificate Signing request (CSR), μαζί με το token και να το στείλει για έγκριση στην αρχή έκδοσης πιστοποιητικών. Αν το αίτημα είναι σωστό και σύμφωνο με τις πολιτικές ασφαλείας, τότε το ψηφιακό πιστοποιητικό εκδίδεται. Τέλος κάθε πάροχος που διαβάζει το πιστοποιητικό που έχει εκδοθεί, κοιτάει την αρχή έκδοσης. Αν ανήκει στις έμπιστες αρχές τότε το πιστοποιητικό θεωρείται έμπιστο.



Εικόνα 8: Δείγμα πιστοποιητικού με SPID value

Όπως φαίνεται και στην Εικόνα 8, το πιστοποιητικό περιέχει τις πληροφορίες του παρόχου που κατέχει το πιστοποιητικό, το δημόσιο κλειδί, το SPID, το χρονικό περιθώριο που το πιστοποιητικό είναι έγκυρο, αλλά και την αρχή που το εξέδωσε. Οι τιμές του πιστοποιητικού δεν θα αναλυθούν αλλά παρατηρούμε την παράμετρο *tnAuthList*. Η τιμή αυτής της παραμέτρου, περιλαμβάνει το SPID του παρόχου. Παρόλα αυτά σε κάποια πιστοποιητικά SHAKEN, η τιμή του *tnAuthList* δεν περιλαμβάνει μόνο το SPID αλλά και τους αριθμούς από τους οποίους ένας συνδρομητής μπορεί να καλέσει, χωρίς όμως ο πάροχος αυτός να τους έχει εκδώσει. Αυτά τα πιστοποιητικά ονομάζονται PoP certificates (Proof of Possesion). Συνεπώς, για να μπορέσει ένα πάροχος να υπογράψει την αυθεντικότητα της κλήσης για έναν αριθμό που δεν του ανήκει, ενημερώνει με το πιστοποιητικό τους αριθμούς από όπου επιτρέπεται να καλέσει ο συνδρομητής.

Σε περίπτωση που ένα πιστοποιητικό λήξει ο πάροχος θα ελέγξει αυτή τη τιμή και αν βρεί ότι έχει ξεπεράσει τον χρόνο εγκυρότητας θα το απορρίψει. Σε περίπτωση όμως που κάποιος κακόβουλος χρήστης ανακαλύψει το ιδιωτικό κλειδί ενός παρόχου, θα μπορεί να υπογράφει τις κλήσεις του και να τις προωθεί κανονικά στο δίκτυο τηλεφωνίας. Έτσι, θα πρέπει ο πάροχος με το που ανακαλύψει ότι το κλειδί του κλάπηκε να ενημερώσει την αρχή έκδοσης ώστε να ακυρώσει το πιστοποιητικό.

Αυτό μπορεί να γίνει χρησιμοποιώντας τα πρωτόκολλα CRL ή OCSP. Με το CRL ο πάροχος που θα επιβεβαιώσει το πιστοποιητικό (ή υπηρεσία επιβεβαίωσης του παρόχου) θα ζητήσει ένα αρχείο που περιλαμβάνει όλα τα μη έγκυρα πιστοποιητικά. Έτσι, θα ελέγξει αν ανήκει το συγκεκριμένο πιστοποιητικό στην λίστα και θα πράξει αναλόγως. Με το OCSP ρωτάει απευθείας την αρχή που εξέδωσε το πιστοποιητικό για την εγκυρότητα του.

3.4.4. Ανάλυση στην διαδικασία υπογραφής των κλήσεων

1. Ο πάροχος λαμβάνει την κλήση μέσω SIP και στέλνει το SIP πακέτο στον STI-AS server ώστε να αυθεντικοποιήσει την ταυτότητα του καλών

```
POST /stir/v1/signing HTTP/1.1
Host: 172.24.74.141:8443
User-Agent: python-requests/2.21.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 166
Content-Type: application/json
{
   "signingRequest":{
      "attest":"A",
      "orig":{ "tn": "4748131408" },
      "dest":{ "tn": [ "4748118185" ] },
      "profile": 1,
      "iat":1559639847,
      "origid":"de305d54-75b4-431b-adb2-eb6b9e546014"
   }
}
```

Εικόνα 9: Αρχείο JSON με τις παράμετρους του STIR/SHAKEN

- Originating DN: ο αριθμός του καλών
- Destination DN: ο αριθμός του καλούντα
- IAT: η χρονική στιγμή που ξεκίνησε η κλήση

- Origination ID: ένα μοναδικό χαρακτηριστικό που βοηθά στην επιστροφή της κλήσης
- Attestation level: ο βαθμός εμπιστευτικότητας (A, B, C)

2. Μόλις το αίτημα για την υπογραφή ληφθεί ο STI-AS δημιουργεί το Identify header που προαναφέραμε, που στην ουσία είναι η ψηφιακή υπογραφή. Ύστερα κωδικοποιείται σε μορφή base64.

- Το header αποτελείται από:
- Τον αλγόριθμο κρυπτογράφησης της υπογραφής
- Το πρωτόκολλο
- Τον τύπο του πρωτοκόλλου

Και το στοιχείο x5u που περιλαμβάνει το http url του server (STI-CR) που περιλαβάνει τα πιστοποιητικά

Τέλος η υπογραφή στο κάτω μέρος διαβεβαιώνει τον τελικό πάροχο πως η κλήση είναι ταυτοποιημένη, αφού περιλαμβάνει την υπογραφή του παρόχου που το κρυπτογράφησε με το ιδιωτικό του κλειδί. Το πακέτο αποστέλλεται.

3. Μόλις λάβει το πακέτο ο SBC τοποθετεί το νέο Identity header στο SIP πακέτο σύμφωνα με την Εικόνα 10

```
INVITE sip: 4748131408@example.com:5060 SIP/2.0
Via: SIP/2.0/UDP example.com:5060
From: "Alice" <sip:47481314O8@5.6.7.8:5060>;tag=123456789
To: "Bob" <sip:4748118185@1.2.3.4:5060>
Call-ID: 1-12345@5.6.7.8
CSeq: 1 INVITE
Max-Forwards: 70
Identity:
eyJhbGciOiJFUzI1NiIsInBwdCI6InNoYWtlbiIsInR5cCI6InBhc3Nwb3J0IiwieDV1Ij
oiaHR0cDovL2Jhc3Nvb24ubXZsMy5kYXRjb24uY28udWsvc2hha2VuXzAuY3J0In0=.eyJ
hdHRlc3QiOiJBIiwiZGVzdCI6eyJ0biI6WyI0NzQ4MTE4MTg1Il19LCJpYXQiOjE1NTk2M
zk4NDcsIm9yaWciOnsidG4iOiI0NzQ4MTMxNDA4In0sIm9yaWdpZCI6ImRlMzA1ZDU0LTc
1YjQtNDMxYi1hZGIyLWViNmI5ZTU0NjAxNCJ9.xUZWsNaKe6xFKHpHFFd5JtXKfYTUTZM9
iKfNK-BK4-nF-dDQQ1h8dvgVzidejchQKMYsFcHAsHcG89b-
MUQWQQ==;info=<http://bassoon.mvl3.datcon.co.uk/shaken_0.crt>;alg=ES25
6;ppt=shaken
```

Εικόνα 10: SIP πακέτο με το identity field

4. Μόλις λάβει ο τελικός πάροχος το πακέτο ο δικός του SBC διαβάζει την ψηφιακή υπογραφή από το SIP μήνυμα και το στέλνει ένα αίτημα επιβεβαίωσης στον STI-VS

5. Ο STI-VS server διαβάζει τις αντίστοιχες λεπτομέρειες και εξάγει το αντίστοιχο ψηφιακό πιστοποιητικό από το STI-CR του πρώτου παρόχου, ώστε να επιβεβαιώσει την αυθεντικότητα της ψηφιακής υπογραφής. Ανάλογα το αποτέλεσμα τοποθετείται και μια τιμή στον παράγοντα *vertstat.* Οι τιμές μπορεί να είναι

- TN-Validation-Passed: επιτυχής ταυτοποίηση
- TN-Validation-Failed: ανεπιτυχής ταυτοποίηση
- No-TN-Validation: δεν βρέθηκε υπογραφή


```
HTTP/1.1 200 OK
X-Span-ID: 02457fca-af45-4e20-8faf-5ea9c2497471
Content-Type: application/json
Date: Tue, 04 Jun 2019 09:17:27 GMT
X-Msw-Message-ID: be9d0ba7-3f57-4483-88e2-f7af78b5a607

{
   "verificationResponse":{
      "attest":"A",
      "origid":"de305d54-75b4-431b-adb2-eb6b9e546014",
      "ppt":"shaken",
      "verstat":"TN-Validation-Passed"
   }
}
```


Εικόνα 11: JSON αρχείο με τον verification status

6. Το αποτέλεσμα συμπεριλαμβάνεται στο πακέτο JSON και στέλνεται πίσω στον SBC ο οποίος αναλόγως πράττει για το πακέτο

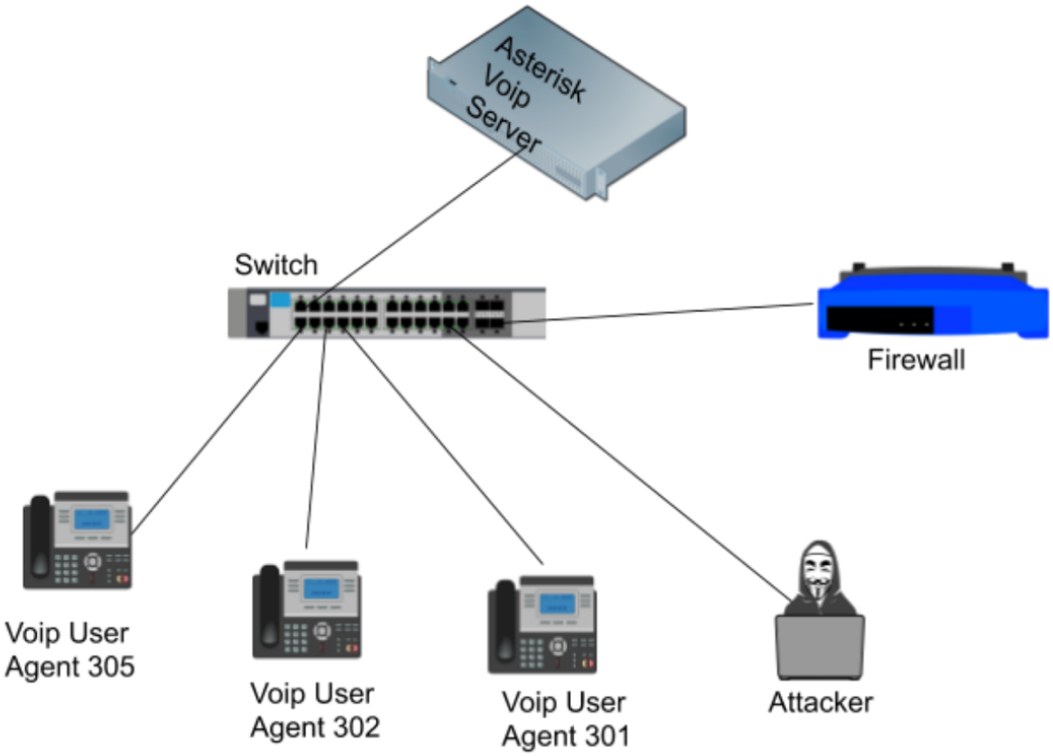
4. Environment Setup - VoIP attacks

4.1. Τοπολογία Lab

Για το proof-of-concept στήθηκε ένα Voip Lab το οποίο αποτελείται από έναν Asterisk Server που «τρέχει» σε Raspberry 3b docker container, ένα Mikrotik switch, 2 softphones (Zoiper και Linphone) και ένα Juniper V-SRX Firewall/Router.

Η επιθέσεις έγιναν από 3 τερματικά με Kali και MacOS, λογισμικό.

- Asterisk (192.168.1.28 outside NAT subnet – 172.17.0.0/16 docker inside subnet) Opensource SIP Server – Raspberry 3b - Docker container
- Attacker1 MacOS (192.168.1.17)
- Attacker2 Kali (192.168.1.18)
- Attacker3 MacOS (Dynamic IP)
- Zoiper 305 EXT (192.168.1.6)
- Linphone 302 EXT (192.168.1.12)



Εικόνα 12: Τοπολογία και υποδομή VoIP

4.2. SIP Enumeration

Το πιο σημαντικό σε μια επίθεση είναι η ανίχνευση και η απαρίθμηση των στοιχείων μιας υποδομής. Συνεπώς, για να μπορέσουμε να επιτεθούμε επιτυχώς στην υπάρχουσα VoIP υποδομή, θα πρέπει να ανιχνεύσουμε και να εντοπίσουμε καθετί που σχετίζεται με την VoIP τεχνολογία, πχ. SIP servers και πόρτες που είναι ανοιχτές.

Τα εργαλεία που χρησιμοποιήθηκαν για την ανίχνευση των SIP τερματικών στο LAB μας ήταν τα:

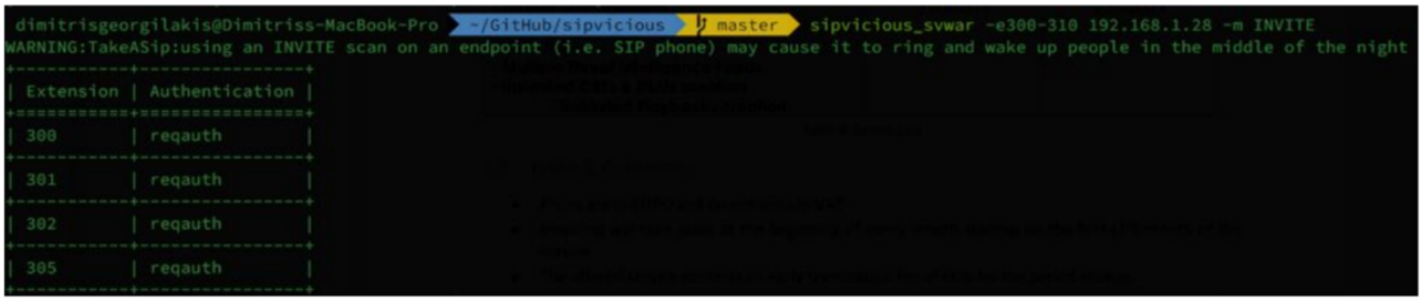
- Svmap. Το svmap είναι ένα ισχυρό SIP scanner το οποίο μπορεί να ανιχνεύσει οποιονδήποτε SIP Server λειτουργεί στην επιτιθέμενη υποδομή.
- Svwar. Το svwar είναι εργαλείο με το οποίο μπορούμε να ανιχνεύσουμε ενεργά SIP extensions, όπως επίσης και μη ενεργά αλλά κατοχυρωμένα/ρυθμισμένα extensions στον server, με την βοήθεια του INVITE πακέτου.

Και τα δύο εργαλεία ανήκουν στην σουίτα του Sipvicious.

Αρχικά όπως φαίνεται και στην εικόνα, χρησιμοποιείται το Svmap ώστε να σαρώσει και να καταγράψει κάθε SIP server στο δίκτυο μας. Το Svmap κατάφερε και εντόπισε έναν Asterisk Server version 16.10 με IP 192.168.1.20 που «ακούει» στην πόρτα 5060 UDP, όπως φαίνεται και στην Εικόνα 13

Εικόνα 13: Svmap tool

Έτσι γνωρίζοντας πλέον τον SIP Server μπορούμε να προχωρήσουμε στην σάρωση των extensions. Σε αυτό το σημείο θα χρησιμοποιήσουμε το Svwar μέσω του οποίου θα στείλουμε ένα INVITE μήνυμα στον Asterisk Server, μαζί με μια λίστα από extensions, με σκοπό να πάρουμε κάποια απάντηση με τα πιθανά υπαρκτά extensions, όπως φαίνεται και στην Εικόνα 14



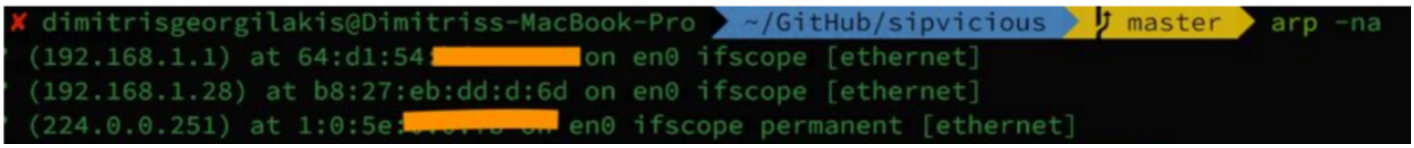
Εικόνα 14: Svwar tool

Έχοντας πλέον εντοπίσει και καταγράψει όλη την VoIP υποδομή, μπορούμε να προχωρήσουμε στο επόμενο βήμα της επίθεσης.

4.3. Man in the Middle

Η επίθεση man in the middle (MITM) είναι η επίθεση στην οποία ο επιτιθέμενος δηλώνει πως είναι κάποιος άλλος, ξεγελώντας το θύμα με σκοπό να τον εμπιστευτεί. Ο επιτιθέμενος με την σειρά του για να κρυφτεί και να μην γίνει αντιληπτός, προωθεί όλα τα δεδομένα στον σωστό προορισμό, παρακολουθώντας και υποκλέπτοντας όμως κάθε πληροφορία.

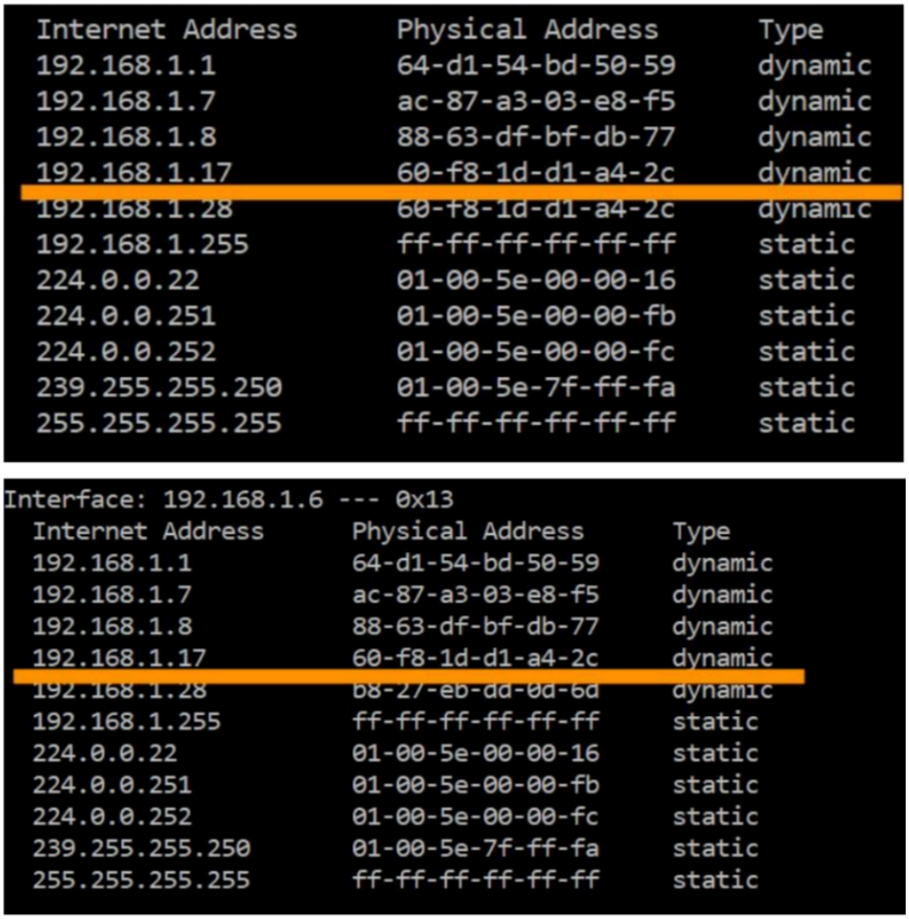
Συνεπώς, έτσι πραγματοποιήθηκε και η επόμενη επίθεση. Σκοπός ήταν να υποκλέψουμε τα RTP πακέτα που αντάλλασσαν τα δυο τερματικά ώστε να ακούσουμε τις κλήσεις τους. Ολοκληρώνοντας την ανίχνευση της υποδομής και βρίσκοντας τον SIP server, κάνουμε ένα ping στον server. Η MAC Address του, καθώς βρισκόμαστε στο ίδιο δίκτυο, αποθηκεύεται στο τοπικό ARP[10] table του τερματικού. Στην συνέχεια θα πρέπει με κάποιο τρόπο να ενημερωθούν όλα τα τερματικά στο δίκτυο ότι ο SIP server, είναι στην πραγματικότητα το τερματικό του κακόβουλου χρήστη. Προφανώς μόλις ολοκληρωθεί η παραπάνω διαδικασία επίθεσης, θα πρέπει ο κακόβουλος χρήστης αφού πρώτα υποκλέπτει την κίνηση των πακέτων, να προωθεί τα πακέτα στον πραγματικό SIP server, ώστε να αποφευχθεί η αναγνώριση της επίθεσης.



Εικόνα 15: ARP table του κακόβουλου χρήστη

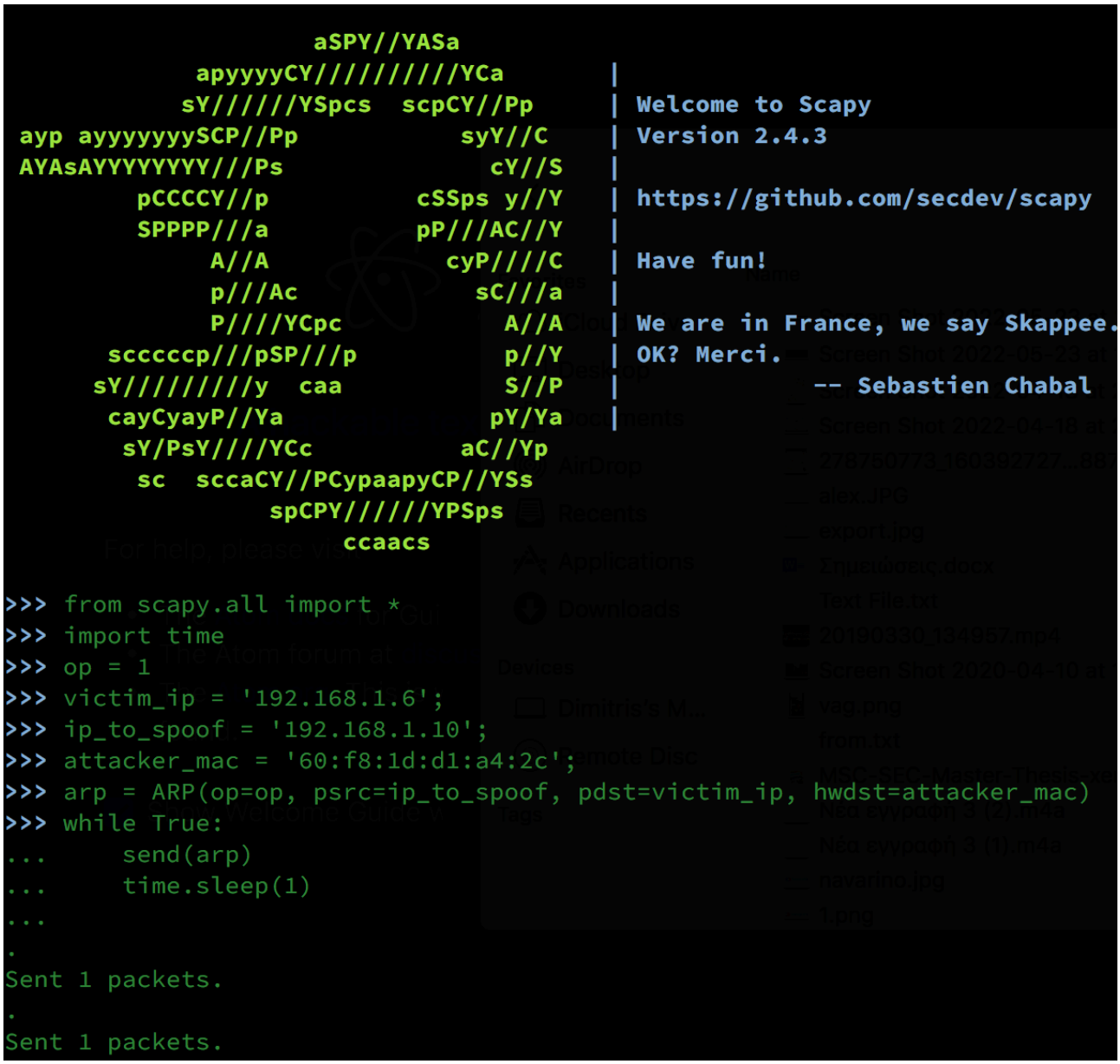
Για να προχωρήσουμε στην επίθεση, χρησιμοποιούμε κώδικα που φτιάξαμε για το Scapy. Το Scapy είναι ένας κώδικας βασισμένος σε Python που δίνει την δυνατότητα στον χρήστη να στέλνει, να υποκλέπτει, να αποκωδικοποιεί διάφορα πρωτόκολλα και να κατασκευάζει SIP πακέτα.

Στην δική μας περίπτωση επιλέξαμε την επίθεση ARP Spoofing[11]. Ο κώδικας μας, στέλνει ένα broadcast πακέτο κάθε 1 δευτερόλεπτο, βομβαρδίζοντας έτσι τα θύματα με το τροποποιημένο πλέον ARP request. Τα περισσότερα θύματα έχουν ήδη στο ARP table τους μια εγγραφή για το request που στέλνουμε, κάτι το οποίο θα σημειωθεί ως διπλή εγγραφή. Τα περισσότερα λειτουργικά συστήματα δεν διαγράφουν τις διπλές εγγραφές.



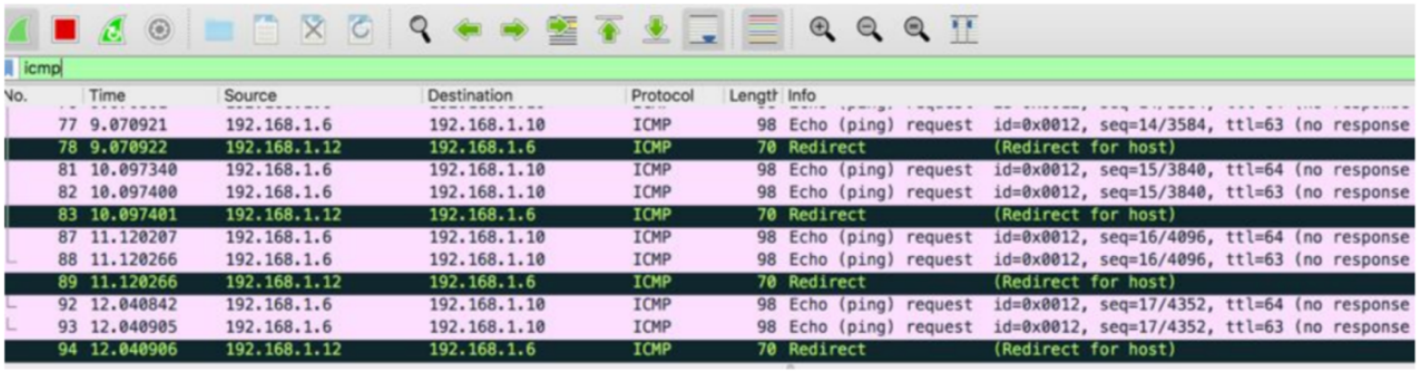
Εικόνα 16: ARP table του θύματος πριν και μετά την επίθεση

Μετά την παραμετροποίηση του κώδικα στο Scapy, η επίθεση είναι έτοιμη. Όπως φαίνεται και στην Εικόνα 17, προσπαθούμε να κατασκευάσουμε ARP replies που περιέχουν την IP του SIP server μαζί με την MAC Address του κακόβουλου τερματικού. Το πακέτο θα σταλεί στο θύμα, ανανεώνοντας έτσι το ARP table του, με σκοπό να συνδεθεί ο user agent στον SIP server στέλνοντας τα πακέτα πρώτα από το σύστημα του κακόβουλου τερματικού. Έτσι ο επιτιθέμενος θα έχει πλήρη πρόσβαση σε όλα τα δεδομένα που θα ανταλλάξουν το θύμα και ο SIP server.



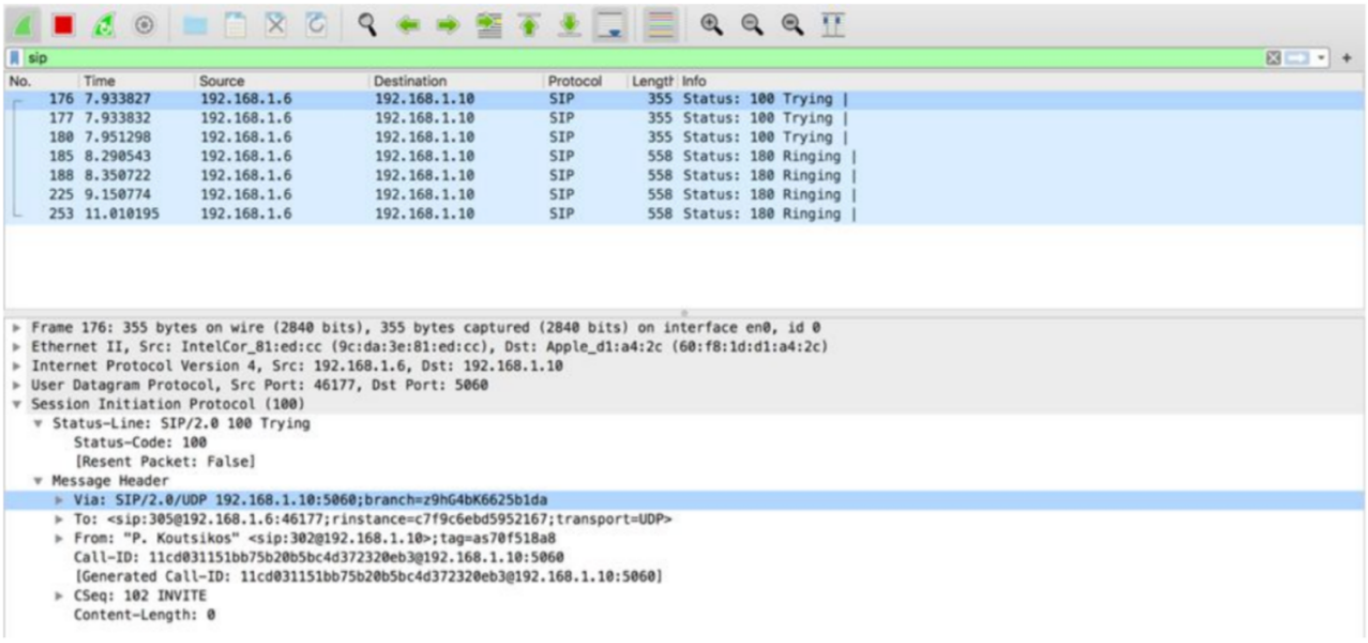
Εικόνα 17: Scapy code

Όπως φαίνεται και στην Εικόνα 16, ο κώδικας έχει ήδη σταλεί με επιτυχία, κάνοντας έτσι το θύμα να ανανεώσει τον ARP πίνακα του. Κάνοντας ένα ping από το τερματικό του θύματος (Εικόνα 18) προς τον Asterisk server, θα δούμε ότι ο κακόβουλος χρήστης λαμβάνει πρώτος το πακέτο και εν συνεχεία το προωθεί στον επιθυμητό προορισμό.



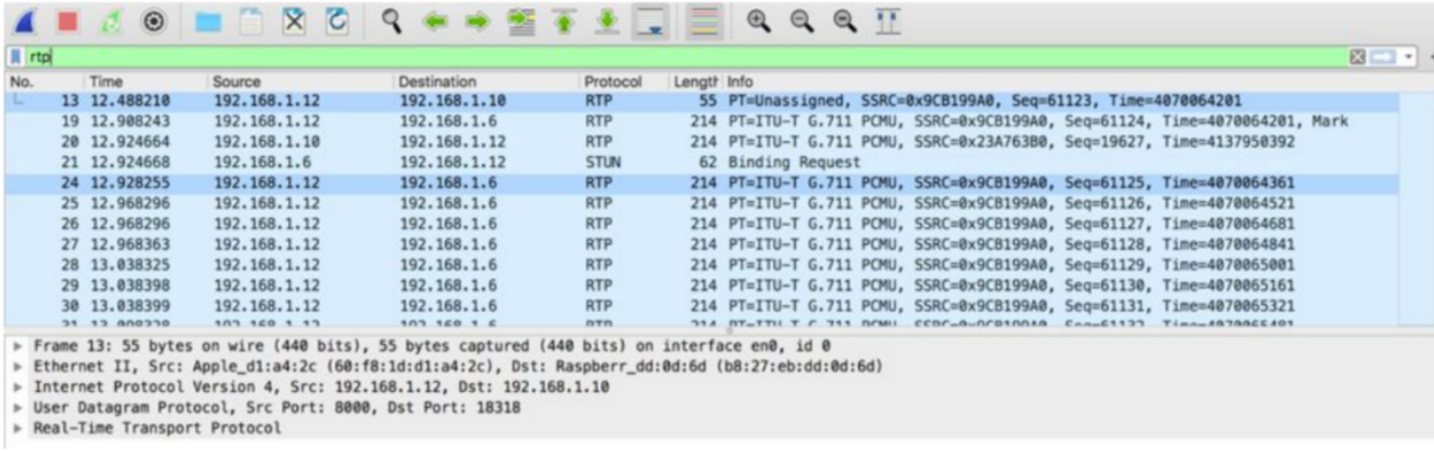
Εικόνα 18:Wireshark capture που δείχνει την αναδρομολόγηση των πακέτων μέσα από τον κακόβουλο χρήστη

Επίσης βλέπουμε στην Εικόνα 19, ότι User Agent του θύματος έχει συνδεθεί στον SIP server, αφού πρώτα περνάει όλη την κίνηση μέσα από το κακόβουλο τερματικό χωρίς να το γνωρίζει



Εικόνα 19: MITM Wireshark capture των πακέτων

Και το ίδιο ισχύει και στην Εικόνα 20 υποκλέπτοντας πλέον τα RTP πακέτα



Εικόνα 20: MITM Wireshark capture των πακέτων RTP

4.4. SIP Attacks - InviteFlood DOS Attack

Η επίθεση Dos, είναι μια μορφή δικτυακής επίθεσης, η οποία αποσκοπεί στην δικτυακή ή συστημική αχρήστευση ενός τερματικού η ακόμα και ολόκληρης της υποδομής. Ένας από τους τύπους μιας Dos επίθεσης, επιτυγχάνεται με την μαζική και μεγάλου όγκου σε συχνότητα, αποστολή μηνυμάτων, σκοπεύοντας έτσι να υπερφορτώσει όλες τους πόρους του θύματος και να τους καταστήσει μη διαθέσιμους.

Η επίθεση πραγματοποιήθηκε μέσω της Dos επίθεσης Invite Flood, κατά την οποία το θύμα δεν κατέστη δυνατό να πραγματοποιήσει καμία κλήση. Όπως θα δούμε και στην συνέχεια, αυτή η επίθεση είναι το κλειδί για τις επόμενες που πραγματοποιήθηκαν. Η πιο διαδεδομένη επίθεση σε κάθε VoIP σύστημα είναι ο βομβαρδισμός με SIP πακέτα την SIP υποδομή του θύματος.

Το InviteFlood είναι ένα εργαλείο που εξαπολύει DOS επιθέσεις χρησιμοποιώντας SIP INVITE πακέτα. Κατά την διάρκεια της DOS επίθεσης InviteFlood, ο SIP Server που δέχεται τον βομβαρδισμό αυτών των μηνυμάτων, αδυνατεί να εξυπηρετήσει τους χρήστες και να πραγματοποιήσει/δρομολογήσει κλήσεις. Όπως προαναφέρθηκε, τα INVITE πακέτα περιλαμβάνουν την φάση της αρχικοποίησης στην διαδικασία μια κλήσης. Συνεπώς αν αυτά τα πακέτα δεν είναι διαθέσιμα για αποστολή ή απορριφθούν από το σύστημα με κάποιο τρόπο, τότε το τερματικό δεν θα μπορεί να πραγματοποιήσει καμία κλήση. Η διαδικασία της φάσης INVITE, είναι επιρρεπής στην επίθεση flooding καθώς χρειάζεται κάποια δευτερόλεπτα για να ολοκληρωθεί και από τις πλευρές. Έτσι ο επιτιθέμενος στέλνει ένα καταιγισμό από παραμετροποιημένα και ψευδή INVITE πακέτα στον SIP server μέσα σε ένα πολύ σύντομο χρονικό διάστημα, κάνοντας έτσι μη διαθέσιμη την υπηρεσία καθώς οι πόροι του SIP server έχουν πλέον εξαντληθεί. Ο SIP server δεν μπορεί να διαχειριστεί όλα αυτά τα αιτήματα, υποβαθμίζοντας έτσι την ποιότητα των τρεχουσών υπηρεσιών, μέχρι αυτές να καταστούν μη διαθέσιμες για όλους.

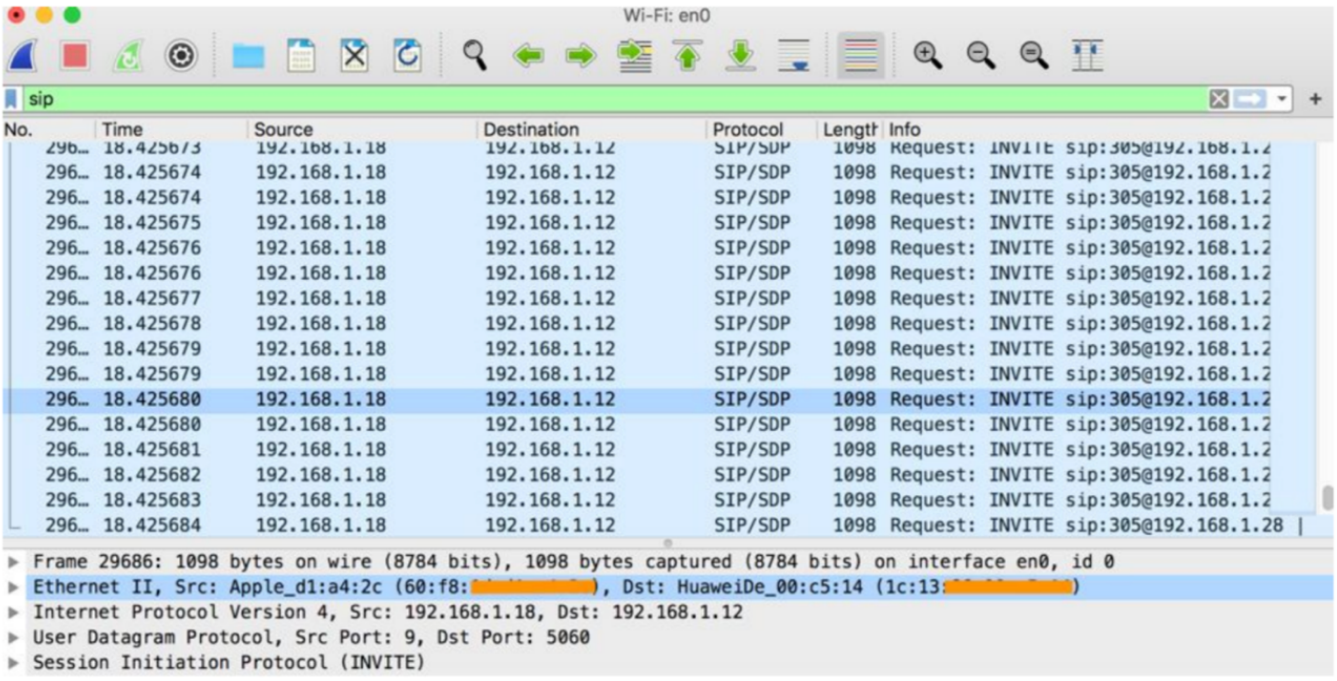
Με αυτό το τρόπο εξαπολύθηκε η επίθεση INVITE Flood ώστε να καταστήσουμε μη διαθέσιμη την VoIP υπηρεσία στα τερματικά των θυμάτων αλλά και με σκοπό να χρησιμοποιηθεί για τις επόμενες επιθέσεις.

Με βάση την αναγνώριση της υποδομής, που καταγράφηκε στο πρώτο μέρος από την οποία καταγράφηκαν οι User Agents (VoIP clients), χρησιμοποιήθηκε ένας τυχαίος αριθμός (extension) της λίστας, ώστε να πραγματοποιηθεί η επίθεση IVNITE Flood. Όπως φαίνεται και στην Εικόνα 21, παραμετροποιήθηκε η εντολή της επίθεσης αναλόγως ώστε να αναφέρεται ο SIP server, το τυχαίο extension που επιλέχθηκε, καθώς και ο αριθμός των πακέτων που θα σταλούν.

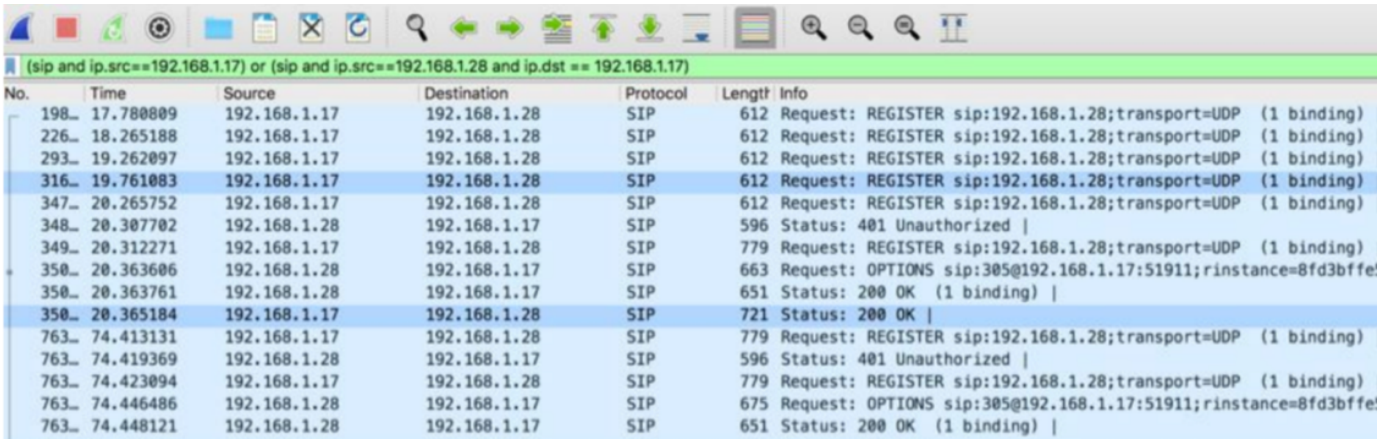
```
root@kali ~/inviteflood/inviteflood <kali/master*>
# sudo ./inviteflood eth0  305 192.168.1.28 192.168.1.12 700000

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 192.168.1.18:9
dest   IPv4 addr:port   = 192.168.1.12:5060
targeted UA             = 305@192.168.1.28

Flooding destination with 700000 packets
sent: 50319239
exiting...
```

Εικόνα 21: Invite flood

Καθώς το θύμα δεχόταν επίθεση, έγινε προσπάθεια σύνδεσης στον SIP server (REGISTER πακέτο) από ένα τυχαίο extension της λίστας μέσω ενός softphone, αλλά όπως φαίνεται στην Εικόνα 18 ο server απάντησε μη διαθέσιμος. Στις Εικόνες 22 και 23 φαίνονται τα INVITE πακέτα που στάλθηκαν από τον επιτιθέμενο, καθώς και την αδυναμία του θύματος να συνδεθεί στον Asterisk server.



Εικόνα 22: Invite flood πακέτα προς τον SIP server



Εικόνα 23: DoS attack στον SIP Server και το μήνυμα μη δυνατής σύνδεσης

4.5. Impersonation – Session Hijack

Συνεχίζοντας με την επόμενη επίθεση, όσο η επίθεση INVITE Flood είναι ακόμα ενεργή, ο επιτιθέμενος είναι ικανός να παραστήσει το θύμα και να παραπλανήσει τον καλούντα. Η επίθεση που χρησιμοποιήθηκε βασίζεται στους τύπους επιθέσεων impersonation και λέγεται Session hijacking.

Στην επίθεση Session hijacking που πραγματοποιήθηκε, ο επιτιθέμενος κατασκεύασε το δικό του REGISTER πακέτο ώστε να παραστήσει το θύμα, αλλάζοντας κάποιες παραμέτρους του REGISTER πακέτου, σπάζοντας ταυτόχρονα τον hashed κωδικό που έλαβε ως απάντηση από τον SIP server. Έτσι ο επιτιθέμενος είναι ικανός να μιμιθεί το θύμα, αφού πλέον είναι ικανός να βάλει το username, το οποίο το έχει από την αναγνώριση της υποδομής που πραγματοποιήθηκε στην πρώτη φάση της επίθεσης, και το password του User Agent που έσπασε μετά την απάντηση του SIP server στο πακέτο REGISTER.

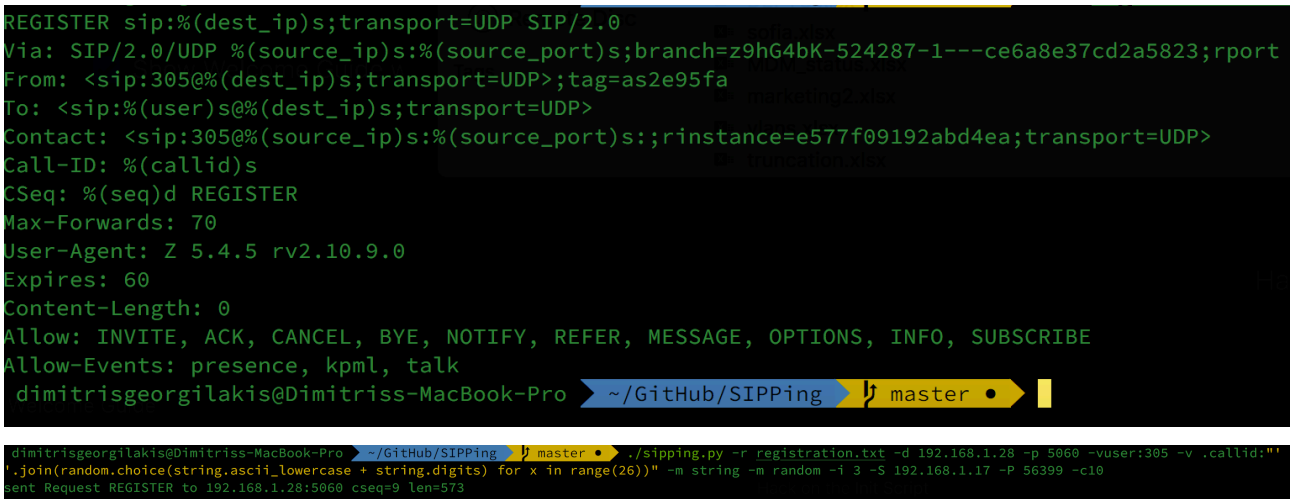
Κατόπιν μελέτης και ανάλυσης των SIP πακέτων σε μια SIP επικοινωνία μεταξύ δυο τερματικών, κατασκευάστηκε ένα μήνυμα SIP REGISTER με την βοήθεια ενός python script, το οποίο τροποποιήθηκε με σκοπό να μιμηθούμε το θύμα. Έτσι στέλνοντας το πρώτο τροποποιημένο REGISTER μήνυμα, αναλύθηκε η απάντηση του πακέτου από τον SIP server (με την βοήθεια του Wireshark). Έχοντας πλέον την απάντηση, η hash του κωδικού ήταν εμφανής κάτι το οποίο οδήγησε τον επιτιθέμενο να δοκιμάσει να σπάσει τον κωδικό με τον οποίο αυθεντικοποιείται το θύμα στον SIP server. Συνεπώς, βάζοντας τον κωδικό και το username στο softphone ο επιτιθέμενος κατάφερε επιτυχώς να αποτρέψει το θύμα να συνδεθεί στον server και να συνδεθεί αυτός με τα στοιχεία θύματος.

Παρακάτω αναλύονται τα βήματα της επίθεσης περιλαμβάνοντας τα πακέτα που απεστάλησαν μεταξύ επιτιθέμενου και SIP server.

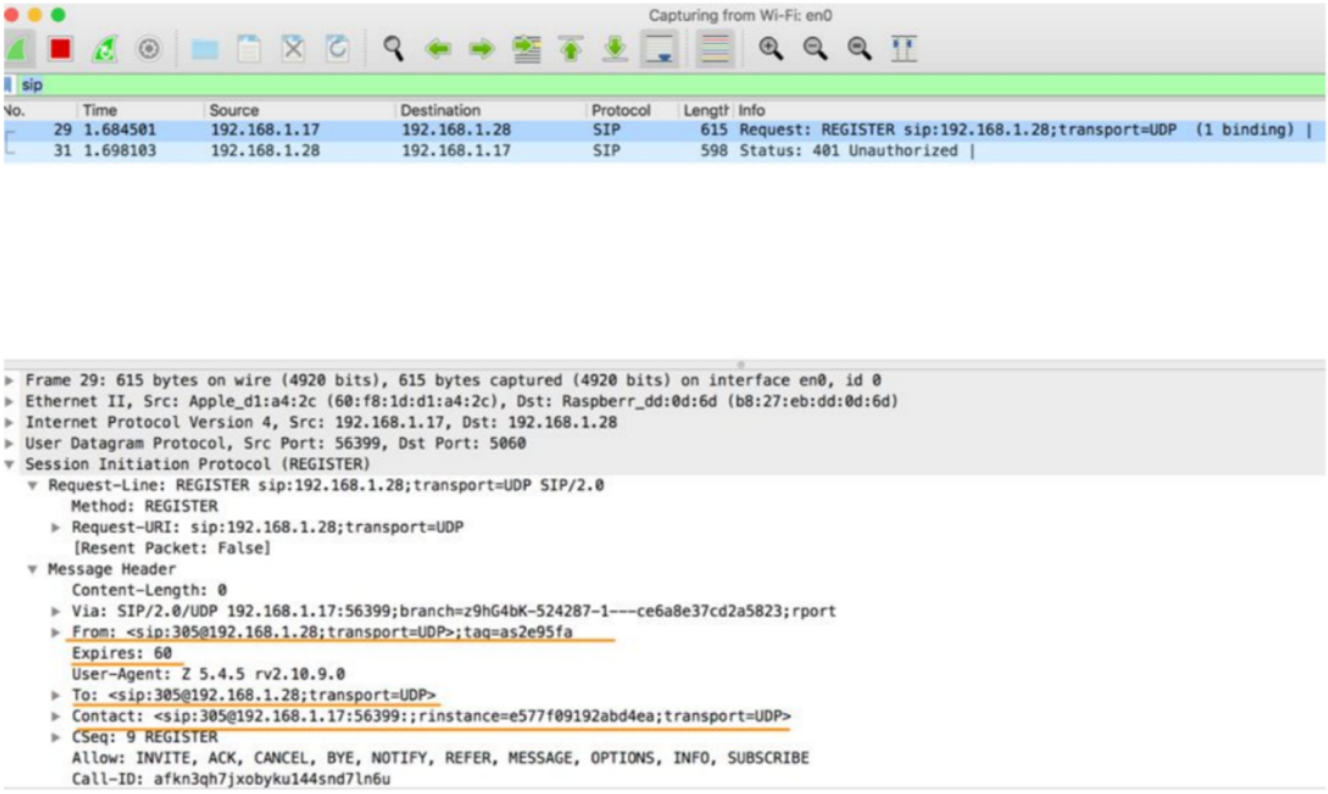
- **Βήμα 1ο:** Ξεκινάει η Dos επίθεση (InviteFlood) προς το θύμα με σκοπό να διακοπεί η σύνδεση του με τον SIP server.

- **Βήμα 2ο:** Όταν ο User Agent προσπαθεί να συνδεθεί σε εναν SIP server, ξεκινάει την διαδικασία της σύνδεσης στέλνοντας ένα registration μήνυμα (REGISTER). Το μήνυμα αυτό περιλαμβάνει τα πεδία “To” και “From” τα οποία υποδηλώνουν την ταυτότητα του User Agent και του SIP server αντίστοιχα, το πεδίο Expiration το οποίο δείχνει σε δευτερόλεπτα, τον χρόνο που θα διαρκέσει η φάση του Registration, το Call-id το οποίο αναγνωρίζει το γκρουπ των SIP μηνυμάτων και υπολογίζεται από μια τυχαία συμβολοσειρά μαζί με το όνομα ή την IP του User Agent. Τέλος το contact header το οποίο περιλαμβάνει το SIP URI το οποίο επιδεικνύει την διαδρομή για να επικοινωνήσει με τον User Agent.

Όπως φαίνεται και στην Εικόνα 24 ο επιτιθέμενος στέλνει το τροποποιημένο μήνυμα REGISTER αφού το κατασκευάσει, στον SIP server με περίοδο λήξης του πακέτου στα 60 δευτερόλεπτα, τα πεδία To/From 305@192.168.1.28 (305 είναι το extension του θύματος), και Contact value το 305@192.168.1.7, παριστάνοντας έτσι το θύμα.



Εικόνα 24: Wireshark capture του τροποποιημένου μηνύματος που εστάλη

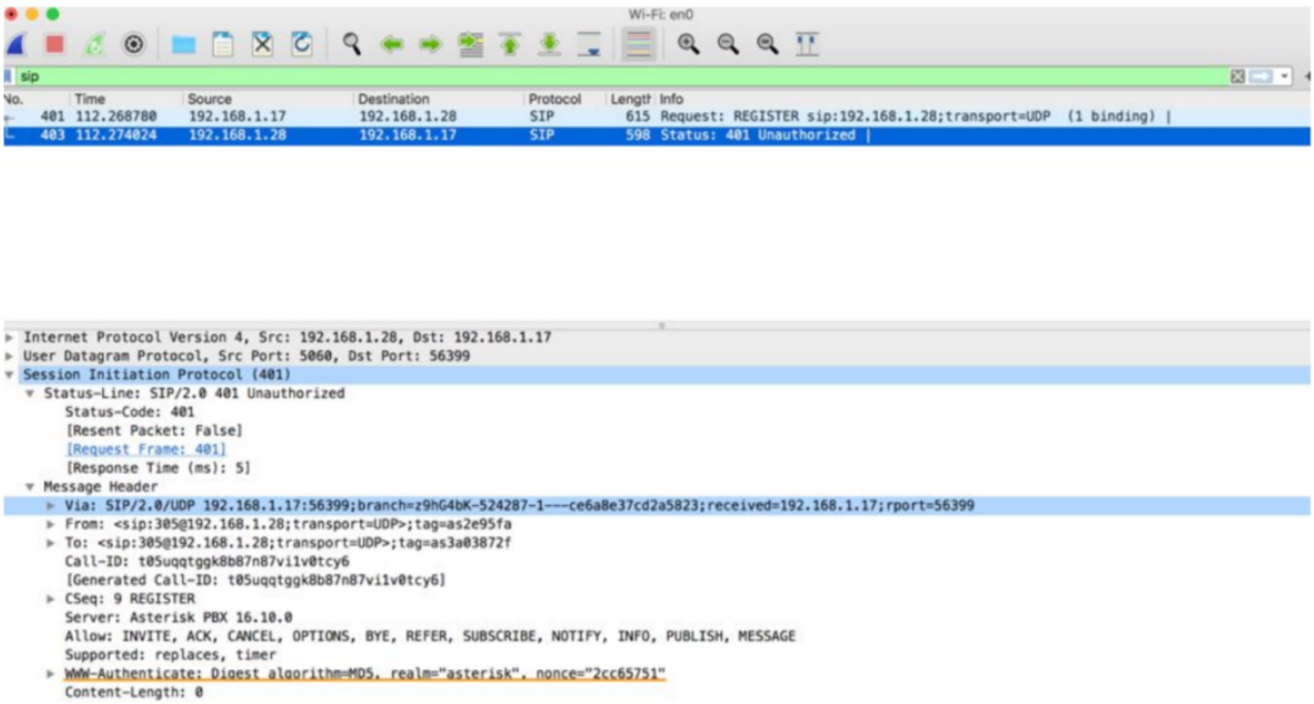


Εικόνα 25: Wireshark capture του μηνύματος Register που εστάλη

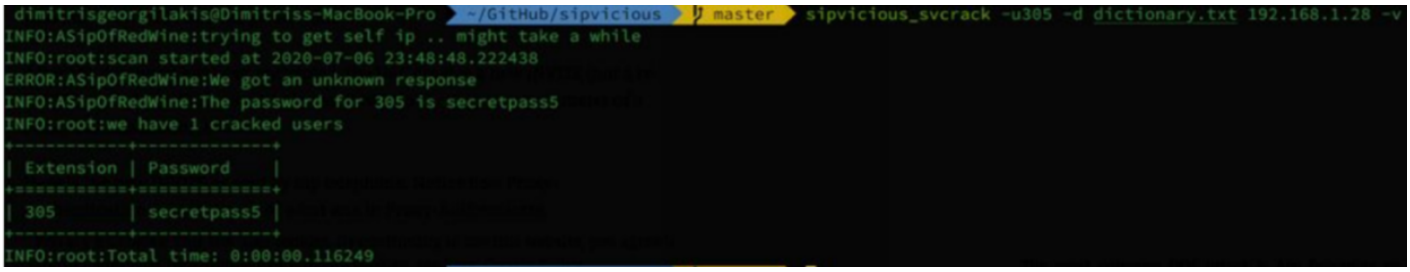
- **Βήμα 3ο:** Ο SIP server αφού παρέλαβε το τροποποιημένο μήνυμα, επιστρέφει στον επιτιθέμενο μήνυμα 401 Unauthorized, όπως φαίνεται στην παραπάνω Εικόνα 25. Η απάντηση δείχνει ότι ο User Agent πρέπει πρώτα να αυθεντικοποιηθεί στον Server, περιλαμβάνοντας όμως δεδομένα τα οποία θα χρησιμοποιηθούν ώστε να κρυπτογραφήσουν τον κωδικό του χρήστη. Περιλαμβάνουν ένα nonce μαζί με το όνομα του αλγορίθμου κρυπτογράφησης που θα χρησιμοποιηθεί.

Παρατηρείται ότι ο αλγόριθμος κρυπτογράφησης που στέλνει ο SIP server στο Unauthorized πακέτο, είναι ο MD5 (Εικόνα 26). Βασιζόμενοι σε αυτό μπορούμε να χρησιμοποιήσουμε την επόμενη μας επίθεση.

Η επίθεση βασίζεται στο πρόγραμμα svcrack το οποίο ανήκει στην σουίτα του sipvicious, με σκοπό να σπάσει ο κωδικός του θύματος. Το svcrack βασίζεται στην επίθεση λεξιλογίου (dictionary attack[12]). Διαβάζει ένα αρχείο με διάφορες συμβολοσειρές το οποίο παρέχεται από τον επιτιθέμενο μαζί με το extension number του θύματος με σκοπό να παράξει τον nonce αριθμό (από την απάντηση του SIP server) και τον κωδικό του θύματος βγάζοντας έτσι ένα MD5 hash ως αποτέλεσμα το οποίο στέλνεται στον SIP server.



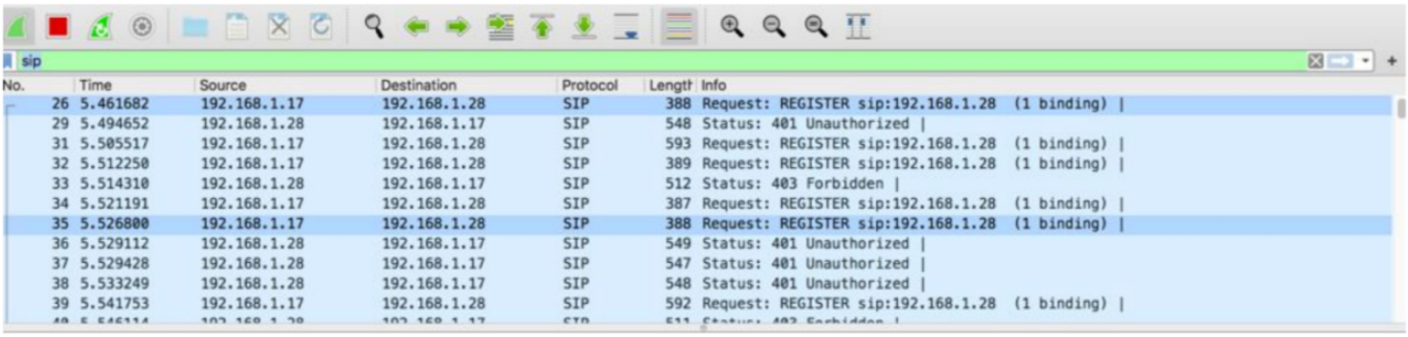
Εικόνα 26: Wireshark capture η απάντηση του SIP server



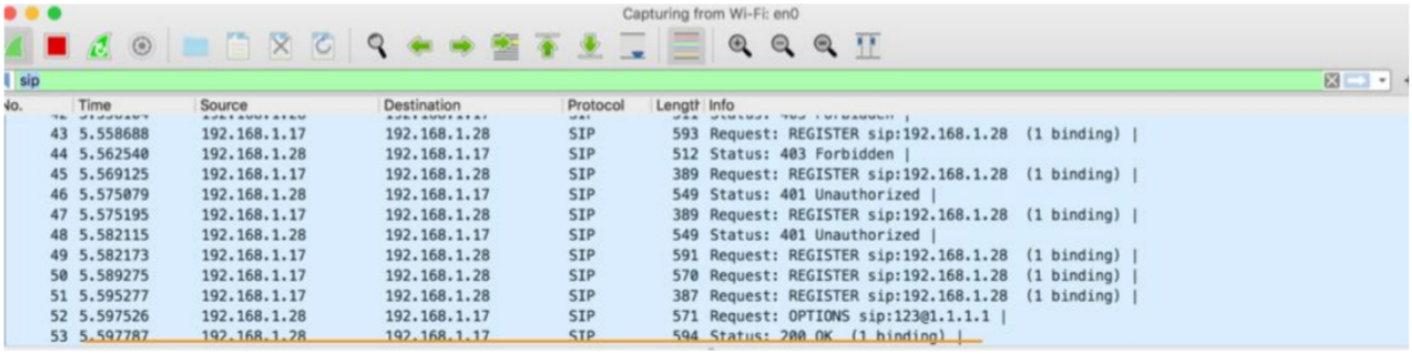
Εικόνα 27: Svcrack

Βήμα 4ο: Σε αυτή την φάση ο User Agent επιστρέφει το ίδιο μήνυμα REGISTRATION request αλλά αυτή τη φορά με το authorization header. Όπως φαίνεται και στην παραπάνω Εικόνα 27, το svcrack δοκίμασε όλους τους πιθανούς συνδυασμούς των κωδικών, που δόθηκαν από το αρχείο “dictionary.txt”, μετατρέποντας τους κωδικούς και στέλνοντας τους ως MD5 hashes στον server, μαζί με το extension number του θύματος. Μετά την ολοκλήρωση όλων των πιθανών συνδυασμών, η επίθεση ήταν επιτυχής αφού “’έσπασε” ο κωδικός του θύματος.

- **Βήμα 5ο:** Στέλνοντας πλέον το πακέτο REGISTER με τον σωστό κωδικό στον SIP server , λάβαμε απάντηση με κωδικό 200 OK, πράγμα που υποδηλώνει ότι επιτυχώς συνδεθήκαμε στον server με το extension του θύματος.



Εικόνα 28: Wireshark capture με τις δοκιμές του svcrack



Εικόνα 29: Wireshark capture από την επιτυχής σύνδεση στον SIP Server

4.6. Επίθεση σε STIR/SHAKEN υποδομή

Σε αυτήν την επίθεση δοκιμάσαμε να μιμηθούμε ένα άλλο τηλεφωνικό αριθμό (callee-ID spoof) και να δούμε πώς θα συμπεριφερθεί ο πάροχος και αν όντως έχει υλοποιήσει κάποια αρχιτεκτονική με SHIR/STAKEN. Η επίθεση έγινε σε δύο SIP παρόχους. Ο πρώτος πάροχος είναι SIP trunk provider και ο δεύτερος national telecommunications provider.

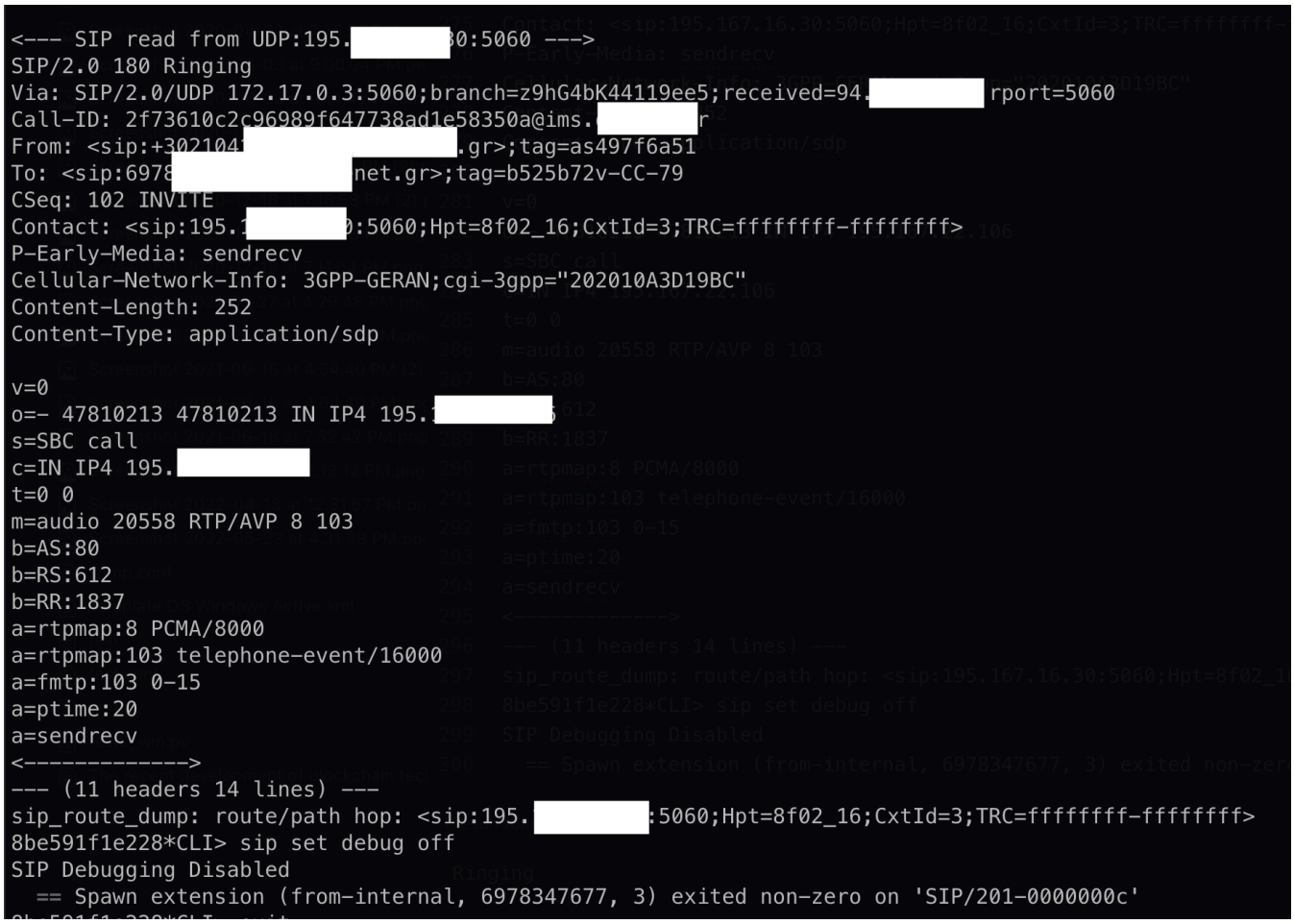
Στον πρώτο πάροχο ο επιτιθέμενος έστειλε ένα τροποποιημένο πακέτο, με σκοπό να αλλάξει τον τηλεφωνικό του αριθμό, προσποιώντας πως είναι κάποιος άλλος.

Έτσι φτιάχτηκε ένα πακέτο SIP, το οποίο περιελάβανε στο invite πακέτο έναν αριθμό τυχαίο σαν caller-ID. Το αποτέλεσμα ήταν ο πάροχος να μας επιτρέψει την κλήση και να αποστείλει την κλήση με τον ψεύτικο αριθμό στο θύμα. Στην παρακάτω εικόνα όπως θα δείτε ο πάροχος έστειλε τον αριθμό +4355657645 ως caller-ID, μέσα από το τροποποιημένο πακέτο και η κλήση έφτασε στον καλούντα, χωρίς πρόβλημα.

```
<--- SIP read from UDP:109.233.115.107:5060 --->
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 172.17.0.3:5060;rport=5060;received=94.70.61.23;branch=z9hG4bK7aae5e57
Record-Route: <sip:109.233.115.107;lr;ftag=as6d3b58fc;did=705.8ca7e776>
From: <sip:+4355657645@172.17.0.3>;tag=as6d3b58fc
To: <sip:+306978[redacted]@eu.st.ssl7.net>;tag=as2b7ab35a
Call-ID: 3059067908baad6f30435830558e0b83@172.17.0.3:5060
CSeq: 103 INVITE
Server: Media GW uk027
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces
Contact: <sip:306978[redacted]@134.19.166.167:5060>
Content-Type: application/sdp
Content-Length: 412

v=0
o=root 1649230425 1649230425 IN IP4 134.19.166.167
s=Media GW uk027
c=IN IP4 134.19.166.167
t=0 0
m=audio 10946 RTP/AVP 8 0 3 4 111 110 101
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:4 G723/8000
a=fmtp:4 annexa=no
a=rtpmap:111 G726-32/8000
a=rtpmap:110 speex/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=silenceSupp:off - - - -
a=ptime:20
a=sendrecv
<-------------->
--- (13 headers 18 lines) ---
sip_route_dump: route/path hop: <sip:109.233.115.107;lr;ftag=as6d3b58fc;did=705.8ca7e776>
Found RTP audio format 8
Found RTP audio format 0
Found RTP audio format 3
Found RTP audio format 4
Found RTP audio format 111
Found RTP audio format 110
Found RTP audio format 101
Found audio description format PCMA for ID 8
Found audio description format PCMU for ID 0
Found audio description format GSM for ID 3
Found audio description format G723 for ID 4
Found audio description format G726-32 for ID 111
Found audio description format speex for ID 110
Found audio description format telephone-event for ID 101
Capabilities: us - (alaw|ulaw|gsm|g723|g726|speex), peer - audio=(ulaw|gsm|g723|alaw|speex|g726)/video=(nothing)/text=(nothing),
Non-codec capabilities (dtmf): us - 0x1 (telephone-event|), peer - 0x1 (telephone-event|), combined - 0x1 (telephone-event|)
Peer audio RTP is at port 134.19.166.167:10946
Really destroying SIP dialog 'c7a525c4-2d4a3477-93c656@109.233.115.107' Method: OPTIONS

<--- SIP read from UDP:109.233.115.107:5060 --->
OPTIONS sip:s@192.168.1.100:5060 SIP/2.0
Via: SIP/2.0/UDP 109.233.115.107:5060;branch=z9hG4bK837a3477
From: sip:keepalive@109.233.115.107;tag=9df48a51
To: sip:s@192.168.1.100:5060
Call-ID: c7a525c4-837a3477-16c656@109.233.115.107
CSeq: 1 OPTIONS
Max-Forwards: 70
```

Εικόνα 30: Crafted SIP Invite packet, πάροχος 1

Στην περίπτωση του 2ου παρόχου, η επίθεση μας ήταν μερικώς επιτυχής. Αυτό σημαίνει πως θέσαμε σαν caller-ID έναν άλλο τυχαίο αριθμό, αλλά αυτή τη φορά ο αριθμός που φάνηκε στο θύμα ήταν ο πραγματικός αριθμός του συνδρομητή. Παρόλα αυτά παρατηρούμε από την παρακάτω Εικόνα 31, πως ο η κλήση ολοκληρώθηκε επιτυχώς, χωρίς ο πάροχος να μπλοκάρει την επικοινωνία.



Εικόνα 31: Crafted SIP Invite packet, πάροχος 2

Παρατηρούμε λοιπόν αν και οι δύο πάροχοι είχαν υλοποιήσει το STIR/SHAKEN πρωτόκολλο καμία κλήση δεν θα είχε ολοκληρωθεί και το θύμα δεν θα είχε ξεγελαστεί.

5. VoLTE

5.1. Εισαγωγή

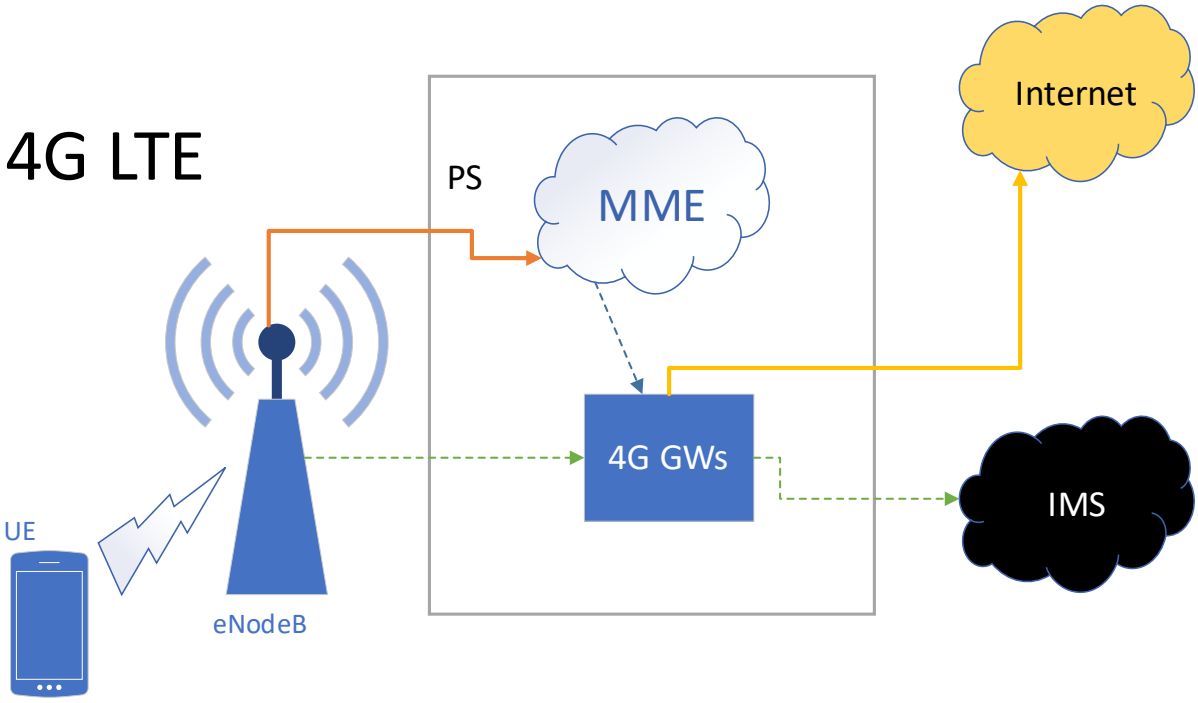
Η μετάβαση της τεχνολογίας σε υπηρεσίες cloud και η ανάγκη για άμεση και γρήγορη πρόσβαση σε αυτές, αναγκάζει τους παρόχους κινητής αλλά και επίγειας επικοινωνίας να εξελίξουν τις τεχνολογίες τους με σκοπό να εξυπηρετήσουν την νέα αυτή τάση. Έτσι, οι εταιρίες κινητής εξέλιξαν την τεχνολογία 3G μεταβαίνοντας στην τεχνολογία 4G, προσφέροντας έτσι μεταξύ άλλων, υψηλές ταχύτητες με το δίκτυο LTE (Long Term Evolution). Η τεχνολογία LTE λειτουργεί πάνω από την υποδομή των packet switch δικτύων, αλλάζοντας έτσι τον τρόπο που λειτουργεί η υπηρεσία φωνής και μηνυμάτων.

Η τεχνολογία VoLTE (Voice over LTE) που πρωτοεμφανίστηκε στην Νότια Κορέα το 2012, είναι η καθορισμένη λύση φωνής στην τεχνολογία δικτύου LTE. Αναδιαμορφώνει όλες τις υπηρεσίες τηλεφωνίας από την τεχνολογία circuit-switched, στην τεχνολογία packet switched εξελίσσοντας έτσι το 4G δίκτυο κινητής επικοινωνίας.

Το VoLTE είναι μια λύση που λειτουργεί σε δίκτυα LTE ενώ βασίζεται στην τεχνολογία VoIP, εν αντιθέσει με τις τεχνολογίες 2G/3G που βασίζονταν στα παραδοσιακά circuit-switched δίκτυα. Η αρχιτεκτονική δομή της υπηρεσίας VoLTE είναι συγκεκριμένη. Περνάει πακέτα φωνής μέσα από το IP δίκτυο ενώ είναι παραμετροποιημένο σύμφωνα με τις απαιτήσεις και τις ανάγκες ενός κινητού δικτύου, όπως high-prioritization of packets βάση δικτύου, QoS (Quality of service), προσαρμογή υπηρεσιών σύμφωνα με την ισχύ και την διαθεσιμότητα του δικτύου. Σε αντίθεση με τις παλιότερες τεχνολογίες κινητής επικοινωνίας 2G/3G το VoLTE προσφέρει καλύτερη ποιότητα φωνής (HD audio), περισσότερες επιλογές όπως video calling, συνεδρίαση και τηλεφωνητή) καθώς και μεγαλύτερη διαλειτουργικότητα μεταξύ άλλων δικτυακών υπηρεσιών όπως Wi-Fi.

5.2. Υποδομή και πρωτόκολλα

Ένα κινητό δίκτυο αποτελείται από δύο στοιχεία: το ασύρματο δίκτυο (radio access network) στο οποίο το τερματικό του χρήστη αποκτά πρόσβαση, μέσω των κεραιών, στο δίκτυο του παρόχου και το δίκτυο πυρήνα (core network) μέσω του οποίου επικοινωνεί το access network με όλη την υποδομή του παρόχου για να πραγματοποιήσει κλήσεις ή να δώσει στον χρήστη, πρόσβαση στο διαδίκτυο. Επιπλέον στα δίκτυα 4G, όπως προαναφέραμε, είναι δίκτυα packet-switched το οποίο σημαίνει πως δεν χρησιμοποιούν πλέον τηλεφωνία PSTN, αλλά διασυνδέονται στον IMS server, με σκοπό να προσφέρουν υπηρεσία φωνής, μέσω της τεχνολογίας VoIP. Φυσικά σε περιπτώσεις που η δυνατότητα χρήσης της τεχνολογίας VoLTE δεν είναι εφικτή, το δίκτυο LTE μπορεί να προσφέρει στον συνδρομητή, την 3G τεχνολογία φωνής, περνώντας τις κλήσεις από το LTE προς το 2G/3G δίκτυο (circuit-switched δίκτυα), δρομολογώντας τα πακέτα μέσα από το core δίκτυο του παρόχου με τους αντίστοιχους δρομολογητές για τις αντίστοιχες υπηρεσίες.



Εικόνα 32: 4G Architecture

Το access δίκτυο 4G, όπως φαίνεται και στην Εικόνα 30, απαρτίζεται από τα εξής μέρη:

- eNodeB: Γνωστό και ως Evolved Nodeb, ονομάζεται ο σταθμός βάσης στα 4G δίκτυα της E-UTRAN τεχνολογίας. Είναι η εξέλιξη του στοιχείου Node B που εντοπίζεται στα 3G δίκτυα. Ο σταθμός βάσης είναι ο συνδετικός κρίκος ώστε η κινητή συσκευή του χρήστη, να αποκτήσει ασύρματη πρόσβαση στο δίκτυο του παρόχου. Εν αντιθέσει με το δίκτυο 3G, ο σταθμός βάσης των 4G δεν χρειάζεται κάποιο μηχανισμό ώστε να ελέγχεται ή να διοικείται για διαδικασίες ελέγχου εντοπισμού, ελέγχου παρεμβολών, διαθεσιμότητα πόρων κλπ. Οι κεραίες eNodeB είναι αυτόνομες και δεν χρειάζονται μηχανισμούς ελέγχου RNC.

- E-UTRAN (Evolved Universal Terrestrial Radio Access Network): Είναι η ασύρματη τεχνολογία που διαχειρίζεται την διασύνδεση ενός τερματικού κινητής επικοινωνίας (User Equipment) με το core δίκτυο LTE. Προσφέρει γρήγορες ταχύτητες με χαμηλό latency και είναι η αντικατάσταση των UMTS και HSDPA δικτύων

Το core δίκτυο (EPC) απαρτίζεται από:

- HSS (Home Subscriber Server): Η κεντρική βάση όπου περιλαμβάνει όλες τις πληροφορίες για τους χρήστες και συνδρομητές του παρόχου. Επιπλέον προσφέρει λειτουργίες για αρχικοποίηση κλήσης, αυθεντικοποίησης του συνδρομητή, πρόσβαση σε υπηρεσίες κ.α.

- PDN - Gateway (Packet Data Network -Gateway): P-GW είναι ο συνδετικός κρίκος των τερματικών των συνδρομητών με τον κόσμο του διαδικτύου.

- Serving Gateway (S-GW): είναι ο δρομολογητής του core δικτύου που προωθεί τα IP πακέτα από το access δίκτυο στο PDN-Gateway.

- MME (Mobility Management Entity): Ελέγχει το control plane του E-UTRAN δικτύου. Λειτουργίες όπως κρυπτογράφηση της επικοινωνίας μεταξύ UE και κεραίας, αποστολή κλήσης και σηματοδοσίας μεταξύ τερματικού-κεραίας (αφου συνδεθεί στον HSS) αλλά και μεταξύ των κεραιών eNodeBs και EPC, είναι στις αρμοδιότητες του.

Το IMS δίκτυο απαρτίζεται από:

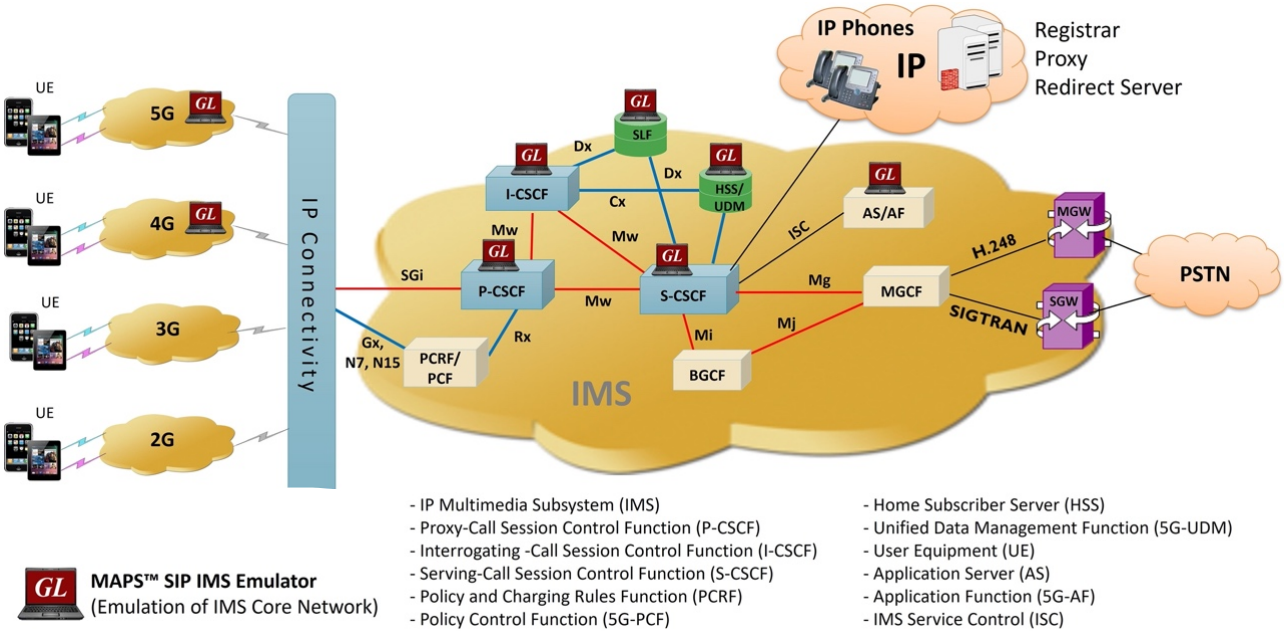
- P-CSCF (Proxy Call Session Control Function): Είναι ο διαμεσολαβητής μεταξύ χρήστη και IMS και το πρώτο σημείο επικοινωνίας των χρηστών με το IMS δίκτυο. Σε αυτό το σημείο ο συγκεκριμένος proxy δέχεται τα αιτήματα από τα τερματικά των συνδρομητών και τα προωθεί στην ανάλογη οντότητα ώστε να τα επεξεργαστεί και να τα εξυπηρετήσει. Συνήθως τα αιτήματα που δέχεται ο proxy είναι η αρχικοποίηση μιας εγγραφής στο δίκτυο IMS ή μια πρόσκληση για μια συνεδρίαση. Επιπλέον όντας το πρώτο σημείο επικοινωνίας των χρηστών, είναι υπεύθυνος να αναλαμβάνει την εγκαθίδρυση της ασφάλειας επικοινωνίας μεταξύ του τερματικού και του IMS, την συμπίεση της σηματοδοσίας, την διαχείριση για κλήσεις ανάγκης και εξουσιοδότησης για πολιτικές ορθής χρήσης.

- I-CSCF (Interrogating Call Session Control Function): Είναι η οντότητα που είναι υπεύθυνη για να καθορίζει ποια λειτουργία CSCF θα πρέπει να εκχωρηθεί για την διαχείριση του αιτήματος του UE. Το αίτημα αυτό έρχεται είτε από το εσωτερικό δίκτυο του παρόχου, ή από roaming υπηρεσία του συνδρομητή.

- S-CSCF (Serving Call Session Control Function): Είναι υπεύθυνο για την διαχείριση των διαδικασιών εγγραφής των UEs, των δρομολογήσεων και της αποθήκευσης των service profiles. Αποφασίζει αν θα τερματίσει την παροχή υπηρεσίας στον συνδρομητή καθώς και να αποστέλλει τις πληροφορίες διεύθυνσης του UE στον HSS.

- MGW (Media Gateway): Είναι η οντότητα που μετατρέπει τα πακέτα RTP σε αναλογικό σήμα ώστε να μπορούν να υποστηριχτούν από τα δίκτυα 2G/3G.

- SGW (Signaling Gateway): Είναι η οντότητα που μεταφέρει και μετατρέπει μηνύματα σήματος μεταξύ διαφορετικών δικτύων σε διαφορετικά μορφές, πχ σήματα από PSTN σε πακέτα IP.



Εικόνα 33: 4G IMS Architecture[13]

Όπως προαναφέραμε όταν το τερματικό του χρήστη συνδεθεί στο E-UTRAN δίκτυο, οι δρομολογητές μεταφέρουν το REGISTER request στον IMS server. Με την αρχικοποίηση του μηνύματος αυτού δημιουργείται και ο πρώτος φορέας για την σηματοδοσία μεταξύ χρήστη και LTE δικτύου. Το UE στέλνει το SIP REGISTER πακέτο και φτάνει στον P-CSCF δρομολογητή ο οποίος με την σειρά του απαντά με τις κατάλληλες παραμέτρους για την αρχικοποίηση της κλήσης, όπως τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί. Το τερματικό στέλνει τις παραμέτρους πίσω καθώς και το hash των παραμέτρων nonce, username και password (όπως έχουμε προαναφέρει), ώστε να αυθεντικοποιηθεί. Αν λάβει ως απάντηση από τον IMS OK, τότε έχει αυθεντικοποιηθεί και είναι έτοιμος για την πραγματοποίηση της κλήσης.

Η σημαντικότερη διαφορά μεταξύ των UTRAN (3G) και E-UTRAN δικτύων είναι ο τρόπος που μεταφέρουν τα δεδομένα στο core δίκτυο τους. Στα 3G δίκτυα τα δεδομένα χωρίζονται σε δεδομένα φωνής, τα οποία δρομολογούνται από το MSC (Mobile Switching Center) στα δίκτυα circuit switched, ώστε να χρησιμοποιηθεί η PSTN τηλεφωνία για την πραγματοποίηση της κλήσης, αλλά και σε packet switching δίκτυα, ώστε να δώσουν πρόσβαση στο διαδίκτυο όταν ο χρήστης το ζητήσει.

Στο LTE (4G) δίκτυο τα δίκτυα circuit switched δεν υφίστανται πλέον καθώς η φωνή χρησιμοποιεί τη τεχνολογία VoIP για την πραγματοποίηση της κλήσης και πιο συγκεκριμένα την τεχνολογία VoLTE. Ο χρήστης μάλιστα μπορεί να χρησιμοποιεί ταυτόχρονα μια σύνδεση στο σύνδεση στο Ίντερνετ, ενώ ταυτόχρονα μιλάει, κάτι το οποίο μέχρι τα δίκτυα 3G ήταν αδύνατο. Αξίζει να σημειωθεί πως τα δίκτυα 4G δίνουν την επιλογή της υποβάθμισης σε 3G όταν η υπηρεσίες τους (πχ VoLTE), δεν είναι διαθέσιμες (Circuit Switching FallBack)

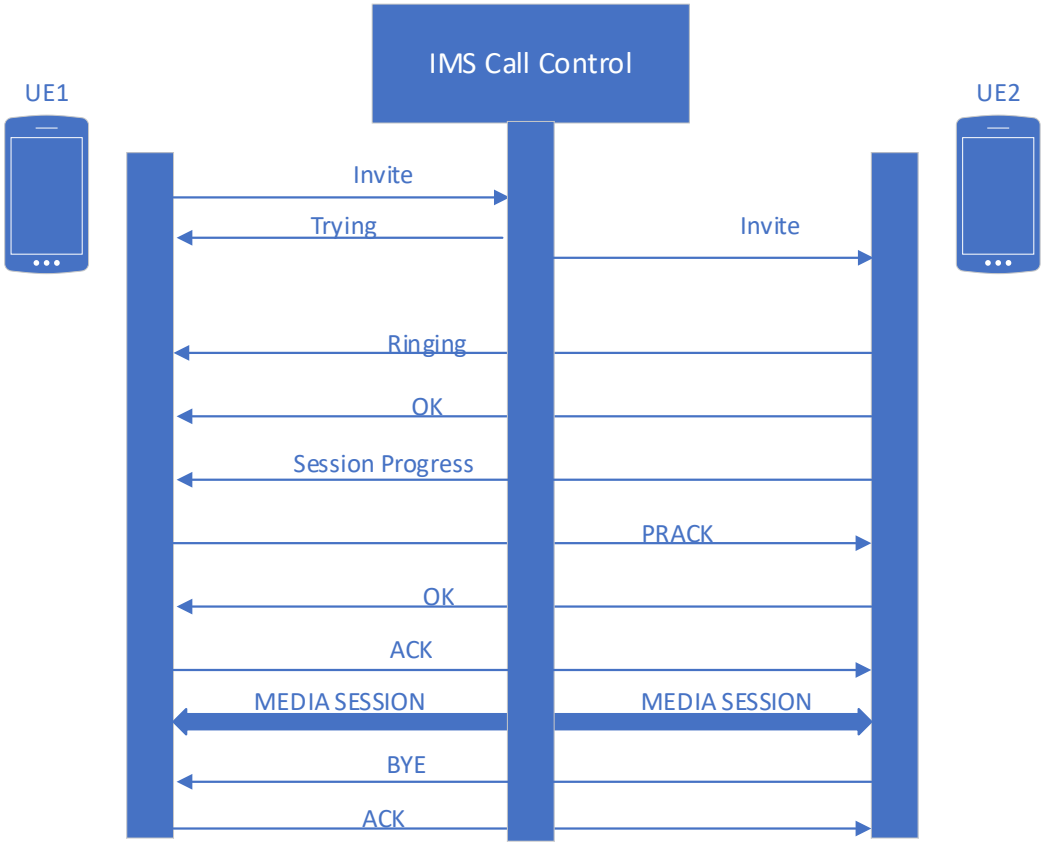
5.3. VoLTE Service

Το VoLTE είναι η υπηρεσία φωνής που παρέχεται στο δίκτυο LTE βασιζόμενη στην τεχνολογία VoIP. Χρησιμοποιεί τα ίδια πρωτόκολλα με το VoIP (τα αναλύσαμε πιο πάνω) όπως SIP, SDP, RTP προσαρμοσμένα στο δίκτυο της κινητής. Ο χρήστης συνδέεται στην κεραία eNodeB, έχοντας έτσι πρόσβαση σε όλο το EPS (Evolved Packet System). Μόλις το UE συνδεθεί στο δίκτυο, προσπαθεί να συνδεθεί στον IMS ώστε να τον αυθεντικοποιήσει.

Ύστερα όταν το τερματικό (UE) αυθεντικοποιηθεί οι κλήσεις δρομολογούνται μέσω του CSCF (Call Session Control Function) και ένας αποκλειστικός φορέας (εικονικό κανάλι) δημιουργείται όταν εγκαθιδρύεται μια κλήση, ώστε να αναγνωρίζει τα πακέτα φωνής και να τα δρομολογεί. Αξίζει να σημειωθεί πως δημιουργούνται 2 φορείς κατά την χρήση της υπηρεσίας VoLTE. Ο πρώτος φορέας και ο πιο σημαντικός αφορά την σηματοδοσία της τηλεφωνίας. Για αυτόν το λόγο έχει και την μεγαλύτερη προτεραιότητα στην ανταλλαγή πακέτων, ώστε να δουλέψει αναίμακτα ακόμα και αν οι πόροι της κεραίας έχουν ελαττωθεί. Επίσης δημιουργείται άλλος ένα φορέας όταν ξεκινάει μια τηλεφωνική επικοινωνία ο οποίος έχει μεγαλύτερη προτεραιότητα στα πακέτα από τα πακέτα δεδομένων (Ίντερνετ) αλλά χαμηλότερη από του πρώτου φορέα. Τέλος, η διαδικασία της κλήσης στην υπηρεσία VoLTE είναι σχεδόν ίδια όπως ακριβώς και σε μια κλήση VoIP.

- Ο καλών στέλνει ένα πακέτο INVITE στον SIP Server στο IMS δίκτυο, περιλαμβάνοντας τον τηλεφωνικό του αριθμό, την IP διεύθυνση καθώς και άλλες παραμέτρους.
- Ο SIP Server αφού επιβεβαιώσει ότι το μήνυμα είναι σωστό απαντάει στον καλών με το μήνυμα TRYING, και εκείνος προωθεί το πακέτο στον καλούντα, με μήνυμα RINGING .

- Αν ο καλούντας δεχτεί την κλήση, στέλνει ένα OK μήνυμα στον SIP Server ο οποίος και δρομολογεί την κλήση στον καλών, ενώ ξεκινάει την χρέωση της συνομιλίας. Όλη η συνομιλία βασίζεται στα RTP πακέτα.
- Για να τερματιστεί η κλήση, αρκεί ένας από τους 2 να στείλει το μήνυμα BYE



Εικόνα 34: VoLTE call flow

5.4. Επιθέσεις και ανάλυση στο VoLTE

Αρκετές έρευνες έχουν διεξαχθεί ώστε να δοκιμάσουν την τεχνολογία VoLTE και τυχόν αδυναμίες. Κατά την διάρκεια της διπλωματικής δεν υπήρχε διαθέσιμο κάποιο kit ώστε να προχωρήσουμε με διάφορες δοκιμές, οπότε θα βασιστούμε σε διάφορες έρευνες που έχουν δοκιμάσει την ασφάλεια του VoLTE.

5.4.1. Αποκρυπτογράφηση της επικοινωνίας μεταξύ UE και IMS

Αυτή η επίθεση, η οποία έχει πραγματοποιηθεί στην έρευνα [1] όπως μας αναφέρει ο ερευνητής, κατάφερε και αποκρυπτογράφησε τα πακέτα μεταξύ UE και IMS χρησιμοποιώντας το module Simtrace πάνω στην SIM. Παρόλα αυτά, κάτι τέτοιο δεν θα μπορούσε να γίνει μέσω της επίθεσης Man-in-the-Middle. Μέσω του module Simtrace η επίθεση πραγματοποιήθηκε έχοντας πρόσβαση πάνω στο τερματικό του θύματος και πιο συγκεκριμένα πάνω στην SIM, στέλνοντας έτσι όλα τα πακέτα σε ένα άλλο τερματικό (redirected packets) με σκοπό την αποκρυπτογράφηση των κλειδιών, που παρήχθησαν από το ISIM module της SIM. Η ISIM (IP Multimedia Services Identity Module) είναι ένα application που λειτουργεί στην SIM κάρτα με σκοπό την αποθήκευση των δεδομένων που αφορούν την διασύνδεση του UE με τον IMS server του παρόχου. Έτσι παρατηρήθηκε πως κατά την διάρκεια του IKEv2 τα πακέτα που στάλθηκαν περιλάμβαναν λεπτομέρειες για την παραγωγή των IPSec κλειδιών. Καθώς τα κλειδιά παράγονται στην ISIM και έπειτα στέλνονται στον πυρήνα του λειτουργικού για να σταλθούν, βάζοντας το Simtrace ενδιάμεσα, κατάφεραν και αποκρυπτογράφησαν τα κλειδιά κάνοντας πλέον την επικοινωνία μη ασφαλή.

5.4.2. Διαρροή του IMEI

Παρατηρήθηκε ότι το IMEI, ένας 15ψήφιος μοναδικός αριθμός για κάθε κινητή συσκευή, περιλαμβάνετε στο πεδίο Contact των SIP μηνυμάτων. Οι ερευνητές του [1] κατάφεραν και βρήκαν το IMEI μέσα από μια απλή κλήση ενός συνδρομητή, αφού πρώτα είχαν πρόσβαση στο κινητό του. Έτσι αν το IMEI καταφέρει και πέσει στα χέρια κάποιου κακόβουλου χρήστη μπορεί να το χρησιμοποιήσει ώστε να:

- Αναφέρει τη κινητή συσκευή ως κλεμμένη και να μπλοκάρει ο πάροχος ή ο κατασκευαστής, την συσκευή.
- Να μιμηθεί τον χρήστη από άλλο τερματικό κάνοντας έτσι κακόβουλες κλήσεις
- Αν συνδυαστεί με άλλα μέρη του κινητού, όπως πχ Wireless MAC address ο κακόβουλος χρήστης θα μπορεί να εντοπίζει τον χρήστη πιο εύκολα, ή να παίρνει πληροφορίες για το κινητό.

5.4.3. Χρήση του VoLTE για δωρεάν χρήση Data

Ο πάροχος όπως αναφέραμε έχει ένα φορέα μόνο για σηματοδοσία προς το UE. Αυτό προσφέρεται δωρεάν. Έτσι, όλη η κίνηση των πακέτων σηματοδοσίας δεν περνά από τον AAA server ή κάποια άλλη οντότητα με σκοπό την καταγραφή για χρέωση. Αντιθέτως τα δεδομένα φωνής, περνάνε από άλλο φορέα και έτσι η χρέωση είναι υποχρεωτική. Παρατηρήθηκε πως κάποια μηνύματα όπως το SIP-INVITE ή ακόμα και το RINGING περνάνε μέσα από τον φορέα σηματοδοσίας. Έτσι οι ερευνητές του [2] δοκίμασαν για 10 ώρες να βομβαρδίζουν με μη ολοκληρωμένες κλήσεις ένα άλλο τερματικό κινητής (χωρίς να απαντάει ο καλών) για δέκα ώρες. Ένα μέγεθος της τάξης των 42 MB παράχθηκε. Επιπλέον, παρατήρησαν ότι το interface του VoLTE είναι εύκολα προσβάσιμο από κάποιο μη εξουσιοδοτημένο χρήστη. Έτσι βρήκαν την ip του server σηματοδοσίας του παρόχου, μέσα από το routing table της κινητής συσκευής (/*proc/net/ipv6_route*) και προχώρησαν σε αποστολή αρκετών ICMP pings προς αυτόν. Οι απαντήσεις ήρθαν κανονικά χωρίς να υπάρχει κάποια χρέωση.

6. VoWiFI

6.1. Εισαγωγή

Το VoWiFi (Voice over WiFi ή WiFi calling) είναι η τεχνολογία που επιτρέπει στον χρήστη της κινητής τηλεφωνίας, να μεταφέρει δεδομένα φωνής στον IMS server του παρόχου, μέσω της σύνδεσης του σε οποιοδήποτε WiFi, χρησιμοποιώντας στην πραγματικότητα την τεχνολογία VoIP. Ο χρήστης μπορεί να πραγματοποιεί και να δέχεται κλήσεις ή μηνύματα στον αριθμό της κινητής του σύνδεσης, μέσα από οποιοδήποτε WiFi δίκτυο στο οποίο έχει πρόσβαση, χωρίς να χρειάζεται την σύνδεση σε κάποια κεραία κινητής. Επιπλέον, είναι μια πολύ καλή λύση για τους συνδρομητές που η ποιότητα της σύνδεσης μεταξύ τερματικού και κεραίας κινητής, δεν είναι ικανοποιητική.

6.2. Αρχιτεκτονική δομή και πρωτόκολλα

Η υπηρεσία VoWiFi είναι διαθέσιμη πλέον παγκοσμίως από όλους τους παρόχους και το μόνο που χρειάζεται ο χρήστης είναι αφού έχει ενεργοποιήσει την υπηρεσία, να συνδεθεί σε οποιοδήποτε δίκτυο WiFi με πρόσβαση στο Ίντερνετ.

Το τερματικό του χρήστη θα κάνει την σύνδεση στο WiFi, με σκοπό να συνδεθεί στο IMS δίκτυο του παρόχου, μέσω του διαδικτύου. Για να ολοκληρωθεί όμως η σύνδεση στο IMS δίκτυο, οι TWAG και ePDG είναι οι οντότητες που θα φέρουν σε επικοινωνία το WLAN δίκτυο του πελάτη με το EPC δίκτυο του παρόχου. Η P-GW που βρίσκεται στο EPC δίκτυο, είναι ο κοινός διαμεσολαβητής για τις συνεδρίες των συνδρομητών είτε το τερματικό κάνει χρήση της VoWiFi υπηρεσίας είτε της VoLTE, προς τον IMS server.

3GPP Access (3rd Generation Partnership Project)

Το 3GPP είναι μια κοινοπραξία πολλών παγκόσμιων εταιριών που σκοπό έχει την ανάπτυξη πρωτοκόλλων κινητών επικοινωνιών. Έτσι το 3GPP υποστηρίζει multi-type access. Σκοπός είναι να προσφέρει ένα «μονοπύρηνο» δίκτυο το οποίο θα αποτελείται από πολλές τεχνολογίες όπως 2G, 3G, 4G οι οποίες θα αλληλοεπιδρούν μεταξύ τους.

Non-3GPP Access

Τα δίκτυα non-3GGP είναι τα δίκτυα τα οποία δεν έχουν οριστεί στο 3GPP. Τα δίκτυα αυτά, είναι τεχνολογίες όπως WLAN, WiMAX, CDMA2000, Fixed Networks, τα οποία μπορούν και αλληλοεπιδρούν με το EPC δίκτυο του παρόχου.
Τα non-3GPP Access δίκτυα χωρίζονται σε Trusted και Untrusted Access.

Trusted Access

Όπως μαρτυρά και το όνομα τους τα δίκτυα αυτά έχουν οριστεί ως έμπιστα δίκτυα και έτσι μπορούν να επικοινωνούν απευθείας με το EPC δίκτυο μέσω του TWAG, ακόμα και με λιγότερη ασφάλεια. Τα δίκτυα αυτά είναι διαχειριζόμενα από τον πάροχο και για αυτό το λόγο ορίζονται ως έμπιστα. Τέτοια δίκτυα είναι τα WiFi hotspots του παρόχου τα οποία απαιτούν αυθεντικοποίηση με 802.1x, ένα standard για port-based access control. Αυθεντικοποιεί το τερματικό που θέλει να αποκτήσει πρόσβαση στο δίκτυο μέσω πολλών πρωτοκόλλων, όπως EAP, PEAP, MS-CHAP.

- TWAG (Trusted Wireless Access Gateway): Είναι η Gateway που συνδέονται όλα τα έμπιστα δίκτυα του παρόχου. Η σύνδεση του με το PGW γίνεται με ένα ασφαλές δίκτυο χρησιμοποιώντας τα πρωτόκολλα GTP, PMIM και όχι κάποιο IPSec. Τέλος το TWAG gateway, είναι συνδεδεμένο με τον AAA server του παρόχου ώστε να αυθεντικοποιεί, και να δίνει πρόσβαση στον συνδρομητή αλλά και να χρησιμοποιεί πληροφορίες που αφορούν την χρέωση.

Un-Trusted Access

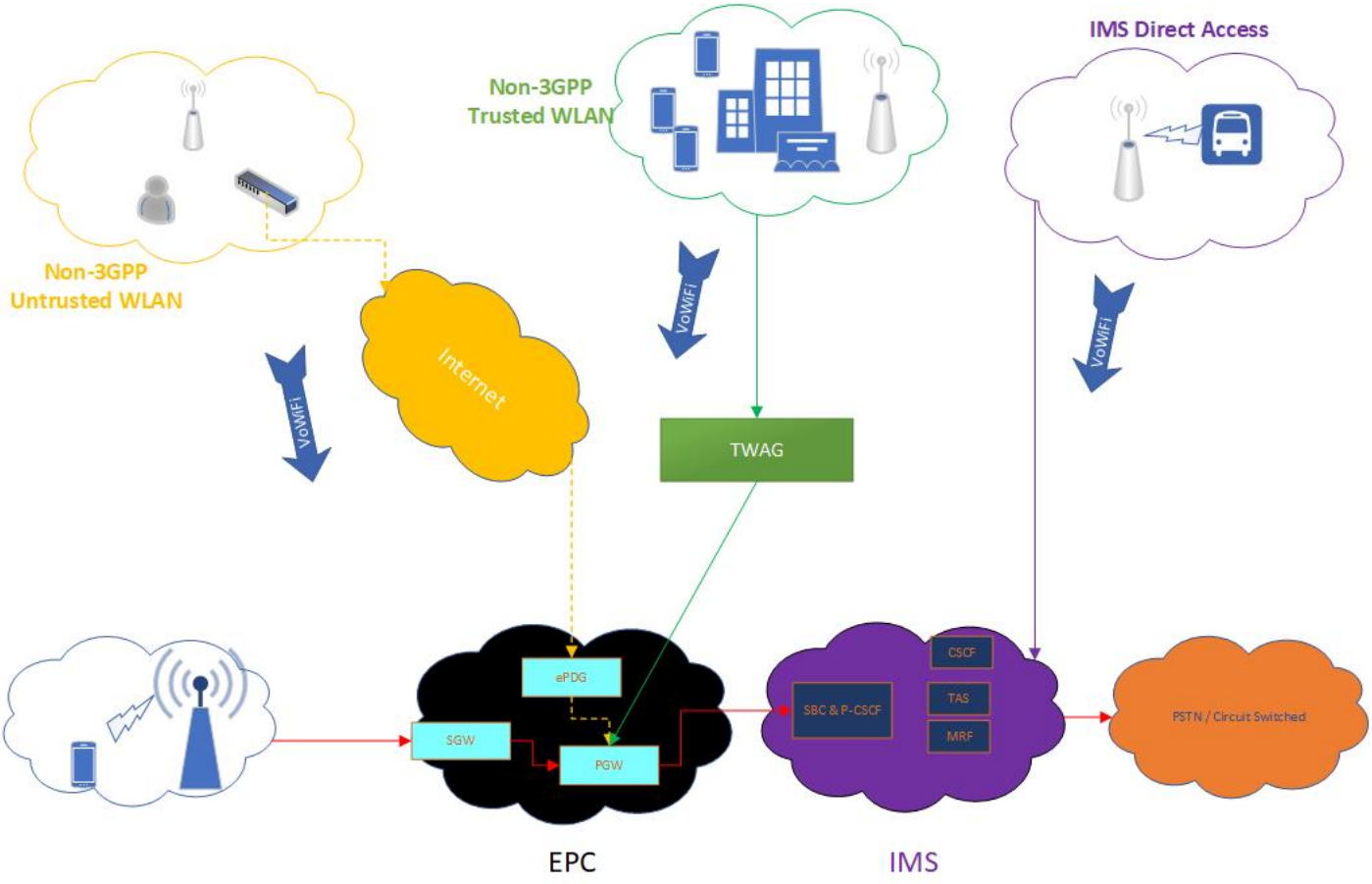
Αφορά non-3GPP δίκτυα τα οποία δεν έχουν οριστεί ως έμπιστα. Η πρόσβαση τους στο EPC δίκτυο πραγματοποιείται μέσω του ePDG, ώστε να οριστούν εκεί παράμετροι ασφάλειας, προτού εισχωρήσουν στο core δίκτυο του παρόχου. Μη έμπιστα δίκτυα αφορά όλα τα μέσα πρόσβασης στο core δίκτυο του παρόχου στο οποίο ο πάροχος δεν έχει καθόλου έλεγχο, όπως οικιακά ή δημόσια WiFi. Σε αυτή την περίπτωση, η οποία αφορά το μεγαλύτερο ποσοστό των οικιακών συνδρομητών, η κίνηση ξεκινά από το οικιακό δίκτυο και φτάνει μέσω του Ίντερνετ στον ePDG ώστε να τερματίσει στον PGW και να καταλήξει στο IMS. Συνεπώς, αφού η κίνηση μεταφέρεται μέσω Ίντερνετ, μια διαδρομή που ο πάροχος δεν μπορεί να εμπιστευτεί καθώς δεν έχει έλεγχο, αυτά τα δίκτυα τα θεωρούνται μη έμπιστα. Έτσι, το UE θα χρειαστεί να αυθεντικοποιηθεί και να διαπραγματευτεί πρωτόκολλα ασφαλείας που θέτονται από τον πάροχο, ώστε να αποκτήσει πρόσβαση στην υπηρεσία VoWiFi. Ένα από αυτά τα πρωτόκολλα ασφαλείας είναι και το IPSec.

Όπως αναφέραμε, για να αποκτήσει πρόσβαση ο συνδρομητής στην υπηρεσία VoWiFi πρέπει περάσει κάποια στάδια.

- **ePDG**: Το ePDG είναι η πρώτη οντότητα που συναντά το UE που είναι υπεύθυνη στο να ασφαλίσει την διασύνδεση της επικοινωνίας προς το EPC δίκτυο.
- **AAA**: Authentication, Authorization και Accounting. Αφορά τον server που θα αυθεντικοποιήσει το UE μέσω του πρωτοκόλλου EAP (extensible authentication protocol).
- **IPSEC**: όπως αναφέραμε επειδή τα δίκτυα αυτά δεν είναι έμπιστα πρέπει η επικοινωνία να είναι ασφαλής. Έτσι, όλη η επικοινωνία μεταξύ UE και IMS είναι κρυπτογραφημένη μέσω του πρωτοκόλλου IPSec. Η ανταλλαγή κλειδιών, ώστε να πραγματοποιηθεί το IPSec tunnel, γίνεται μέσω του IKEv2 πρωτοκόλλου. Το IKEv2 αποτελείται από 2 φάσεις:

  i. **IKE_SA_INIT**, όπου στην φάση αυτή γίνεται διαπραγμάτευση των παραμέτρων χωρίς κρυπτογράφηση για το IKE_SA στέλνοντας τις τιμές Diffie-Hellman.
  Το UE αρχικοποιεί το IKE_INIT και ανταλλάζει κλειδιά μέσω DH[14]. Ο ePDG μεταφέρει την κίνηση μεταξύ UE και AAA server ο οποίος αυθεντικοποιεί τον χρήστη.
  ii. **IKE_AUTH**, σε αυτή την φάση γίνεται μεταφορά των ταυτοτήτων και από τις δύο πλευρές, καθώς και η αυθεντικοποίηση, ώστε να εγκαθιδρύσουν το IPSec tunnel. Αυτή η φάση είναι κρυπτογραφημένη από το κλειδί DF που παράχθηκε στην προηγούμενη φάση.

Αφού ολοκληρωθεί επιτυχώς η αυθεντικοποίηση, ο server στέλνει τα κλειδιά που παράχθηκαν στο ePDG ο οποίος θα τα χρησιμοποιήσει για να αυθεντικοποιήσει για το IKE_INIT μέρος



Εικόνα 35: VoWiFi Architecture and structure

IMS Direct Access

Σε αυτά τα δίκτυα ο συνδρομητής έχει απευθείας πρόσβαση στο IMS δίκτυο, μέσω κάποιου application το οποίο είναι υπεύθυνο για την αυθεντικοποίηση του χρήστη.

6.3. Επιθέσεις και ανάλυση στο VoWiFi

Πολλοί οργανισμοί και εταιρίες έχουν δοκιμάσει να βρουν διάφορες ευπάθειες στην τεχνολογία VoWiFi καθώς πλέον αποτελεί ένα σημαντικό κομμάτι επικοινωνίας στην εποχή μας και άρα ένας σημαντικός στόχος για πολλούς κακόβουλους χρήστες.

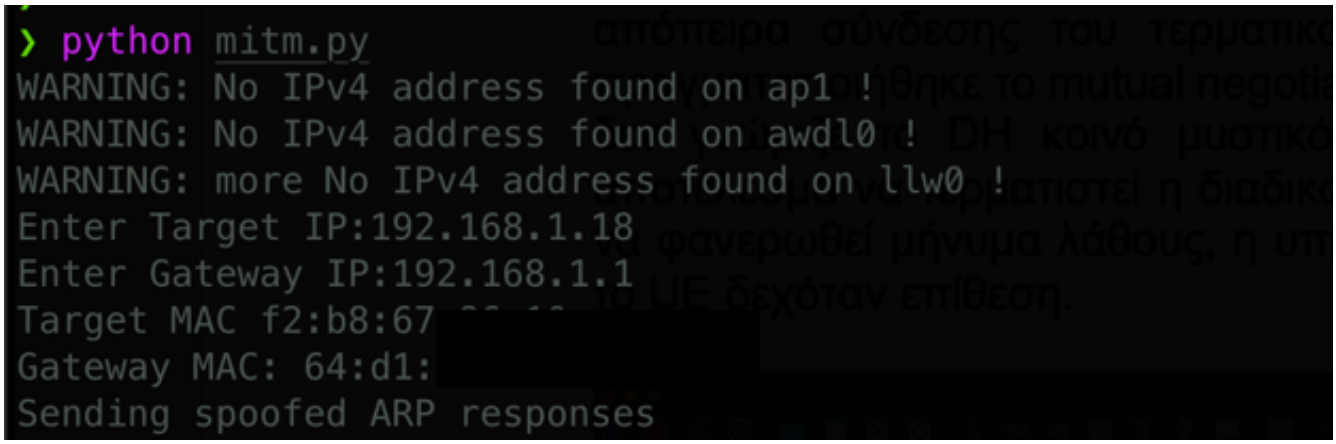
Μελετώντας διάφορες μελέτες μπορέσαμε και βρήκαμε διάφορες ευπάθειες, οι οποίες αναλύονται παρακάτω.

6.3.1. ARP Spoofing to extract IMSI

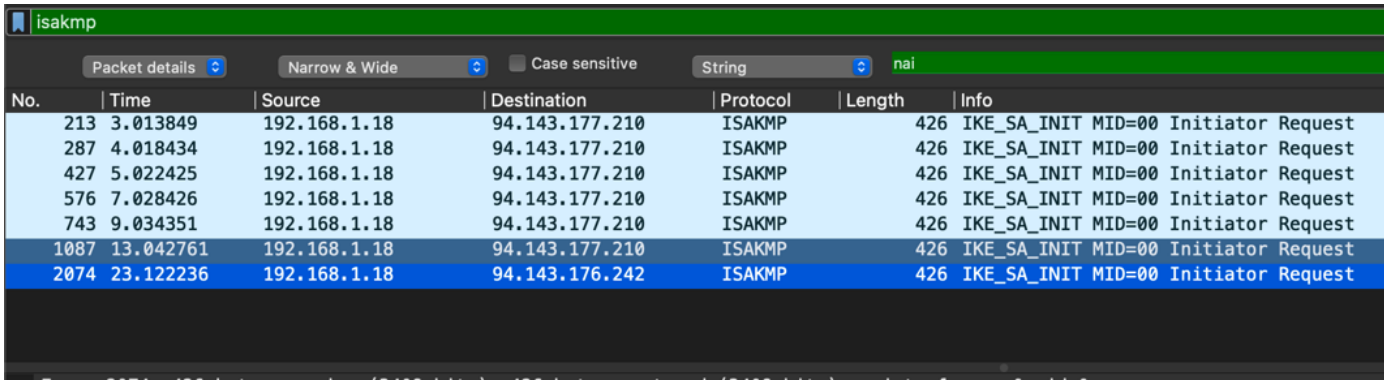
Οι ερευνητές στην δημοσίευση [1] μας παρουσιάζουν την δυνατότητα να εξάγουμε το IMSI από το τηλέφωνο. Πρακτικά ανακατευθύνουν το τερματικό να «δει» ως ePDG gateway το τερματικό του κακόβουλου χρήστη, μέσω των ARP Spoofing και DNS poisoning επιθέσεων και να ξεκινήσει την διαδικασία του IPSec. Το κακόβουλο τερματικό μιμήθηκε την λειτουργία του ePDG λειτουργώντας ως IPSec server, μέσω του opensource λογισμικού StrongSwan. Στο βήμα IKE_AUTH η συσκευή στέλνει το IMSI κάτι το οποίο είναι επικίνδυνο, καθότι το IMSI είναι κρυφό. Η διαρροή του IMSI μπορεί να βοηθήσει τον επιτιθέμενο να συνδέσει το IMSI με άλλες διευθύνσεις από το τερματικό του θύματος, όπως WiFi MAC Address, όποτε και ο εντοπισμός του να γίνεται πλέον πολύ εύκολα. Επίσης αξίζει να σημειωθεί πως δεν έγινε mutual authentication και από τις δύο πλευρές καθότι δεν βρέθηκε ποτέ ο IMS server, δημιουργώντας έτσι μια παθητική επίθεση DoS. Κανένα μήνυμα λάθους δεν φάνηκε στον χρήστη.

6.3.2. **DoS Attack on Huawei P30 VoWiFi**

Η επίθεση που πραγματοποιήθηκε σε αυτό το μέρος ήταν μια DoS επίθεση στο τερματικό του χρήστη με την βοήθεια του ARP Spoofing. Ο επιτιθέμενος μιμήθηκε το gateway του δικτύου με αποτέλεσμα να περνάνε όλα τα δεδομένα μέσα από το τερματικό του. Όπως φαίνεται και στις Εικόνες 29,30 έγινε απόπειρα σύνδεσης του τερματικού στο IMS του παρόχου αλλά δεν πραγματοποιήθηκε το mutual negotiation μεταξύ τους, καθώς ο επιτιθέμενος δεν γνώριζε το DH κοινό μυστικό (DH shared secret). Αυτό είχε σαν αποτέλεσμα να τερματιστεί η διαδικασία σύνδεσης στον IMS server. Χωρίς να φανερωθεί μήνυμα λάθους, η υπηρεσία VoWiFi ήταν μη διαθέσιμη, όσο το UE δεχόταν επίθεση.



Εικόνα 36: ARP attack script



Εικόνα 37: Wireshark capture από το τερματικό του επιτιθέμενου με την MITM επίθεση

7. Μέτρα αντιμετώπισης και μείωσης των ευπαθειών

Μετά τις επιθέσεις που αναλύσαμε από διάφορους ερευνητές στο VoLTE και κάποιες στο VoWiFI, καθώς και με τα τεστ που έγιναν από εμάς στο VoIP και VoWiFi, μπορούμε να εντοπίσουμε ή να μειώσουμε τις ευπάθειες αλλά και να προτείνουμε πιθανές λύσεις για την αντιμετώπιση τους.

7.1. Αναφορική παρουσίαση των ευπαθειών στα VoIP, VoLTE και VoWiFi

Επίθεση	Τεχνολογία		
	VoIP	VoLTE	VoWiFi
MITM (Arp Spoofing)	✓	✓	✓
DoS Attack	✓	✓	✓
Impersonation	✓	✓	✓
Eavesdropping	✓	✓	✓
Ping Flood	✓	✓	
Malformed Packet	✓	✓	
IPSec Extraction		✓	✓
Brute-Force	✓		
Rainbow Tables attack	✓		
DNS Poisoning	✓		✓
Session Highjack	✓	✓	✓
IMEI extraction		✓	✓
ISIM extraction		✓	✓
InviteFlood DOS Attack	✓		
Call Spoof ID	✓		

Πίνακας 1: Συγκριτικός πίνακας επιθέσεων στις τεχνολογίες VoIP, VoLTE και VoWiFi

7.2. Προτάσεις αντιμετώπισης και αποφυγής ευπαθειών

7.2.1. VoIP

Στο δικό μας μοντέλο επίθεσης παρατηρήσαμε τις αδυναμίες υλοποίησης του Asterisk server καθώς και τις αδυναμίες της υποδομής. Βασιζόμενοι σε αυτά προτείνουμε τις παρακάτω λύσεις:

Μέτρα αντιμετώπισης ως προς το λογισμικό

- SSL/TLS υλοποίηση είναι πλέον απαραίτητη, καθώς η εξαγωγή των κωδικών, που μεταφέρονται στο δίκτυο, είναι σχεδόν αδύνατη. Επιθέσεις όπως MITM είναι σχεδόν αδύνατες για κάποιον που βρίσκεται στο δίκτυο, χωρίς να έχει άμεση πρόσβαση στο τερματικό. Επιπλέον, η επίθεση Busy-Reply, καθίσταται αδύνατη καθώς ο κώδικας δεν έχει καθόλου πρόσβαση στα κρυπτογραφημένα πακέτα και προφανώς στο πακέτο σηματοδοσίας (στο οποίο βασίζεται η επίθεση)
- sRTP (secure RTP) είναι το πρωτόκολλο του οποίο πρέπει να υλοποιείται σε κάθε SIP Server, καθώς εμποδίζει τον επιτιθέμενο να υποκλέπτει τα πακέτα σε κατανοητή μορφή. Αυτό το μέτρο άμυνας εμποδίζει την επίθεση RTP Injection, καθώς ο επιτιθέμενος δεν έχει τον τρόπο να κρυπτογραφήσει τα κακόβουλα πακέτα που θα στείλει σε μια τρέχουσα συνεδρία των συνομιλητών.
- Τακτικός έλεγχος για αναβαθμίσεις συστήματος ώστε να αποφευχθούν νέες επιθέσεις που εντοπίστηκαν είτε σε πρωτόκολλα είτε στο λογισμικό.
- Ενεργοποίηση του συστήματος για διαγραφή duplicated mac-address ώστε να αποφευχθεί η επίθεση MITM
- Αλλαγή της default hash function MD5, στον SIP Server σε SHA256, ώστε να αποφευχθεί η ανάκτηση του κωδικού registration
- Δύσκολοι και μεγάλοι κωδικοί για την αυθεντικοποίηση των VoIP τερματικών. Ακόμα και υλοποίηση της SHA256 hash function να γίνει, αν ο κωδικός είναι μικρός σε μέγεθος αλλά και εύκολος, μπορεί να ανακτηθεί με μια επίθεση που βασίζεται σε rainbow tables.
- Στις περιπτώσεις επίθεσης των παρόχων θα έπρεπε να είχε υλοποιηθεί μια υποδομή με STIR/SHAKEN πρωτόκολλα ώστε να αποφευχθεί η επίθεση με το ψεύτικο caller-ID.

Μέτρα αντιμετώπισης ως προς την υποδομή

- Παραμετροποίηση της υποδομής σε ξεχωριστά VLAN δίκτυα. Ένα ξεχωριστό vlan δίκτυο θα πρέπει να υπάρχει σε κάθε VoIP υποδομή με σκοπό τον περιορισμό της VoIP υπηρεσίας από τα υπόλοιπα. Έχοντας ένα vlan στο δίκτυο φωνής, το ρίσκο μια επίθεσης από κακόβουλους χρήστες χωρίς πρόσβαση, είναι μηδαμινό. Τέλος χάρις στον διαχωρισμό των δικτύων, η εφαρμογή πολιτικών ασφαλείας πρόσβασης γίνεται πολύ πιο εύκολα διαχειρίσιμη.
- Εγκατάσταση IDS/IPS συστημάτων, ώστε να ανιχνεύεται εγκαίρως τυχόν επίθεση προς την υποδομή. Τα συστήματα IDS/IPS έχουν μηχανισμούς που μπορούν να ανιχνεύσουν αλλά και να σταματήσουν επιθέσεις όπως MITM ή DOS.
- Πολιτικές ασφαλείας πρόσβασης στην υποδομή, μέσω Firewalls (είτε layer 4 είτε layer 7) που επιτρέπουν σε συγκεκριμένα πρωτόκολλα να έχουν πρόσβαση όπου οριστεί.
- Υποδομή VPN ώστε να αποτρέπεται η σύνδεση των τερματικών στον SIP Server απευθείας μέσω Ίντερνετ, καθώς τα πακέτα SIP είναι μη κρυπτογραφημένα.

7.2.2. VoWiFi

Μετά από ανάλυση των επιθέσεων, μπορούμε πλέον να συμπεράνουμε τις ευπάθειες των που προέκυψαν και να προτείνουμε κάποιες λύσεις:

- IPSec extraction keys. Όπως αναφέρθηκε το UE κάνει χρήση του IPSec για να συνδεθεί στον IMS server από οποιοδήποτε WiFi με σκοπό να κρυπτογραφήσει και να πιστοποιήσει την ακεραιότητα των πακέτων. Παρόλα αυτά η επίθεση ώστε να βρεθούν τα κλειδιά του IPSec ολοκληρώθηκε επιτυχώς. Χρησιμοποιώντας το SimTrace ο ερευνητής του [1], κατάφερε και διάβασε τα πακέτα CK/IK τα οποία παράγονται από το shared secret που κάνει χρήση το IPSec.

Έτσι, μια μορφή αντιμετώπισης θα ήταν να χρησιμοποιηθεί μια SIM ενσωματωμένη στο τερματικό, κάτι που θα εμπόδιζε το SimTrace να πετύχει την επίθεση.

- Έλεγχος πακέτων στο PDN gateway με σκοπό να γίνεται εξονυχιστικός έλεγχος των πακέτων ώστε να αποτραπεί τυχόν επίθεση impersonation (IMEI μαζί με IMSI).

- Παρατηρήθηκε όπως αναφέραμε προηγουμένως, πως το SIP Register πακέτο περιελάβανε την τιμή του IMSI, κάτι το οποίο στάλθηκε χωρίς κρυπτογράφηση στον IMS server, άρα πριν την εγκαθίδρυση του IPSec. Στην προκειμένη περίπτωση θα πρέπει να στέλνεται και αυτό το πακέτο κρυπτογραφημένο. Θα μπορούσε να χρησιμοποιηθεί κάποιο πρωτόκολλο EAP όπως το EAP-TTLS το οποίο χρειάζεται ένα server certificate ώστε να πιστοποιήσει τον server και να συνδεθεί σε αυτόν, αφού πρώτα έχει εγκατασταθεί το certificate αυτό στο UE.
- Τέλος όπως αναφέραμε και προηγουμένως αν και ο χρήστης θα πρέπει να είναι υποψιασμένος, είναι δύσκολο να καταλάβει τυχόν αντίστοιχες επιθέσεις, οπότε θα πρέπει να προσέχει σε ποια δίκτυα WiFi συνδέεται.
- Σε περίπτωση που δεν γνωρίζει την ασφάλεια και την εμπιστευτικότητα του δικτύου στο οποίο συνδέεται, θα πρέπει να χρησιμοποιεί κάποιο VPN, προτού προχωρήσει σε οποιαδήποτε ενέργεια. Προφανώς επειδή το VPN κρυπτογραφεί όλα τα πακέτα είναι και το πιο ασφαλές πρωτόκολλο για να συνδεθεί κάποιος σε ένα άγνωστο δίκτυο και να αποφύγει τυχόν υποκλοπές.

7.2.3. VoLTE

Μετά τις ευπάθειες που αναφέρθηκαν μπορούμε να προτείνουμε κάποιες λύσεις. Οι λύσεις αναφέρονται παρακάτω:

- Προτείνουμε να γίνεται έλεγχος και στον φορέα σηματοδοσίας του παρόχου και να χρεώνει κανονικά με ορθή πολιτική, τα σήματα αυτά. Έτσι ο επιτιθέμενος δεν θα μπορεί να χρησιμοποιήσει τον φορέα σηματοδοσίας με ειδικά τροποποιημένα πακέτα για δωρεάν χρήση της υπηρεσίας. Προφανώς θα πρέπει να προχωρήσει και στις ανάλογες τροποποιήσεις στον AAA server.
- Προτείνεται να γίνεται έλεγχος των πακέτων στον φορέα σηματοδοσίας και να μην υπάρχει ελεύθερη αποστολή αλλά και χρήση όλου του φάσματος από μη σχετικά πρωτόκολλα SIP.
- Καθώς φαίνεται ότι δεν υπάρχει μηχανισμός ώστε να ελέγχει εξονυχιστικά τα πακέτα, ο επιτιθέμενος μπορεί να «κρύψει» διάφορα δεδομένα μέσα σε ένα πακέτο SIP, όπως κάναμε στην επίθεση του VoIP στο τμήμα 4.5. Η επίθεση SIP tunneling μπορεί να διακοπεί αν σε κάποιον SIP server του παρόχου γίνεται ανίχνευση των πακέτων.

- Κρυπτογράφηση του μηνύματος SIP register καθότι περιλαμβάνει τις τιμές των IMEI και IMSI. Όπως παρατηρήσαμε το SIP REGISTER μήνυμα στέλνεται πριν ξεκινήσει η διαδικασία του IPSec.

8. Σύνοψη – Συμπεράσματα

Ο στόχος της διπλωματικής αυτής ήταν να βρεθούν αλλά και να δοκιμαστούν τυχόν ευπάθειες στις τεχνολογίες VoIP, VoLTE και VoWiFi.

Στο πρώτο μέρος αφού κάναμε μια εισαγωγή για την ιστορία αλλά και την τεχνολογική εξέλιξη στις υπηρεσίες φωνής και πως αυτές επηρέασαν την ζωή μας, προχωρήσαμε στο δεύτερο μέρος στην ανάλυση των τεχνολογιών αυτών και πρωτόκολλα που χρησιμοποιούν. Στο τρίτο μέρος προσπαθήσαμε να επιτεθούμε στις ευπάθειες που θεωρήσαμε ότι υπάρχουν βάση κατασκευής και υλοποίησης, αναλύοντας παράλληλα και επιθέσεις που έγιναν από άλλους ερευνητές. Στην τεχνολογία VoIP όλες οι επιθέσεις ολοκληρώθηκαν επιτυχώς, σε ένα σύστημα με υποδομές ασφαλείας. Επιπλέον, παρουσιάσαμε τα εργαλεία αλλά και τους κώδικες που χρησιμοποιήσαμε για τις επιθέσεις αυτές. Οι επιθέσεις που αναφέρθηκαν στο VoLTE ήταν αναλύσεις από άλλους ερευνητές, καθότι δεν υπήρχε ο απαραίτητος εξοπλισμός. Στο τέταρτο μέρος προτείναμε διάφορες λύσεις που θεωρούμε ότι μειώνουν ή αντιμετωπίζουν τις ευπάθειες αυτές.

Παρουσιάζοντας διάφορες επιθέσεις που έχουν ως σκοπό την εξαγωγή κλειδιών IPSec, τον εντοπισμό του IMEI αλλά και του IMSI, (δεδομένα τα οποία αν πέσουν σε λάθος χέρια γίνονται αρκετά επικίνδυνα), την αποστολή δεδομένων δωρεάν μέσω του φορέα σηματοδοσίας, αλλά και επιθέσεις DoS, κάνοντας τον χρήστη ανίκανο να χρησιμοποιήσει την υπηρεσία φωνής, μας κάνει να αναρωτιόμαστε αν οι τεχνολογίες αυτές είναι ασφαλείς και πάντα διαθέσιμες. Το μόνο σίγουρο είναι πως οι τεχνολογίες VoLTE και VoWiFi είναι σχετικά καινούργιες αλλά και συνεχώς εξελισσόμενες, κάτι το οποίο δίνει την ευκαιρία σε πολλούς κατασκευαστές και παρόχους να διορθώσουν σοβαρά προβλήματα που υπάρχουν στις υποδομές τους αλλά και στον τρόπο χρήσης των τεχνολογιών αυτών.

Η τεχνολογία VoIP είναι πλεον αρκετά διαδεδομένη και σχεδόν καθολική ως υπηρεσία φωνής σε πολλές χώρες. Οι επιθέσεις που παρουσιάστηκαν είχαν διάφορες βαθμίδες επικινδυνότητας δείχνοντας έτσι την μεγάλη γκάμα από επιθέσεις που μπορούν να βλάψουν μια υποδομή VoIP ακόμα και αν είναι ασφαλής.

ΠΑΡΑΡΤΗΜΑ Ι

1. Multimedia Messaging Service
2. Wireless Application Protocol
3. High Speed Packet Access
4. Synchronous optical networking
5. https://www.rampfesthudson.com/what-is-fdm-tdm-and-cdm/
6. IP Multimedia Subsystem
7. Plain old telephone service
8. OSI model
9. User Datagram Protocol
10. Address Resolution Protocol
11. https://en.wikipedia.org/wiki/ARP_spoofing
12. https://en.wikipedia.org/wiki/Dictionary_attack
13. https://www.globenewswire.com/news-release/2022/03/17/2405549/0/en/GL-Announces-Internet-Protocol-Multimedia-Subsystem-Network-Emulation-Test-Suite.html
14. Diffie–Hellman
15. operating company number
16. service provider identifier

ΠΑΡΑΡΤΗΜΑ ΙΙ

MITM code using scapy

```
from scapy.all import *

def getmac(targetip):
	arppacket= Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(op=1, pdst=targetip)
	targetmac= srp(arppacket, timeout=2 , verbose= False)[0][0][1].hwsrc
	return targetmac

def spoofarpcache(targetip, targetmac, sourceip):
	spoofed= ARP(op=2 , pdst=targetip, psrc=sourceip, hwdst= targetmac)
	send(spoofed, verbose= False)

def restorearp(targetip, targetmac, sourceip, sourcemac):
	packet= ARP(op=2 , hwsrc=sourcemac , psrc= sourceip, hwdst= targetmac , pdst=
targetip)
	send(packet, verbose=False)
	print ('ARP Table restored to normal for', targetip)

def main():
	targetip= input("Enter Target IP:")
	gatewayip= input("Enter Gateway IP:")

	try:
		targetmac= getmac(targetip)
		print ("Target MAC", targetmac)
	except:
		print ("Target machine did not respond to ARP broadcast")
		quit()

	try:
		gatewaymac= getmac(gatewayip)
		print ("Gateway MAC:", gatewaymac)
	except:
		print ("Gateway is unreachable")
		quit()
	try:
		print ("Sending spoofed ARP responses")
		while True:
			spoofarpcache(targetip, targetmac, gatewayip)
			spoofarpcache(gatewayip, gatewaymac, targetip)
	except KeyboardInterrupt:
		print ("ARP spoofing stopped")
		restorearp(gatewayip, gatewaymac, targetip, targetmac)
		restorearp(targetip, targetmac, gatewayip, gatewaymac)
		quit()

if __name__=="__main__":
	main()
```

Call spoof

```
#!/bin/bash
rm extensions.conf
sed "s/CALLSPOOF/$1" < ext-temp.conf > extensions.conf
asterisk -rx "core restart now"
```

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] Sreepriya Chalakkal, “PRACTICAL ATTACKS ON VOLTE AND VOWIFI”; https://ernw.de/download/newsletter/ERNW_Whitepaper_60_Practical_Attacks_On_VoLTE_And_VoWiFi_v1.0.pdf

[2] Chi-Yu Li∗, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, “Insecurity of Voice Solution VoLTE in LTE Mobile Networks”; 2015, https://www.researchgate.net/publication/301415349_Insecurity_of_Voice_Solution_VoLTE_in_LTE_Mobile_Networks

[3] Piers O’Hanlon, Ravishankar Borgaonkar, “Mobile Subscriber WiFi Privacy”; 2017, https://ieeexplore.ieee.org/document/8227304/authors#authors

[4] Tian Xie, Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Jiawei Li, Mi Zhang, “The Dark Side of Operational Wi-Fi Calling Services”; https://www.egr.msu.edu/~mizhang/papers/2018_CNS_WiFiCalling.pdf

[5] Shawn McGann, Douglas C. Sicker, “An Analysis of Security Threats and Tools in SIP-Based VoIP Systems”,

[6] PIERS O’HANLON, Ravishankar Borgaonkar. “Mobile subscriber WiFi privacy”. https://www.ieee-security.org/TC/SPW2017/ MoST/proceedings/OHanlon_MoST17.pdf.

[7] VoWifi (Voice over Wi-Fi) https://www.gsma.com/futurenetworks/ip_services/vowifi

[8] “VoLTE Service Description and Implementation Guidelines”, https://www.gsma.com/futurenetworks/wp-content/uploads/2014/10/FCM.01-VoLTE-Service-Description-and-Implementation-Guidelines-Version-2.0.pdf”

[9] Solomon Ndungu, “GSM (Global System for Mobile communication)”, techtarget.com/searchmobilecomputing/definition/GSM

[10] HANDLEY M , JACOBSON V, PERKINS C. SDP: Session Description Protocol https://www.rfc-editor.org/rfc/rfc4566.txt

[11] “What is Voice over Wi-Fi” https://ribboncommunications.com/company/get-help/glossary/voice-over-wi-fi

[12] 3GPP. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses. 2018. Available also from: https://www.etsi.org/deliver/etsi_ts/133400_133499/133402/15.01.00_60/ts_133402v150100p. pdf. Technical Specificatio

[13] 3GPP. Universal Mobile Telecommunications System (UMTS);LTE; Architecture enhancements for non-3GPP accesses. 2018. https://www.etsi.org/deliver/etsi_ts/123400_123499/23402/15.03.00_60/ts_123402v150300p.pdf. Technical Specification (TS). 3rd Generation Partnership Project (3GPP). Version 15.3.0.

[14] SAUTER, Martin. FROM GSM TO LTE: AN INTRODUCTION TO MOBILE NETWORKS AND MOBILE BROADBAND. 1st ed. Chichester: John Wiley & Sons Ltd, 2011. ISBN 978-0-470-97824-5

[15] ANDREWS, Jeffrey G.; GHOSH, Arunabha; MUHAMED, Rias; ZHANG, Jun. Fundamentals of LTE. 1st ed. Upper Saddle River: Prentice Hall, 2010. ISBN 978-0137033119.

[16] HEINE, Gunnar; SAGKOB, Holger. GPRS: Gateway to Third Generation Mobile Networks. 1st ed. Cambridge (Mass): Artech House, 2003. ISBN 1580531598.

[17] UMTS Protocol Analyzer [online]. Brno: GL Communications Inc., 2019 [visited on 2019-04-21].

[18] LTE Network Architecture https://www.tutorialspoint.com/lte/lte_network_architecture.htm

[19] ARKKO, J.; HAVERINEN, H. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) [Internet Requests for Comments]. RFC Editor, 2006. ISSN 2070-1721. Available also from: https://www.rfc-editor.org/rfc/rfc4187. txt. RFC. RFC Editor.