ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΚΑΔΗΜΑΙΚΟ ΕΤΟΣ 2012-2013

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ

"Ενίσχυση του Επιπέδου Ασφάλειας σε IMS περιβάλλοντα"

Ιωαννίδης Σωκράτης (MTE1050)

ΕΠΙΒΛΕΠΩΝ: Επικ. Καθηγητής Κ. Λαμπρινουδάκης

Περιεχόμενα

Πίνακας Εικόνων

Περίληψη

Η παρούσα διπλωματική έχει ως στόχο την μελέτη των τηλεπικοινωνιακών δικτύων νέας γενιάς IMS και τις απειλές που δέχονται όσον αφορά την ασφάλεια των χρηστών και των υπηρεσιών τους. Για τον σκοπό αυτό έχει υλοποιηθεί το περιβάλλον OpenIMS Core το οποίο αποτελεί ένα λειτουργικό περιβάλλον IMS και πάνω σε αυτό θα εφαρμοστούν επιθέσεις που θα έχουν ως στόχο την κατάλυση της ιδωτικότητας, της εμπιστευτικότητας και της διαθεσιμότητας του δικτύου. Στην συνέχεια θα γίνει προσπάθεια να αντιμετωπιστούν οι συγκεκριμένες επιθέσεις, προτείνοντας κατάλληλους μηχανισμούς ασφάλειας.

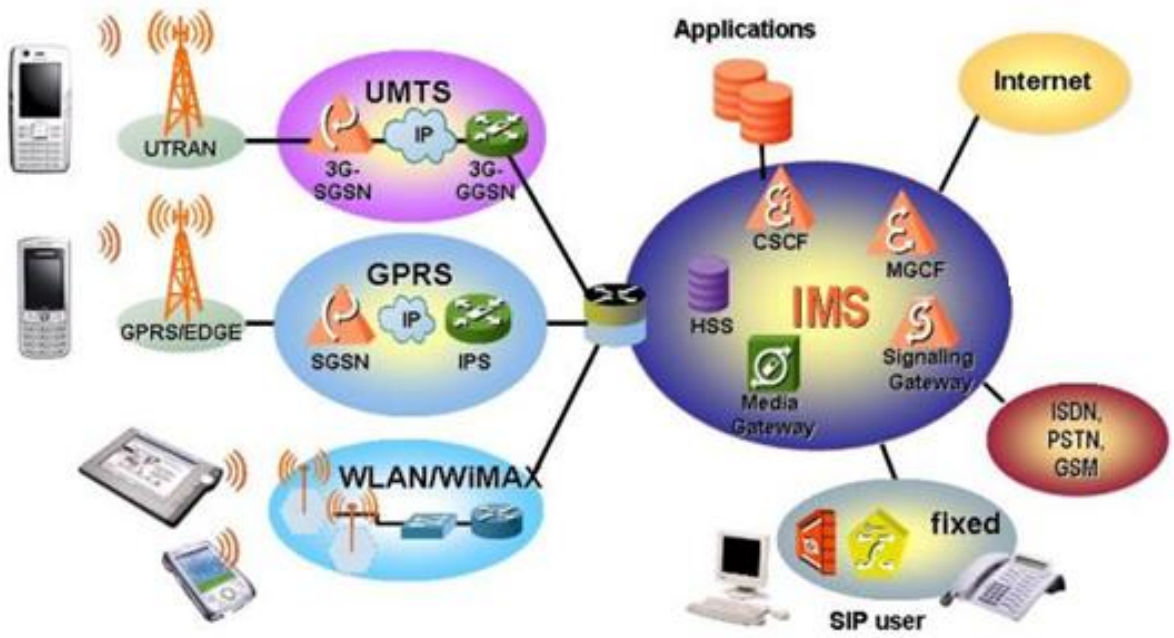
Κεφάλαιο 1

1.1 Εισαγωγή

Τα τηλεπικοινωνιακά δίκτυα έχουν υποστεί πολύ μεγάλες αλλαγές τα τελευταία χρόνια. Στο πεδίο των κινητών δικτύων, τα δίκτυα πρώτης γενιάς (1G) εμφανίστηκαν στα μέσα της δεκαετίας του 80’ και σκοπός τους ήταν να προσφέρουν στους χρήστες βασικές υπηρεσίες. Οι υπηρεσίες αυτές περιστρέφονταν γύρω από την μετάδοση φωνής. Την δεκαετία του 90’ και καθώς οι απαιτήσεις αυξάνονταν εμφανίστηκαν τα δίκτυα δεύτερης γενιάς (2G) τα οποία προσέφεραν στους χρήστες τις πρώτες υπηρεσίες μεταγωγής δεδομένων καθώς και κάποιες στοχευμένες υπηρεσίες γύρω από την μεταγωγή δεδομένων. Πλέον καθώς η τεχνολογία των κινητών συσκευών έχει αναπτυχθεί ραγδαία και οι απαιτήσεις των πελατών έχουν αυξηθεί, έχουν αναπτυχθεί τα δίκτυα τρίτης και τέταρτης γενιάς (3G και 4G) τα οποία γνωρίζουν ιδιαίτερη άνθηση στις μέρες μας. Τα δίκτυα αυτά προσφέρουν υψηλή μετάδοση δεδομένων και προηγμένες υπηρεσίες μεταγωγής πακέτων.

Στον αντίποδα τα δίκτυα σταθερών επικοινωνιών τα δίκτυα που υπερίσχυαν μέχρι και το πρόσφατο παρελθόν ήταν αυτά των Public Switched Telephone Network (PSTN) και το Integrated Services Digital Network (ISDN) τα οποία χρησιμοποιούνται ακόμα και σήμερα από κάποιους παρόχους για την μετάδοση υπηρεσιών φωνής. Η εμφάνιση του ADSL και η αυξημένη ζήτησή του από τους χρήστες, που επιτρέπει να

μετάδοση πακέτων με υψηλό ρυθμό μετάδοσης με χαμηλό σταθερό κόστος έχει φέρει στο προσκήνιο υπηρεσίες πραγματικού χρόνου με υψηλό QoS όπως για παράδειγμα το Video Streaming και το Voice over IP (VoIP).



Εικόνα 1. IMS Integrated Networks

Η μεγάλη αύξηση των χρηστών κινητών υπηρεσιών, η ανάπτυξη των IP δικτύων και η επιθυμία των τηλεπικοινωνιακών παρόχων για μείωση των λειτουργικών εξόδων έχουν οδηγήσει στην ανάγκη ενοποίησης των δικτύων κινητών και σταθερών επικοινωνιών. Καθώς όλα τα δίκτυα τείνουν προς την κατεύθυνση του IP έτσι και τα στοίχημα είναι να μπορέσουμε να εφαρμόσουμε την IP τεχνολογία σε αυτό το κομμάτι με το απαιτούμενο QoS.

Το τηλεφωνικό δίκτυο ενδείκνυται για παροχή του κοινού παρονομαστή μεταξύ των διάφορων δικτυακών τεχνολογιών, μέσω χρήσης peer-to-peer συνδέσεων πάνω στο επίπεδο του IP. Το κενό αυτό έρχεται να καλύψει το IP Multimedia Subsystem (IMS) επιτρέποντας τους μηχανισμούς για την σύγκλιση των διάφορων τεχνολογιών.

Το IMS δίκτυο μας παρέχει την απαιτούμενη αρχιτεκτονική ελέγχου των υπηρεσιών πολυμέσων και της σύνδεσης των χρηστών στο IP δίκτυο αποτελώντας την τεχνολογία κλειδί. Είναι και ανεξάρτητο από τις τεχνολογίες πρόσβασης και σε αυτό το κομμάτι οφείλει την μεγάλη διείσδυση του. Η αρχιτεκτονική του IMS προσφέρει διάφορες υπηρεσίες πολυμέσων στους χρήστες χρησιμοποιώντας πρωτόκολλα βασισμένα στο internet. Επίσης έχει την πολύ σημαντική ικανότητα να συνδυάζει την κινητικότητα με το IP δίκτυο. Μια δυνατότητα απαραίτητη για τις κινητές τηλεφωνίες. Στην εικόνα 1 παρουσιάζεται ένα ενοποιημένο δίκτυο επικοινωνιών με βάση την τεχνολογία του IMS.

1.2 Υπηρεσίες του IMS

Τα IMS δίκτυα προσφέρουν ποικίλες υπηρεσίες και εφαρμογές στους χρήστες. Οι συσκευές που συνδέονται στα δίκτυα IMS κατά την ενεργοποίησή τους συνδέονται και εγγράφονται στο δίκτυο μέσο της αρχικής ανταλλαγής μηνυμάτων (registration). Της αρχικές πληροφορίες για την εγγραφή στο δίκτυο, όπως για παράδειγμα τα στοιχεία της ταυτότητας του συνδρομητή, τις αντλούν από τις κάρτες USIM αν πρόκειται για δίκτυο κινητής τηλεφωνίας είτε μέσω του modem αν πρόκειται για σταθερό δίκτυο. Κατά την διάρκεια αυτής της αρχικής εγγραφής η συσκευή και το δίκτυο αυθεντικοποιούνται και πιστοποιούνται το ένα στο άλλο.

Αφού πραγματοποιηθεί η εγγραφή της συσκευής-χρήστη στο δίκτυο, τότε όλες οι υπηρεσίες του IMS δικτύου είναι έτοιμες προς χρήση. Παραδείγματα τέτοιων υπηρεσιών που μπορούν να χρησιμοποιήσουν οι χρήστες του IMS είναι:

- Συνεδρίες φωνής
- Συνεδρίες video
- Push to Talk
- Presence
- Αποστολή μηνυμάτων
- Διαμοιρασμός Εικόνων
- Peer-to-peer video sharing
- Παιχνίδια

Στις περιπτώσεις υπηρεσιών φωνής το δίκτυο IMS αναλαμβάνει την αναζήτηση των τερματικών που θέλουν να επικοινωνήσουν και μέσω της υπηρεσίες presence θα διαπιστώσει την διαθεσιμότητά τους. Στην συνέχεια θα εγκαθιδρύσει μια συνεδρία SIP (Session Initiation Protocol) μεταξύ των δύο συσκευών. Το δίκτυο IMS αναλαμβάνει την διαχείριση όλης της σηματοδοσίας που απαιτείται για την εγκαθίδρυση, την πραγματοποίηση και τον τερματισμό των κλήσεων είτε είναι φωνής είτε video. Παράλληλα με τις υπηρεσίες συνεδρίας φωνής και video υπάρχει και η δυνατότητα αποστολή γραπτών μηνυμάτων από το ένα τερματικό στο άλλο.

Με την υπηρεσία push to talk προσομοιώνεται η χρήση καναλιού ασυρμάτου (walkie-talkie) στα τερματικά του IMS δικτύου. Έτσι η επικοινωνία μεταξύ των δύο τερματικών πραγματοποιείται με το πάτημα ενός κουμπιού, σε περίπτωση που υπάρχει ένδειξη ελεύθερου καναλιού και τότε το κανάλι καταλαμβάνεται από τον χρήστη για επικοινωνία. Όταν γίνει η επικοινωνία ο χρήστης ελευθερώνει το κουμπί να μπορέσει ο συνομιλητής να χρησιμοποιήσει το κοινό κανάλι. Η παρούσα εφαρμογή χρησιμοποιείται σε περιπτώσεις όπου η επικοινωνία μεταξύ δύο τερματικών εμπεριέχει μεγάλα κενά και πρέπει να είναι άμεση. Από πλευράς πόρων το pusk to talk είναι πολύ αποδοτικό καθώς χρησιμοποιεί το κανάλι φωνής μόνο όταν χρειάζεται ο χρήστης να στείλει φωνή και είναι ελεύθερο στη συνέχεια.

Επίσης στις εφαρμογές των δικτύων IMS να προσθέσουμε την δυνατότητα διαμοιρασμού εικόνων και video (image sharing, Peer-to-peer video sharing) καθώς και την δυνατότητα να παίξουν οι χρήστες online παιχνίδια.

Κεφάλαιο 2

2.1 Η εξέλιξη του IMS

Τα τηλεπικοινωνιακά δίκτυα εξελίχτηκαν από τα πρώτα χρόνια της δημιουργίας τους σε μεγάλο βαθμό ώστε να φτάσουμε στα δίκτυα νέας γενιάς όπως είναι αυτό του IMS.

Αρχικά τα δίκτυα που χρησιμοποιούνταν ήταν αυτά της μεταγωγής κυκλώματος. Τα δίκτυα κινητής τηλεφωνίας GSM και τα δίκτυα σταθερής τηλεφωνίας PSTN χρησιμοποιούν μεταγωγή κυκλώματος. Στα δίκτυα αυτής της τεχνολογίας υπάρχει διαχωρισμός της επικοινωνίας μεταξύ των τερματικών σε δύο επίπεδα. Τα επίπεδα αυτά είναι το επίπεδο της σηματοδοσίας και το επίπεδο μέσων.

Το δίκτυο IMS διαφοροποιεί και αυτό την σηματοδοσία από τα πολυμέσα. Οι μόνοι κόμβοι που επεξεργάζονται μηνύματα σηματοδοσίας και πολυμέσα είναι οι τερματικές συσκευές. Όλοι οι κόμβοι του IMS δικτύου δεν χειρίζονται και τα δύο μειώνοντας με αυτό τον τρόπο την πολυπλοκότητα του δικτύου.

Κατά την εξέλιξη των GSM δικτύων και καθώς αυξάνονταν η ανάγκη για τη χρήση του διαδικτύου σε κινητές συσκευές, εισάγετε η μεταγωγή πακέτου σε αυτά. Η εξέλιξη του GSM δικτύου με μεταγωγή πακέτου ονομάζετε GPRS και αποτέλεσε την βάση για την περεταίρω εξέλιξη των δικτύων μεταγωγής πακέτου.

Το IMS είχε αρχικά παρουσιαστεί το 1999 από ένα βιομηχανικό forum που ονομαζόταν 3G.IP. Το 3G.IP είχε ορίσει την αρχική αρχιτεκτονική του IMS το οποίο δόθηκε στο 3rd Generation Partnership Project (3GPP), ως μέρος προς προτυποποίηση για κινητά τηλέφωνα 3G σε δίκτυα UMTS. Πρωτοεμφανίστηκε στην έκδοση 5, ως εξέλιξη από τα δίκτυα 2G στα δίκτυα 3G, όταν είχε εισαχθεί το SIP σε αυτά.

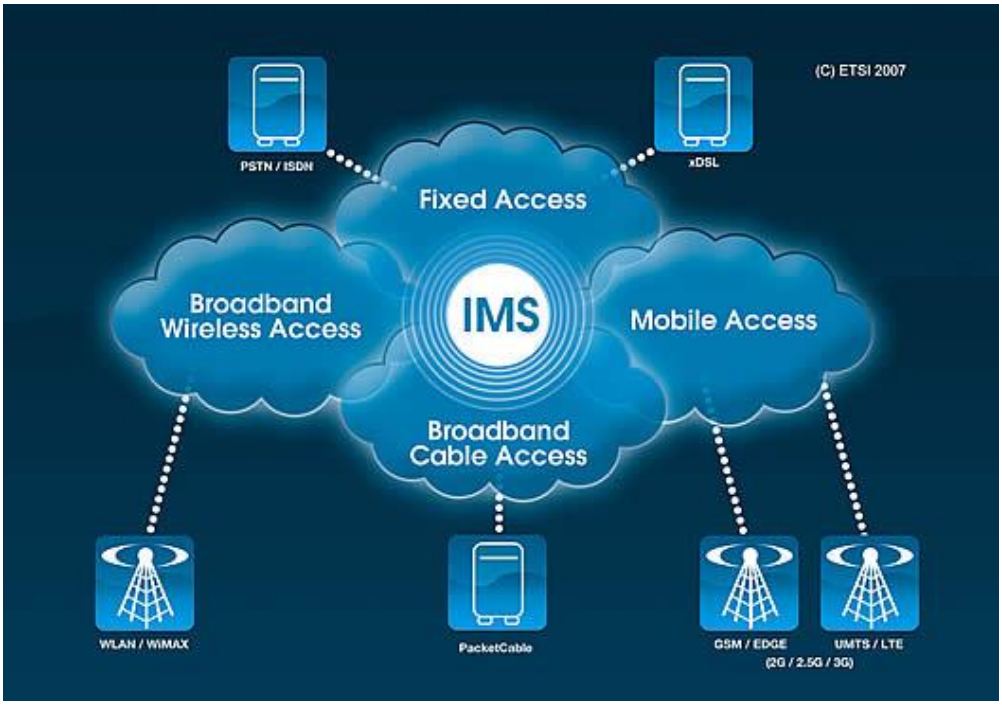
Η 3GPP σε συνεργασία με την TISPAN εμφάνισαν αργότερα την έβδομη έκδοση του IMS η οποία είχε δύο νέες οντότητες, την AGCF (access gateway control function) και την PES (PSTN emulation service). Οι οντότητες αυτές χρησιμοποιούνταν για την επικοινωνία του IMS δικτύου με ενσύρματα δίκτυα παλαιότερης γενιάς τα οποία όμως δεν είχαν πάψει να βρίσκονται εγκατεστημένα σε πολλούς τηλεπικοινωνιακούς παρόχους και λόγω κόστους δεν γινόταν να καταργηθούν άμεσα. Η AGCF αποτελούσε γέφυρα συνδεσιμότητας των IMS δικτύων με τα δίκτυα Megaco/H.248. Αντίστοιχα και η PES προσέφερε αντίστοιχες υπηρεσίες στο IMS δίκτυο.

2.2 Ο Στόχος του IMS

Το IMS δημιουργήθηκε την εποχή που τα δίκτυα μεταγωγής πακέτων δεν μπορούσαν να προσφέρουν ικανοποιητικές υπηρεσίες όσον αφορά το IP και δεν είχε γίνει διαδεδομένο το διαδίκτυο στις κινητές συσκευές.

Έτσι στόχος του IMS ήταν να εφαρμόσει τεχνολογίες αιχμής που υπήρχαν στον χώρο τον τηλεπικοινωνιών την περίοδο αυτή και να εισάγει με αυτό τον τρόπο άμεσα το διαδίκτυο στα κινητά τηλέφωνα. Ακόμα έπρεπε να αποτελέσει μια κοινή πλατφόρμα ώστε πάνω σε αυτή να αναπτυχθούν οι διάφορες υπηρεσίες που θα υποστήριζε, μέσω διαφορετικών δικτύων πρόσβασης σε αυτό.

Το IMS δίκτυο, όπως και όλα τα IP δίκτυα, είναι χαμηλού επιπέδου και δεν εξαρτάται από τον τρόπο πρόσβασης σε αυτό. Έτσι οι χρήστες μπορούν να συνδέονται σε αυτό είτε μέσω σύνδεσης xDSL (Digital Subscriber Line), είτε μέσω WLAN (Wireless Local Access Network), μέσω οπτικού δικτύου ή μέσω δικτύου κινητής τηλεφωνίας (GSM, GPRS). Έτσι επιτυγχάνεται ο αρχικός σκοπός του IMS που είναι να αποτελέσει την βάση πολλών διαφορετικών και ενοποιημένων τηλεπικοινωνιακών δικτύων.



Εικόνα 2. IMS μέσω διαφορετικών δικτύων πρόσβασης

Ορίστηκαν τα βασικά σημεία του IMS δικτύου μέσω των απαιτήσεων που έπρεπε αυτό να καλύψει:

- Υποστήριξη εγκατάστασης συνόδων πολυμέσων πάνω στο IP.
- Υποστήριξη μηχανισμού QoS (quality of service).
- Υποστήριξη σύνδεσης με το διαδίκτυο και δίκτυα μεταγωγής κυκλώματος.
- Υποστήριξη περιαγωγής (roaming).
- Υποστήριξη ισχυρών ελέγχων του χρήστη και της επικοινωνίας.

- Υποστήριξη δυνατότητας άμεσης εισαγωγής νέων υπηρεσιών.

Η απαίτηση υποστήριξης IP συνόδων πολυμέσων είναι η βασικότερη εκ των παραπάνω για τα δίκτυα IMS. Αποτελεί την αμεσότερη επικοινωνία μεταξύ δύο χρηστών του δικτύου IMS μέσω φωνής αλλά μέσω και εικόνας (video). Η υποστήριξη της συγκεκριμένης επικοινωνίας πραγματοποιείται πάνω από δίκτυα μεταγωγής πακέτου (IP) ανάλογα με την περίπτωση.

Ένα ακόμα σημαντικό κομμάτι του δικτύου IMS είναι η παρεχόμενη ποιότητα υπηρεσίας, γνωστή ως QoS. Το επίπεδο QoS διαπραγματεύεται μεταξύ του δικτύου και του τερματικού δίνοντας την δυνατότητα στους παρόχους να παρέχουν στους τελικούς χρήστες διαφορετικά επίπεδα ποιότητας υπηρεσίας. Ένα από αυτά τα επίπεδα ποιότητας υπηρεσίας είναι το εύρος ζώνης που καταλαμβάνει ο κάθε χρήστης της υπηρεσίας.

Όπως αναφέρθηκε παραπάνω τα δίκτυα παλαιότερης τεχνολογίας που υπάρχουν ήδη εγκατεστημένα από τους διάφορους τηλεπικοινωνιακούς παρόχους θα συνεχίσουν για αρκετά ακόμα χρόνια να λειτουργούν για λόγους κόστους της αντικατάστασής τους. Τα δίκτυα αυτά είναι δίκτυα PSTN και τα παλαιότερα κυψελωτά δίκτυα κινητής τηλεφωνίας. Έτσι το IMS θα πρέπει να μπορεί να συνεργαστεί με τα παραπάνω δίκτυα και να αποτελέσει το σκαλοπάτι από τα legacy δίκτυα στα δίκτυα νέας γενιάς (εικόνα 2). Ακόμα θα πρέπει να υπάρχει η δυνατότητα υποστήριξης παιότερων υπηρεσιών που είναι πολύ διαδεδομένες, όπως για παράδειγμα η περιαγωγή (roaming).

Το IMS προσφέρει την δυνατότητα στους παρόχους να εισάγουν διαφορετικές πολιτικές πρόσβασης και υπηρεσιών στους χρήστες. Οι πολιτικές αυτές χωρίζονται σε δύο γενικές κατηγορίες:

- Καθολικές πολιτικές που εφαρμόζονται σε όλους τους χρήστες.
- Ανεξάρτητες πολιτικές που εφαρμόζονται μεμονομένα σε χρήστες ή σε ομάδες χρηστών.

Καθολικές πολιτικές είναι για παράδειγμα η χρήση codecs πολυμέσων που θα υποστηρίζει το IMS δίκτυο. Τέτοιοι είναι οι G.711 και G.729 και χρησιμοποιούνται για την μετάδοση πολυμέσων.

Αντίστοιχα οι ανεξάρτητες πολτικές θα βασίζονται στα πακέτα υπηρεσίας που παρέχονται στους χρήστες. Για παράδειγμα σε κάποιους χρήστες που έχουν επιλέξει χαμηλό πακέτο θα επιτρέπονται μόνο υπηρεσίες μετάδοσης φωνής και όχι υπηρεσίες video ή ανταλλαγής μηνυμάτων.

Με το IMS η εισαγωγή νέων υπηρεσιών από τον εκάστοτε πάροχο είναι εύκολη και γρήγορη σε σχέση με το παρελθόν. Δεν χρειάζεται η πιστοποίηση της υπηρεσίας όπως συμβαίνει σε διαφορετικές περιπτώσεις, αρκεί η εξέλιξη της υπηρεσίας και η εφαρμογή της στο δίκτυο.

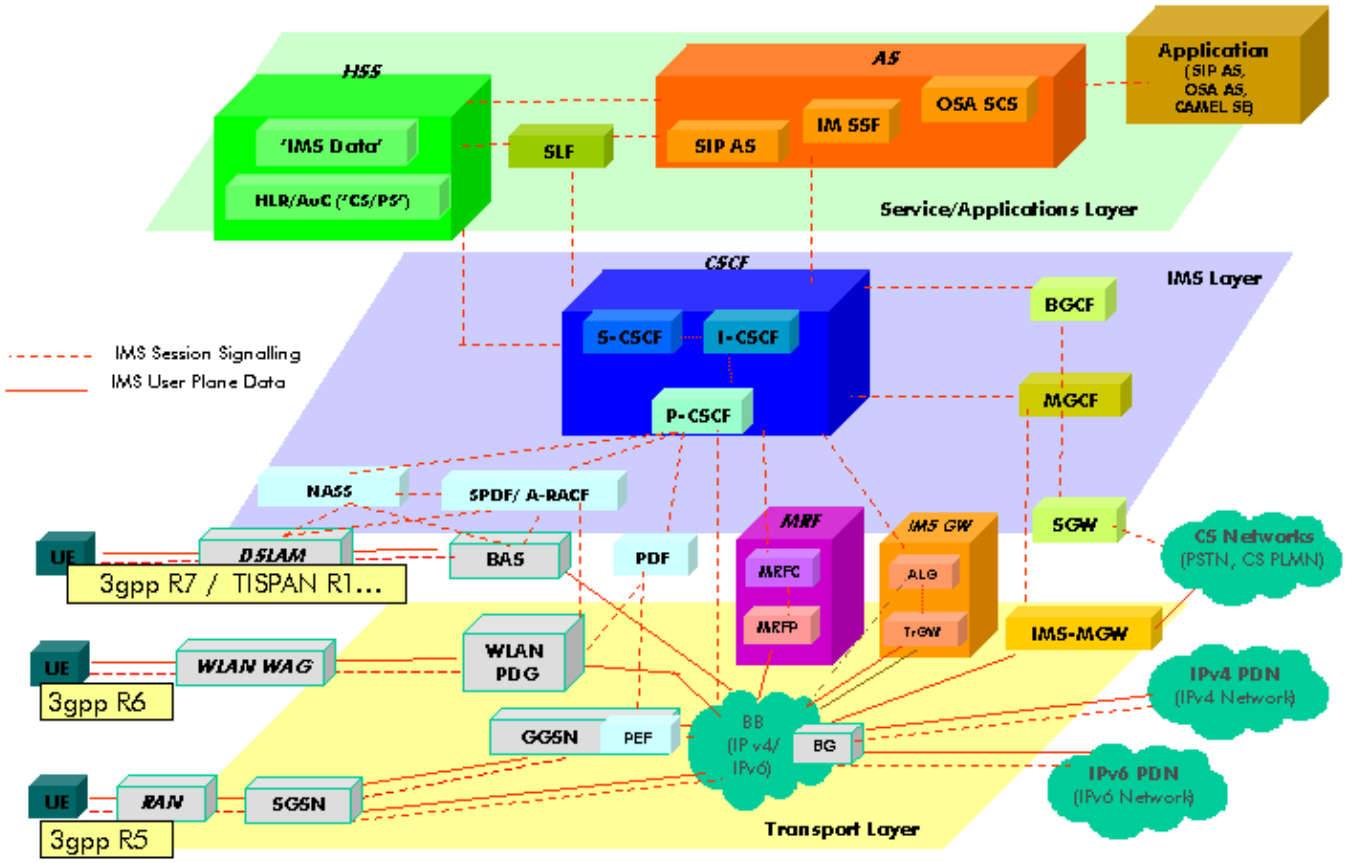
Κεφάλαιο 3

Αρχιτεκτονική του IMS

Το 3GPP έχει τυποποιήσει την αρχιτεκτονική του δικτύου IMS όπως παριστάνεται στην εικόνα 3. Ο κάθε τηλεπικοινωνιακός πάροχος ανάλογα με το μέγεθός του και τις ανάγκες του για υπηρεσίες και επεκτάσεις εφαρμόζει με τον δικό του τρόπο την αρχιτεκτονική και τις λειτουργίες που έχει τυποποιήσει το 3GPP.

Οι βασικές οντότητες του IMS είναι οι εξής:

- Τερματικός εξοπλισμός UE (User Equipment)
- Βάσεις συνδρομητών HSS (Home Subscriber Server) και SLF (Subscriber Location Function)
- SIP Servers CSCF (Call Session Control Function)
- AS (Application Servers)
- MRF (Media Resource Function)
- BGCF (Breakout Gateway Control Function)
- SGW (Signaling Gateway)
- MGCF (Media Gateway Controller Funtion)
- MGW (Media Gateway)



Εικόνα 3. Αρχιτεκτονική IMS

3.2 Βάσεις Συνδρομητών HSS και SLF

Η HSS (Home Subscriber Server) αποτελεί την κύρια βάση δεδομένων των χρηστών του δικτύου IMS. Υποστηρίζει όλες τις υπόλοιπες οντότητες του IMS οι οποίες διαχειρίζονται κλήσεις.

Περιέχει της σχετικές με τους χρήστες πληροφορίες (subscriber profiles) και διενεργεί λειτουργίες αυθεντικοποίησης και εξουσιοδότησης αυτών. Μπορεί να παρέχει στο δίκτυο πληροφορίες την τοποθεσία των χρηστών αλλά και για τις IP διευθύνσεις τους.

Η βάση SLF (Subscriber Location Function) χρησιμοποιείται σε περίπτωση που το δίκτυο διαθέτει πολλές HSS και σε αυτή αποθηκεύονται οι πληροφορίες αντιστοίχισης IP συνδρομητών με την αντίστοιχη HSS.

3.2.1 Ταυτότητες Χρηστών

Το IMS χρησιμοποιεί ταυτότητες χρηστών διαφόρων τύπων. Αυτές είναι:

- IP Multimedia Private Identity (IMPI)
- IP Multimedia Public Identity (IMPU)
- Globally Routable User Agent URI (GRUU)
- Wildcarded Public User Identity

Οι δύο πρώτοι τύποι ταυτότητας αποτελούνται από Uniform Resource Identifier (URIs), που μπορεί να είναι είτε ψηφία (πχ +30 2310 123456) ή αλφαριθμητικά της μορφής sip:user@ims.com.

Η IMPI (IP Multimedia Private Identity) αποτελεί την μοναδική και μόνιμη ταυτότητα του χρήστη και του ανατίθεται από τον πάροχο του IMS δικτύου. Χρησιμοποιείται κατά την εγγραφή του χρήστη στο δίκτυο (registration), κατά την εξουσιοδότηση του χρήστη, την διαχείρισή του από το δίκτυο και κατά την χρέωσή του. Κάθε χρήστης του IMS δικτύου έχει μια IMPI.

Η IP Multimedia Public Identity (IMPU) χρησιμοποιείται από οποιοδήποτε χρήστη του IMS για να αιτηθεί υπηρεσίες σε άλλους χρήστες. Μπορεί να υπάρχουν πολλαπλές IMPU για κάθε IMPI. Η IMPU μπορεί να διαμοιραστεί και με άλλο τηλέφωνο, έτσι ώστε όλοι να μπορούν να επικοινωνούν μέσω αυτής σε πολλαπλά τηλεφωνικά νούμερα. Ένα τέτοιο παράδειγμα είναι η χρήση ενός κοινού αριθμού κλήσης για μια ολόκληρη οικογένεια όπου κάθε μέλος έχει διαφορετικά τηλεφωνικά νούμερα.

Η Globally Routable User Agent URI (GRUU) είναι μια ταυτότητα που ταυτοποιεί μοναδικά έναν συνδιασμό IMPU και τερματικού χρήστη. Υπάρχουν δύο τύποι GRUU:

- Public-GRUU (P-GRUU)
- Temporary GRUU (T-GRUU)

Η P-GRUU αποκαλύπτουν την IMPU και είναι μακράς χρήσης. Η T-GRUU δεν αποκαλύπτουν την IMPU και είναι έγκυρες μέχρι η επαφή να απεγγραφεί από το δίκτυο (de-registered) ή μέχρι να λήξει η τρέχουσα εγγραφή (registration).

Globally Routable User Agent URI (GRUU) is an identity that identifies a unique combination of IMPU and UE instance. There are two types of GRUU: Public-GRUU (P-GRUU) and Temporary GRUU (T-GRUU).

Και τέλος με τις ταυτότητες χρηστών Wildcarded Public User Identity εκφράζεται ένα σύνολο από IMPU που αποτελούν μια ομάδα.

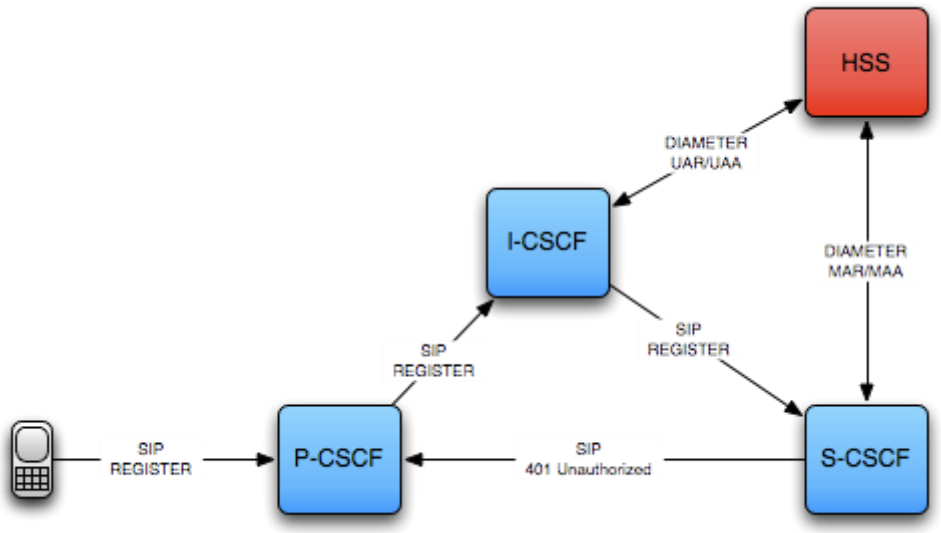
Στην HSS αποθηκεύονται οι IMPU, IMPI, IMSI, MSISDN, subscriber service profiles, service triggers καθώς και άλλες πληροφορίες για τους χρήστες.

3.3 Call Session Control Function (CSCF)

Ο Call Session Control Function (CSCF) αποτελεί έναν SIP server και είναι κεντρική οντότητα του πυρήνα των δικτύων IMS. Βασική λειτουργία του είναι να διαχειρίζεται την σηματοδοσία SIP του δικτύου.

Υπάρχουν τρείς λειτουργίες που διατελεί ένας CSCF. Κάθε μία λειτουργία μπορεί, ανάλογα με τον σχεδιασμό του δικτύου να αποτελεί και διαφορετικό κόμβο ή μπορεί ένας κόμβος CSCF να διενεργεί και τους τρείς συνολικά διαφορετικούς ρόλους. Οι κόμβοι CSCF χωρίζονται στους εξής:

- Proxy CSCF (P-CSCF)
- Interrogation CSCF (I-CSCF)
- Serving CSCF (S-CSCF)



Εικόνα 4. Οι κόμβοι CSCF

3.3.1 Proxy CSCF

Ο Proxy CSCF αποτελεί το πρώτο κόμβο μεταξύ του τερματικού χρήστη και του IMS Core για την μεταφορά της σηματοδοσίας SIP. Όλη η επικοινωνία σε επίπεδο σηματοδοσίας από το τερματικό του χρήστη προς το IMS ή από το IMS προς το τερματικό περνάει από τον proxy CSCF. Βασική του λειτουργία είναι η σωστή προώθηση των μηνυμάτων στο εσωτερικό του IMS ή στον χρήστη αντίστοιχα. Πολλά δίκτυα χρησιμοποιούν ένα επιπλέον κόμβο μεταξύ του IMS και των χρηστών, τον Session Border Controller (SBC) κυρίως για λόγους ενισχυμένης ασφάλειας του δικτύου.

Ο P-CSCF πέραν από τις λειτουργίες διαμεσολάβησης εμπεριέχει και λειτουργίες ασφάλειας του δικτύου (σε περίπτωση απουσίας κόμβου SBC). Οι λειτουργίες αυτές περιλαμβάνουν την αυθεντικοποίηση του χρήστη μέσω της ταυτότητάς του. Η λειτουργία αυτή πραγματοποιείται εκ μέρους όλου του IMS δικτύου. Έτσι αποφορτίζονται οι υπόλοιποι κόμβοι από αυτή τη διαδικασία καθώς η ταυτότητα του χρήστη είναι πλέον πιστοποιημένη. Ακόμα σε επίπεδο ασφάλειας, ο P-CSCF, ελέγχει την ορθότητα των μηνυμάτων SIP που εισέρχονται στο δίκτυο επιτρέποντας επιθέσεις με malformed πακέτα SIP ή ακόμα και πιθανά λάθη στην μετάδοση.

Ένα ακόμα σημαντικό σημείο του κόμβου P-CSCF είναι ότι έχει λειτουργία απόκρυψης της εσωτερικής τοπολογίας του δικτύου IMS προς τους χρήστες (topology hiding). Οι χρήστες γνωρίζουν ή μπορούν να ανακαλύψουν μέσω DNS servers μόνο την IP διεύθυνση και απευθύνονται σε αυτόν κάθε φορά που χρειάζεται να επικοινωνήσουν. Ο proxy CSCF στην συνέχεια έχει την ευθύνη για μεταφορά των μηνυμάτων στον σωστό κόμβο εσωτερικά του IMS. Αντίστοιχα τα μηνύματα που στέλνονται από το IMS προς το τερματικό έχουν την IP διεύθυνση του P-CSCF και όχι του κόμβου απ’ όπου ξεκίνησαν. Αυτή την διεργασία την εκτελεί ο P-CSCF.

Συνοψίζοντας οι λειτουργίες του P-CSCF είναι οι εξής:

- Σε κάθε τερματικό χρήστη ορίζεται ένας P-CSCF και δεν αλλάζει για όλη την διάρκεια του registration.
- Αποτελεί τον διαμεσολαβητή όλης της επικοινωνίας σηματοδοσίας. Τα τερματικά αγνοούν όλα τα μηνύματα που δεν προέρχονται από τον P-CSCF.
- Παρέχει την αυθεντικοποίηση του χρήστη.
- Εφαρμόζει κατά περίπτωση IPSec ή TLS στην επικοινωνία με το τερματικό. Έτσι αποφεύγονται επιθέσεις τύπου spoofing ή επιθέσεις replay και προστατεύεται η ιδιωτικότητα του χρήστη.
- Ανιχνεύει την σηματοδοσία και διασφαλίζει ότι τα τερματικά δεν θα στείλουν μηνύματα που δεν υπακούουν στους κανόνες δρομολόγησης που επιβάλει το δίκτυο.
- Μπορεί να εφαρμόσει λειτουργίες συμπίεσης των SIP μηνυμάτων.
- Μπορεί να εφαρμόσει πολιτικές Policy Decision Function (PDF) οι οποίες χρησιμοποιούνται για QoS της υπηρεσίας (έλεγχος πολιτικής, έλεγχος εύρους ζώνης κτλ).
- Παράγει αρχεία χρέωσης των χρηστών.

3.3.2 Interrogating CSCF

Ο Interrogating CSCF (I-CSCF) αποτελεί μια ακόμα έναν κόμβο SIP του δικτύου IMS. Η IP του διαφημίζεται από έναν εσωτερικό DNS Server έτσι ώστε να μπορούν οι υπόλοιποι κόμβοι να επικοινωνούν μαζί του. Ο DNS αυτός αποτελεί διαφορετικό

server από αυτόν που χρησιμοποιείται από τις τερματικές συσκευές για την ανακάλυψη του P-CSCF, ο οποίος είναι εξωτερικός του δικτύου (external DNS) για λόγους ασφάλειας της τοπολογίας. Προωθεί τα μηνύματα SIP από το P-CSCF στους κατάλληλους κόμβους του IMS. Συγκεκριμένα:

- Στέλνει ερωτήματα στην HSS για να ανακτήσει την διεύθυνση του S-CSCF που έχει ανατεθεί στον εκάστοτε χρήστη.
- Προωθεί στη συνέχεια τα μηνύματα στην στον κατάλληλο S-CSCF.
- Μπορεί να διατελέσει λειτουργίες topology hiding σε περίπτωση που δεν έχει αναλάβει αυτή τη λειτουργία ο P-CSCF ή ο SBC (αν υπάρχει στο δίκτυο).

Χρησιμοποιεί πέραν του πρωτοκόλλου SIP και το πρωτόκολλο Diameter για την επικοινωνία με την HSS.

3.3.3 Serving CSCF

Ο Serving CSCF (S-CSCF) αποτελεί κεντρικό κόμβο του IMS για την διαχείριση της σηματοδοσίας. Αποτελεί έναν εξυπηρετητή SIP αλλά έχει παράλληλα και λειτουργίες ελέγχου συνόδου. Βρίσκεται πάντα στο home δίκτυο και επικοινωνεί με την HSS για να κατεβάζει τα προφίλ των συνδρομητών. Χρησιμοποιεί πέραν του πρωτοκόλλου SIP και το πρωτόκολλο Diameter για την επικοινωνία με την HSS για να κατεβάσει τα προφίλ των χρηστών και για να δημιουργήσει τα user-to-S-CSCF associations. Τα προφίλ των χρηστών που αποθηκεύονται στον S-CSCF χρησιμοποιούνται μόνο για διαχειριστικούς λόγους και δεν αλλάζουν. Σε περίπτωση που αλλάξει κάτι στο προφίλ του συνδρομητή τότε κατεβαίνει εκ νέου από την HSS, όπου και γίνεται η αλλαγή.

Οι λειτουργίες που διενεργεί ο S-CSCF είναι οι εξής:

- Διαχειρίζεται τα μηνύματα σηματοδοσίας που έχουν να κάνουν με το SIP registration. Κατά την διαδικασία αυτή γίνεται και ο καθορισμός θέσης του συνδρομητή (πχ διεύθυνση IP συνδρομητή) και ο συνδυασμός αυτής της θέσης με την διεύθυνση SIP.
- Αποτελεί ενδιάμεσο κόμβο για όλη την σηματοδοσία του IMS και μπορεί να διαχειρίζεται όλα τα μηνύματα που ανταλλάσσονται.
- Αποφασίζει σε ποιόν Application Server θα προωθηθεί το κάθε μήνυμα SIP για να δοθούν τελικά οι κατάλληλες υπηρεσίες.
- Παρέχει υπηρεσίες δρομολόγησης κλήσεων χρησιμοποιώντας την βάση ENUM (Electronic Numbering) μέσω ENUM lookups.
- Επιβάλει πολιτικές του παρόχου σε όλους τους χρήστες.

Υπάρχει δυνατότητα να χρησιμοποιηθούν πολλές S-CSCF στο IMS δίκτυο για λόγους κατανομής φόρτου (laod distribution) αλλά και υψηλής διαθεσιμότητας του δικτύου λόγω του πολύ σημαντικού ρόλου που διατελεί. Είναι ρόλος της HSS

να αναθέσει S-CSCF στους χρήστες όταν διερωτάται από τον I-CSCF. Ο ορισμός αυτός μπορεί να γίνει μέσω capabilities που αντιστοιχίζονται μεταξύ συνδρομητή και S-CSCF.

3.4 Application Server

Οι κόμβοι τύπου application server φιλοξενούν και διαχειρίζονται τις υπηρεσίες των χρηστών του δικτύου IMS. Επικοινωνούν με την οντότητα S-CSCF χρησιμοποιώντας το πρωτόκολλο SIP και με την HSS μέσω του πρωτοκόλλου Diameter.

Οι υπηρεσίες που φιλοξενούν οι application servers μπορεί να είναι προωθήσεις κλήσεων φραγές και πολλές άλλες οι οποίες μπορούν να εισαχθούν κατά βούληση του διαχειριστή χωρίς κάποια έγκριση ή πιστοποίηση. Παρέχουν δηλαδή υπηρεσίες πέραν των βασικών υπηρεσιών του IMS, όπως για παράδειγμα είναι η υπηρεσία κλήσης φωνής.

Οι AS και βρίσκονται στο home δίκτυο των παρόχων και μπορούν να είναι πολλοί για λόγους διαχείρισης του φόρτου εργασίας αλλά και για την υψηλή διαθεσιμότητα των υπηρεσιών. Συνήθως υπάρχουν περισσότεροι του ενός AS, για λόγους load balancing αλλά και για παροχή ποικίλων υπηρεσιών.

3.5 Media Server

Οι Media Servers (MS) αποτελούν κόμβους που διαχειρίζονται τα πολυμέσα του δικτύου. Τέτοια πολυμέσα είναι οι τόνοι κλήσης, τα ηχογραφημένα μηνύματα και άλλα.

Κάθε Media Server χωρίζεται σε δύο ρόλους, τον Media Resource Function Controller (MFRC) και τον Media Resource Function Processor (MRFP).

Η MRFC αποτελεί μια λειτουργία διαχείρισης της σηματοδοσίας των S-CSCF και AS με σκοπό να ελέγχει τον MRFP. Ο MRFP από την μεριά του εκτελεί λειτουργίες διαχείρισης των πολυμέσων. Μπορεί επίσης να ελέγχει την πρόσβαση σε διαμοιραζόμενα πολυμέσα.

3.6 Breakout Gateway Control Function

Ο κόμβος Breakout Gateway Control Function (BGCF) αποτελεί έναν κόμβο τύπου SIP proxy που επεξεργάζεται αιτήματα δρομολόγησης μέσω ενός S-CSCF όταν διαπιστωθεί από την βάση ENUM/DNS ότι δεν βρίσκεται εντός δικτύου και πρέπει να αποσταλεί σε εξωτερικό δίκτυο. Τέτοια δίκτυα μπορεί να είναι διαφορετικής τεχνολογίας, όπως για παράδειγμα τα PSTN δίκτυα. Η δρομολόγηση γίνεται βάση τηλεφωνικών αριθμών.

Η βασικοί ρόλοι του κόμβου BGCF είναι:

- Να εντοπίσει το σωστό δίκτυο στο οποίο πρέπει να γίνει μεταγωγή κυκλώματος για την δρομολόγηση της κλήσης.
- Να εντοπίσει την κατάλληλη πύλη PSTN

3.7 PSTN Gateway

Η πύλη PSTN παρέχει την διεπαφή του δικτύου IMS με τα δίκτυα παλαιότερης γενιάς PSTN με σκοπό να δρομολογεί αλλά και να δέχεται κλήσεις από αυτά τα δίκτυα. Ο ρόλος της PSTN Gateway είναι ιδιαίτερα σημαντικός καθώς επιτρέπει την συνδεσιμότητα των δικτύων IMS με τα πολύ διαδεδομένα δίκτυα PSTN.

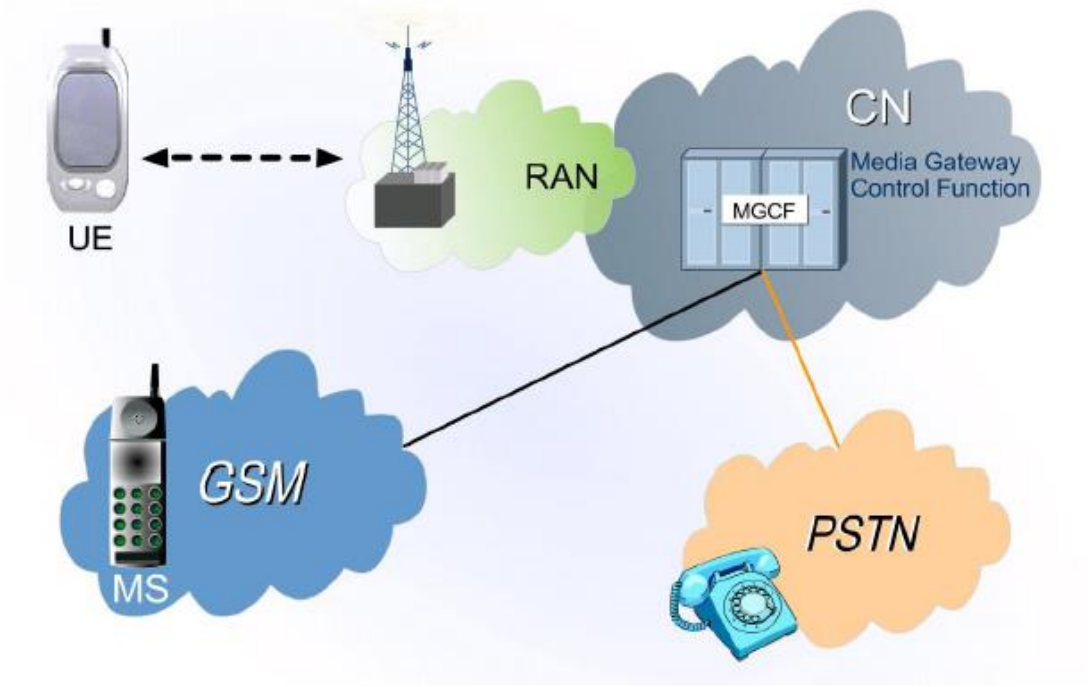
Για την διακίνηση της σηματοδοσίας, οι PSTN Gateways μετατρέπουν το πρωτόκολλο SIP over IP σε ISUP (ISDN User Part) ή SS7 over MTP (Message Transfer Part).

Για την διακίνηση της φωνής χρησιμοποιείται το πρωτόκολλο RTP (real time protocol) από την μεριά του IMS και μετατρέπεται σε Pulse-code modulation (PCM) από την μεριά του PSTN και αντίστροφα.

Οι πύλες PSTN διαθέτουν μια διεπαφή Signaling Gateway (SGW) η οποία κάνει την μετατροπή των παραπάνω πρωτοκόλλων μεταξύ των δικτύων.

Κεντρική οντότητα της πύλης PSTN αποτελεί ο Media Gateway Control Function (MGCF). Πραγματοποιεί την παραπάνω μετατροπή πρωτοκόλλων που περιγράφηκε και πραγματοποιεί την αντιστοίχησή τους. Πραγματοποιεί και έλεγχο των πόρων του Media Gateway.

Η οντότητα Media Gateway (MGW) πραγματοποιεί την διεπαφή των πολυμέσων μεταξύ IMS και PSTN δίκτυο. Επιπρόσθετα μετατρέπει τα codecs που χρησιμοποιεί το IMS σε αυτά των PSTN δικτύων και αντίστροφα (Εικόνα 5).



Εικόνα 5. MGCF και λειτουργία

3.8 Home and Visited Networks

Καθώς το IMS δίκτυο αποτελεί εξέλιξη των ήδη υπαρχουσών τεχνολογιών τηλεπικοινωνιακών δικτύων, έτσι χρησιμοποιεί την φιλοσοφία πολλών από αυτά. Έτσι και στην περίπτωση του IMS έχουμε την λογική του home και visited δικτύων, όπως υπάρχει και στα δίκτυα GSM και GPRS.

Στην περίπτωση των κυψελωτών δικτύων κινητής τηλεφωνίας, όταν ο χρήστης κινείται εντός εμβέλειας του παρόχου υπηρεσίας τότε βρίσκεται στο home δίκτυο. Σε περίπτωση που κινηθεί εκτός κάλυψης τότε χρησιμοποιεί τις κυψέλες άλλου παρόχου οπότε βρίσκεται στο visited δίκτυο. Και στις δύο περιπτώσεις η επικοινωνία είναι συνεχής και ο χρήστης δεν βλέπει διαφορά στην παροχή της υπηρεσίας. Η διαφοροποίηση βρίσκεται στις συμφωνίες μεταξύ των παρόχων για την διασύνδεση μεταξύ των δικτύων τους και την ομαλή δρομολόγηση των κλήσεων.

Αυτή την φιλοσοφία δανείζεται και το δίκτυο IMS μέσω του κόμβου P-CSCF ο οποίος είναι και ο μόνος που μπορεί να εγκατασταθεί και στο home δίκτυο αλλά και στο visited.

3.9 Πρωτόκολλα Επικοινωνίας

Το IMS δίκτυο, όπως αναφέρθηκε και παραπάνω, δημιουργήθηκε μέσα από την εξέλιξη και χρησιμοποίηση των ήδη υπαρχουσών τεχνολογιών, που γνωρίζουν

μεγάλη δημοτικότητα και είναι εκτενώς δοκιμασμένα και αποδεκτά από την τεχνολογική κοινότητα.

Έτσι και στο κομμάτι των πρωτοκόλλων επικοινωνίας, το IMS χρησιμοποιεί για τους σκοπούς του ήδη γνωστά και δημοφιλή πρωτόκολλα.

3.9.1 Session Initiation Protocol (SIP)

Για τον έλεγχο συνόδου στα IMS δίκτυα έχει επιλεγεί το πρωτόκολλο SIP. Το SIP είναι ένα ευρέως διαδεδομένο πρωτόκολλο ελέγχου συνεδριών για μετάδοση φωνής πάνω από τα IP δίκτυα και δυνατό του σημείο αποτελεί η απλότητά του στην διαχείριση, στον φόρτο που επιβάλει στο δίκτυο αλλά και στην εισαγωγή νέων υπηρεσιών.

Το πρωτόκολλο SIP βρίσκεται στο επίπεδο υπηρεσιών κατά OSI. Δουλεύει σε συνεργασία με διάφορα πρωτόκολλα χαμηλότερων επιπέδων όπως το Session Description Protocol (SDP), το Real-time Transport Protocol (RTP) και το Internet Protocol (IP). Για την ασφάλεια της μεταδιδόμενης πληροφορίας δύναται να χρησιμοποιήσει κρυπτογράφηση με το Transport Layer Security (TLS).

Το SIP βασίζεται στο μοντέλο request/response του πρωτοκόλλου HTTP. Για κάθε ανάγκη επικοινωνίας δημιουργείται ένα αίτημα (request) το οποίο προκαλεί από το δεύτερο μέρος της επικοινωνίας μια τουλάχιστον απάντηση (response). Το SIP δανείζεται πολλά πεδία επικεφαλίδας από το HTTP βοηθώντας στην απλότητα διαχείρισης.

Example of SIP Message Request

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060
 ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>
 ;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4
client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Εικόνα 6. Παράδειγμα μηνύματος SIP

Κάθε πόρος ενός δικτύου SIP (πχ τερματικό χρήστη, υπηρεσίες) διαθέτουν ένα μοναδικό χαρακτηριστικό, το SIP URI (uniform resource identifier). Η σύνταξή του βασίζεται στην γενική προτυποποίηση που ακολουθούν και τα ηλεκτρονικά ταχυδρομεία και οι υπηρεσίες διαδικτύου και είναι της μορφής sip:user:password@host:port. Το "sip:" ορίζει την ύπαρξη του URI scheme που ακολουθεί. Σε περίπτωση που χρησιμοποιείται ασφάλεια στην μετάδοση τότε το scheme ξεκινάει με "sips:" για να υποδηλώσει ότι σε κάθε κόμβο που προωθείται το μήνυμα χρησιμοποιείται ο μηχανισμός ασφάλειας Transport Layer Security (TLS) για όλο το μονοπάτι επικοινωνίας. Ο μηχανισμός TLS προστατεύει από επιθέσεις man-in-the middle πάνω στο κανάλι σηματοδοσίας. Δεν μας παρέχει ασφάλεια από άκρο σε άκρο καθώς εφαρμόζεται για την μετάδοση από τον ένα κόμβο στον άλλο κάθε φορά για όλο το μονοπάτι. Αυτό προϋποθέτει ότι όλοι οι ενδιάμεσοι κόμβοι είναι έμπιστοι.

Το SIP είναι πρωτόκολλο επιπέδου εφαρμογής και ως εκ τούτου χρησιμοποιεί πολλά πρωτόκολλα χαμηλότερων επιπέδων από αυτό. Συνήθως χρησιμοποιούνται τα πρωτόκολλα UPD (πόρτα 5060), RTP (Real-time Transport Protocol) και TLS (πόρτα 5061).

Το SIP χρησιμοποιείται για τους παρακάτω σκοπούς:

- Εγκατάσταση και τερματισμός κλήσεων φωνής και video.
- Διαχείριση των κλήσεων.
- Τροποποίηση εγκαθιδρυμένων κλήσεων (αλλαγή πορτών, IP, εισαγωγή επιπλέον χρήστη στην συνομιλία κα).
- Μετάδοση μηνυμάτων (instant messaging).
- Διαχείριση της μετάδοσης των πολυμέσων.

Στόχος του SIP είναι να πετύχει την παροχή της απαιτούμενης σηματοδοσίας για την χρήση υπηρεσιών φωνής σε IP δίκτυα με λειτουργίες αντίστοιχες των δικτύων PSTN και του πρωτοκόλλου SS7. Η μεγάλη διαφοροποίηση μεταξύ των δύο έγκειται στο γεγονός ότι το SS7 είναι κεντροποιημένο πρωτόκολλο, δηλαδή βασίζεται σε ένα σύνθετο κεντρικό δίκτυο, όπου και συγκεντρώνεται η ευφυΐα του συστήματος και τερματικά με χαμηλές δυνατότητες. Αντίθετα το SIP αποτελεί ένα πρωτόκολλο peer-to-peer, χρησιμοποιώντας ένα απλό δίκτυο κορμού και μεταφέροντας την ευφυΐα του συστήματος στα άκρα του δικτύου (τερματικές συσκευές και εξυπηρετητές). Έτσι όλες οι δυνατότητες στην περίπτωση του SS7 βρίσκονται στο δίκτυο ενώ στο SIP στα τερματικά.

Τα μηνύματα του SIP είναι κωδικοποιημένα και ακολουθούν την παρακάτω αρίθμηση ανά κατηγορία:

- Provisional (1xx): Τα αιτήματα έχουν ληφθεί και βρίσκονται υπό επεξεργασία.

- Success (2xx): Η ενέργεια λήφθηκε με επιτυχία, ήταν ορθή και αποδεκτή.
- Redirection (3xx): Υπάρχει ανάγκη λήψης επιπλέων ενεργειών (συνήθως από τον αποστολέα) με σκοπό να ολοκληρωθεί το αίτημα.
- Client Error (4xx): Το αίτημα περιέχει λάθος στην σύνταξη ή δεν μπορεί να εκπληρωθεί από τον εξυπηρετητή.
- Server Error (5xx): Ο εξυπηρετητής απέτυχε να ικανοποιήσει ένα ορθό αίτημα.
- Global Failure (6xx): Το αίτημα δεν μπορεί να ικανοποιηθεί από κανέναν εξυπηρετητή.

Μερικά βασικά μηνύματα του SIP παρουσιάζονται παρακάτω:

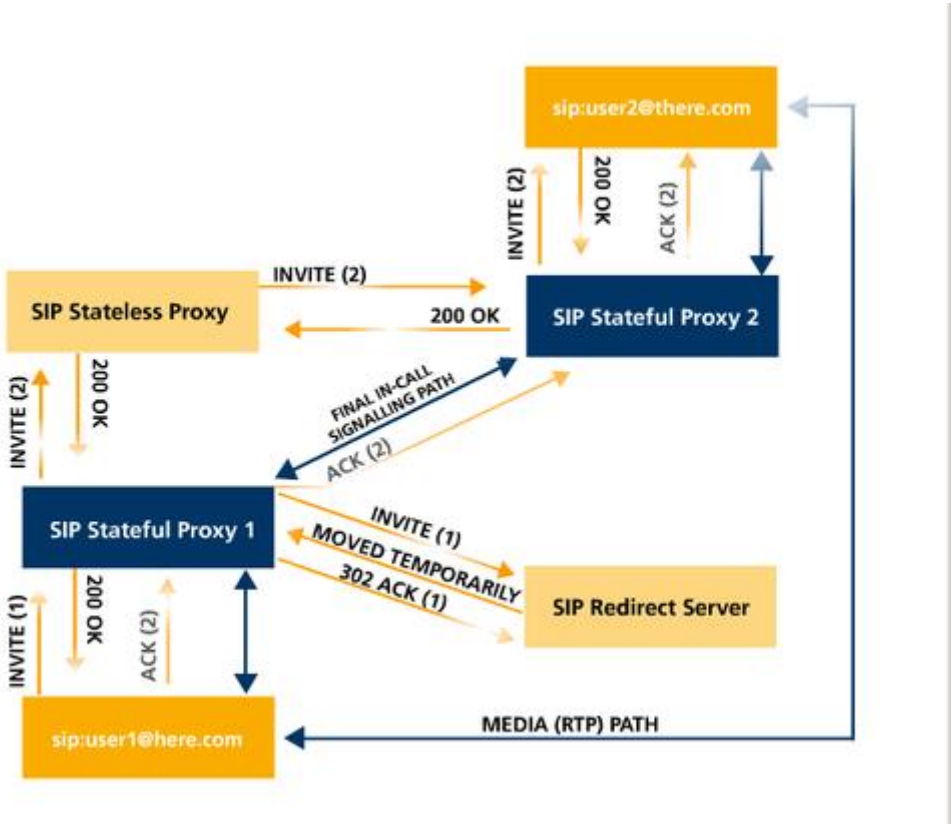
- REGISTER: Χρησιμοποιείται από ένα UA για να υποδείξει την τρέχουσα διεύθυνση IP που διαθέτει και το URI στο οποίο επιθυμεί να δέχεται κλήσεις.
- INVITE: Χρησιμοποιείται για να εγκαθιδρύσει μια συνεδρία πολυμέσων μεταξύ των UAs.
- ACK: Χρησιμοποιείται για την επιβεβαίωση σωστής ανταλλαγής μηνυμάτων.
- CANCEL: Τερματίζει ένα τρέχων αίτημα.
- BYE: Τερματίζει μια συνεδρία μεταξύ δύο χρηστών που συνομιλούν.
- OPTIONS: Αιτείται πληροφορίες σχετικά με τις δυνατότητες ενός καλούντα, χωρίς να ιδρύσει κλήση.
- PRACK (Provisional Response Acknowledgement): Τα μηνύματα PRACK βελτιώνουν την αξιοπιστία του δικτύου βάζοντας επιβεβαίωση λήψης στα μνήματα Responses (1xx). Αποστέλλεται ως απάντηση στα μηνύματα αυτά.

Το SIP χρησιμοποιεί δικούς του μηχανισμούς με σκοπό την αξιόπιστη μεταφορά των δεδομένων του (transactions). Έτσι ορίζεται η κατάσταση κάθε επικοινωνίας (internal state) καθώς επίσης γίνεται και χρήση timers.

Οι πελάτες στέλνουν αιτήματα και οι εξυπηρετητές απαντούν σε αυτά τα αιτήματα με ένα ή περισσότερα μηνύματα. Οι αποκρίσεις αυτές μπορούν να είναι μηνύματα Provisional (1xx) και ένα ή περισσότερα μηνύματα τερματισμού (2xx-6xx).

Ένα ακόμα χαρακτηριστικό της ανταλλαγής μηνυμάτων είναι ότι μπορούν να είναι μηνύματα invite και non-invite. Η διαφορά μεταξύ των δύο αυτών κατηγοριών είναι ότι στην πρώτη περίπτωση μπορεί να γίνει δημιουργία μια μακράς επικοινωνίας, η οποία ονομάζεται διάλογος και να συμπεριλαμβάνει μηνύματα επιβεβαίωσης (ACK) ενώ η δεύτερη όχι.

Λόγω των παραπάνω το SIP μπορεί να χρησιμοποιήσει μη αξιόπιστα πρωτόκολλα χαμηλότερων επιπέδων, όπως για παράδειγμα το UDP (εικόνα 7).



Εικόνα 7. Επικοινωνία SIP

3.9.2 Diameter Protocol

Το diameter είναι ένα πρωτόκολλο τύπου authentication, authorization and accounting (AAA). Χρησιμοποιείται ως εναλλακτικό του πρωτοκόλλου RADIUS στα δίκτυα και αποτελεί εξέλιξή του.

Στο IMS το diameter χρησιμοποιείται για την επικοινωνία των κόμβων S-CSCF και I-CSCF με την βάση HSS για την ανταλλαγή των προφίλ των χρηστών του δικτύου και την πιστοποίηση αυτών όσο αφορά την αυθεντικότητά τους και την εξουσιοδότησή τους για την χρήση του δικτύου και των υπηρεσιών που προσφέρει.

3.9.3 Real Time Protocol (RTP)

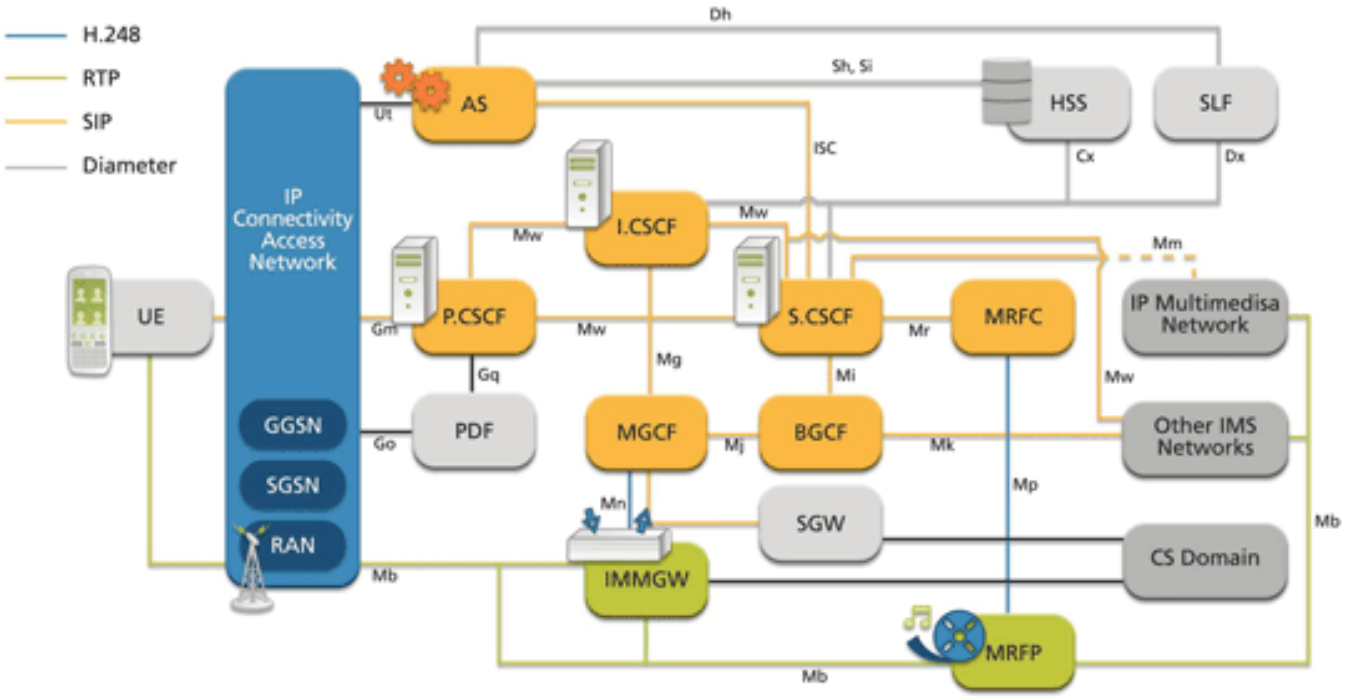
Το πρωτόκολλο Real Time Protocol (RTP) ορίζει την τυποποίηση της διάταξης των πακέτων για την μεταφορά φωνής και video πάνω στα δίκτυα IP. Χρησιμοποιείται από το IMS για την ροή των πολυμέσων.

Το RTP έχει δυνατότητα ανίχνευσης και διόρθωσης του φαινομένου jitter σε μια εισερχόμενη ροή δεδομένων.

3.9.4 Διασυνδέσεις IMS

Το IMS προσωποποιεί τις διεπαφές (interfaces) μεταξύ των διάφορων κόμβων που μπορούν να εγκατασταθούν σε αυτό. Για τις διεπαφές αυτές ορίζονται και τα πρωτόκολλα επικοινωνίας που θα χρησιμοποιούνται.

Στην εικόνα 8 εμφανίζεται η αρχιτεκτονική του IMS και οι διάφορες διεπαφές μεταξύ των κόμβων. Αντίστοιχα στον πίνακα 8 εμφανίζονται οι σημαντικότερες διεπαφές, με τα αντίστοιχα πρωτόκολλα που χρησιμοποιούνται καθώς και η περιγραφή τους για τις λειτουργίες που διατελούν.



Εικόνα 8. Διεπαφές του IMS στην αρχιτεκτονική του

Interface Name	IMS entities	Description	Protocol
Cr	MRFC, AS	Used by MRFC to fetch documents (e.g. scripts, announcement files, and other resources) from an AS. Also used for media control related commands.	TCP/SCTP channels
Cx	(I-CSCF, S-CSCF), HSS	Used to send subscriber data to the S-CSCF; including Filter criteria and their priority. Also used to furnish CDF and/or OCF addresses.	Diameter
Dh	AS (SIP AS, OSA, IM-SSF) <-> SLF	Used by AS to find the HSS holding the User Profile information in a multi-HSS environment. DH_SLF_QUERY indicates an IMPU and DX_SLF_RESP return the HSS name.	Diameter
Dx	(I-CSCF or S-CSCF) <-> SLF	Used by I-CSCF or S-CSCF to find a correct HSS in a multi-HSS environment. DX_SLF_QUERY indicates an IMPU and DX_SLF_RESP return the HSS name.	Diameter
Gm	UE, P-CSCF	Used to exchange messages between SIP user equipment (UE) or Voip Gateway and P-CSCF	SIP
ISC	S-CSCF <-> AS	Reference point between S-CSCF and AS. Main functions are to :	SIP
ISC Ici Izi	S-CSCF <-> AS IBCFs TrGWs	Supply the AS with information to allow it to execute multiple services	SIP SIP RTP
ISC Ici Izi Ma	S-CSCF <-> AS IBCFs TrGWs I-CSCF <-> AS		RTP SIP
ISC Ici Izi	S-CSCF <-> AS IBCFs TrGWs	Used to exchange messages between an IBCF and another IBCF belonging to a different IMS network.	SIP SIP RTP
ISC Ici Izi Ma Ma Mg Mi Ma Mg Mi Mj	S-CSCF <-> AS IBCFs TrGWs I-CSCF <-> AS I-CSCF <-> AS MGCF -> I,S-CSCF S-CSCF -> BGCF I-CSCF <-> AS MGCF -> I,S-CSCF S-CSCF -> BGCF BGCF -> MGCF	Used to forward media streams from a TrGW to another TrGW belonging to a different IMS network. Main functions are to: Originate a session on behalf of a user or Public Service Identity, if the AS has no knowledge of a S-CSCF assigned to that user or Public Service Identity Convey charging function addresses	RTP SIP SIP SIP
Ma Mg Mi	I-CSCF <-> AS MGCF -> I,S-CSCF S-CSCF -> BGCF	ISUP signalling to SIP signalling and forwards SIP signalling to I-CSCF	SIP
Ma Mg Mi Mj Mk Mm	I-CSCF <-> AS MGCF -> I,S-CSCF S-CSCF -> BGCF BGCF -> MGCF BGCF -> BGCF I-CSCF, S-CSCF, external IP network	Used to exchange messages between S-CSCF and BGCF Used for the interworking with the PSTN/CS Domain, when the BGCF has determined that a breakout should occur in the same IMS network to send SIP message from BGCF to MGCF Used for the interworking with the PSTN/CS Domain, when the BGCF has determined that a breakout should occur in another IMS network to send SIP message from BGCF to the BGCF in the other network Used for exchanging messages between IMS and external IP networks	SIP SIP SIP
Mn	MGCF, IM-MGW	Allows control of user-plane resources	H.248
Mx	BGCF/CSCF, IBCF	Used for the interworking with another IMS network, when the BGCF has determined that a breakout should occur in the other IMS network to send SIP message from BGCF to the IBCF in the other network	SIP SIP
Mw	P-CSCF, I-CSCF, S-CSCF, AGCF	Used to exchange messages between CSCFs. AGCF appears as a P-CSCF to the other CSCFs	SIP SIP H.248
Rf	P-CSCF, I-CSCF, S-CSCF, BGCF, MRFC, MGCF, AS	Used to exchange offline charging information with CDF	Diameter Diameter
Sh	AS (SIP AS, OSA SCS), HSS	Used to exchange User Profile information (e.g., user related data, group lists, user service related information or user location information or charging function addresses (used when the AS has not received the third party REGISTER for a user)) between an AS (SIP AS or OSA SCS) and HSS. Also allow AS to activate/deactivate filter criteria stored in the HSS on a per subscriber basis	Diameter

Εικόνα 9. Διεπαφές μεταξύ κόμβων και χρησιμοποιούμενα πρωτόκολλα

Κεφάλαιο 4

Η σηματοδοσία στο IMS

Το πιο σημαντικό κομμάτι της σηματοδοσίας που ανταλλάσσεται εντός του δικτύου IMS είναι αυτή του πρωτοκόλλου που διενεργεί τον έλεγχο των συνόδων. Όπως αναφέραμε παραπάνω το πρωτόκολλο αυτό είναι το SIP και προσθέτει τις δυνατότητες που χρειάζεται το δίκτυο για την παροχή των υπηρεσιών του. Είναι πλέον το πιο διαδεδομένο πρωτόκολλο επικοινωνίας σε υπηρεσίες VoIP μαζί με το πρωτόκολλο H.323.

Το SIP αποτελεί τον φορέα για το πρωτόκολλο SDP (Session Description Protocol). Το SDP φέρει υπηρεσίες για το IMS του τύπου όπως IP διευθύνσεις και πόρτες επικοινωνίας καθώς και χρησιμοποιούμενοι κώδικες.

Αντίστοιχα το πρωτόκολλο RTP (real time protocol) χρησιμοποιείται για την μεταφορά των πολυμέσων αποτελώντας στην ουσία τον φορέα τους.

4.1 Επίπεδο Συνόδου στο IMS

Το IMS δημιουργήθηκε με σκοπό να χρησιμοποιεί τις υφιστάμενες δικτυακές υποδομές IP, έτσι βασική προϋπόθεση για την σύνδεση ενός τερματικού είναι η σύνδεσή του πάνω στο IP δίκτυο του παρόχου.

Το δίκτυο πρόσβασης δεν είναι σημαντικό για το IMS δίκτυο καθώς μπορεί να γίνει χρήση πολλών τεχνολογιών. Μπορεί να είναι για παράδειγμα μια DSL γραμμή ή dial-up εφόσον πρόκειται για ενσύρματο δίκτυο. Στις ασύρματες επικοινωνίες μπορεί να χρησιμοποιηθεί GPRS ή WLAN.

Από τη στιγμή που θα συνδεθεί το τερματικό στο IP δίκτυο, μέσω του δικτύου πρόσβασης, τότε υπάρχει η δυνατότητα να γίνει ανακάλυψη του P-CSCF και να γίνει σύνδεση στις υπηρεσίες του IMS.

4.1.1 Απόδοση διεύθυνσης IP

Κατά την εκκίνησή του, το τερματικό του χρήστη πρέπει να λάβει μια IP διεύθυνση από το IP δίκτυο με σκοπό να συνδεθεί σε αυτό και κατ' επέκταση να συνδεθεί στο IMS.

Τον ρόλο αυτό αναλαμβάνει ένας DHCP server, ο οποίος κάνει τον ορισμό της διεύθυνσης στα τερματικά.

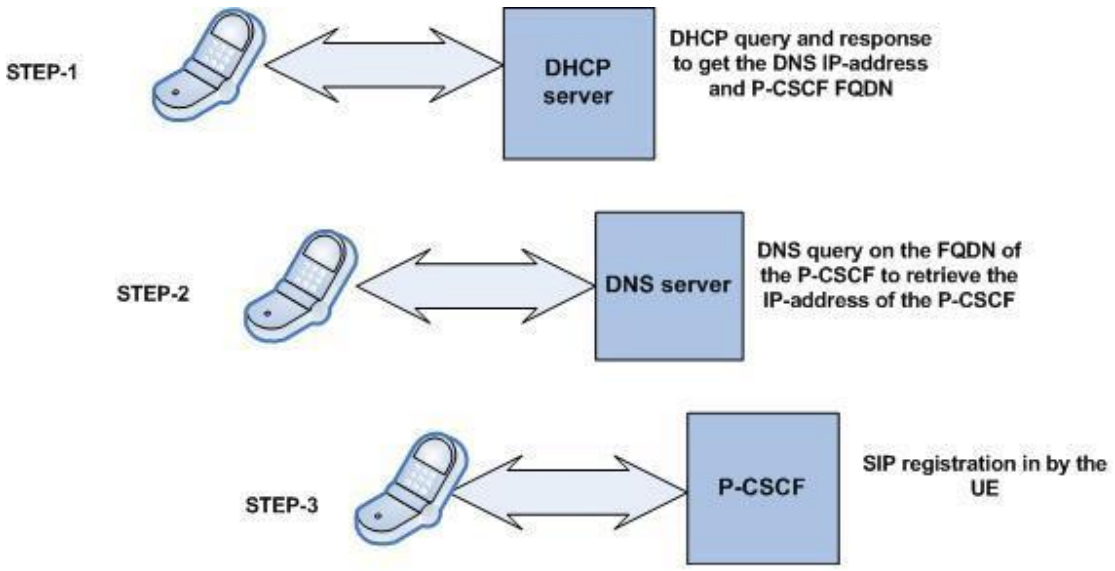
4.1.2 Ανακάλυψη του P-CSCF

Από την στιγμή που το τερματικό αποκτήσει πρόσβαση στο IP δίκτυο ξεκινάει η διαδικασία ανακάλυψης του πρώτου και μοναδικού κόμβου με τον οποίο έχει επικοινωνία, τον P-CSCF.

Στην διαδικασία αυτή λαμβάνει μέρος ο DHCP server αλλά και ένας DNS Server. Αυτοί οι εξυπηρετητές είναι ορατοί στα τερματικά (external servers) και ως εκ τούτου είναι σημαντικό να διαφοροποιούνται από τους εξυπηρετητές που χρησιμοποιούνται από τον πυρήνα του IMS (internal DHCP and DNS).

Η διαδικασία που ακολουθεί είναι η εξής (εικόνα 10):

- Το UE στέλνει ερώτημα στον external DHCP με σκοπό να ανακαλύψει την διεύθυνση του DNS και το domain του P-CSCF.
- Ο DHCP αποκρίνεται στο τερματικό με τις παραπάνω πληροφορίες.
- Το τερματικό στέλνει ερώτημα στον external DNS με σκοπό να μάθει την διεύθυνση του P-CSCF.
- Ο DNS αποκρίνεται με την IP διεύθυνση του P-CSCF.
- Το τερματικό είναι έτοιμο να στείλει το SIP registration στον P-CSCF.



Εικόνα 10. Διαδικασία Ανακάλυψης του P-CSCF

4.1.3 Εγγραφή στο δίκτυο IMS

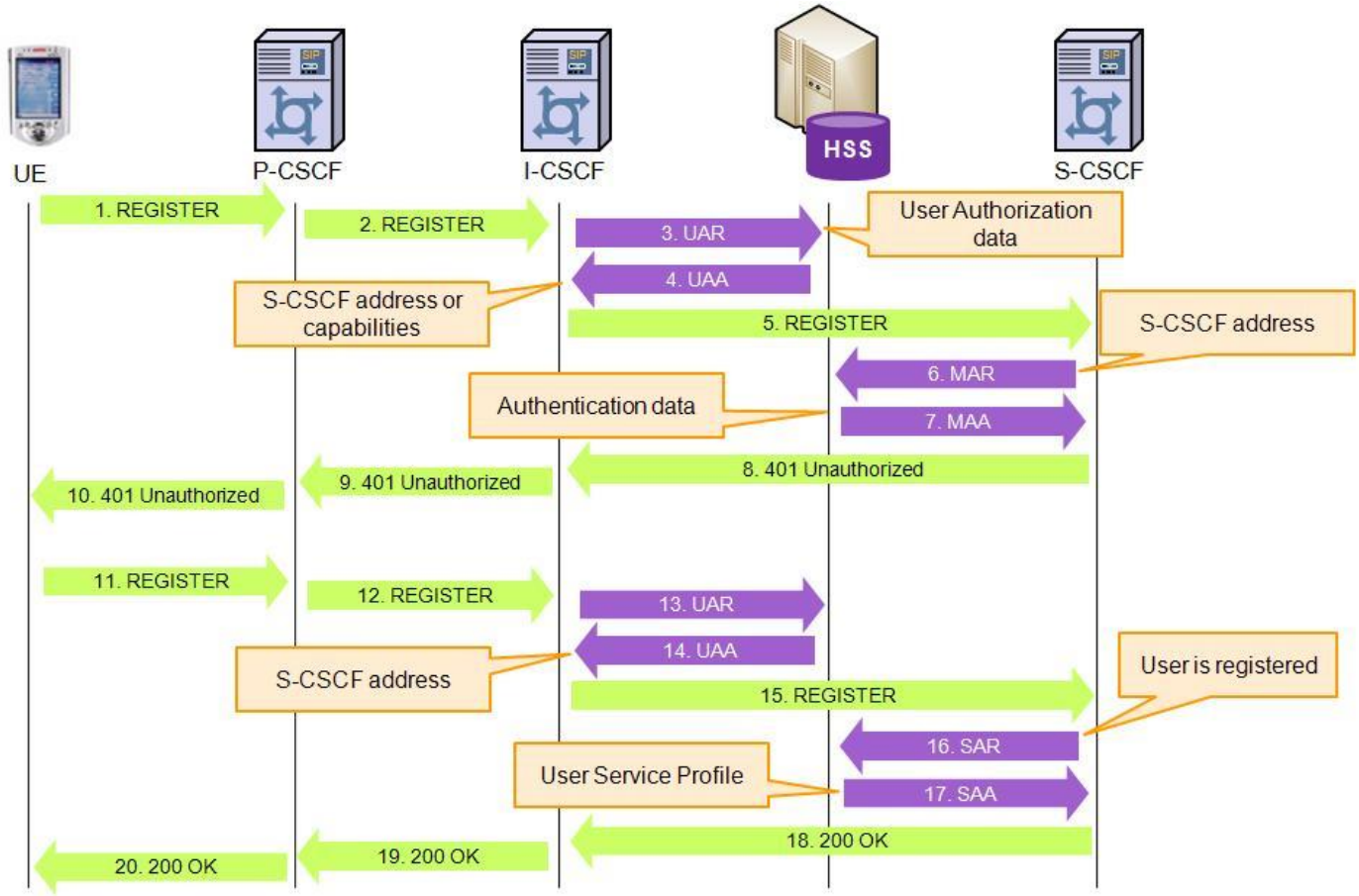
Όπως αναφέρθηκε παραπάνω όταν το τερματικό χρήστη εγγραφεί στο δίκτυο και εντοπίσει την διεύθυνση του P-CSCF είναι έτοιμο να αρχίσει την διαδικασία εγγραφής στο IMS (registration).

Κατά την διαδικασία αυτή το UE ζητάει πιστοποίηση της αυθεντικότητάς του και την εξουσιοδότησή του από το δίκτυο για τις διάφορες υπηρεσίες που παρέχει.

Η διαδικασία που ακολουθείται για την εγγραφή του χρήστη είναι η εξής (εικόνα 11):

- Το UE αποστέλλει ένα μήνυμα Register στον P-CSCF.
- Ο P-CSCF προωθεί το Register στον I-CSCF.
- Ο I-CSCF στέλνει ερώτημα μέσω Diameter στην HSS για την S-CSCF που εξυπηρετεί τον αντίστοιχο χρήστη (S-CSCF address ή capabilities).
- Στην συνέχεια ο I-CSCF προωθεί το Register στον S-CSCF.
- Ο S-CSCF στέλνει ερώτημα στην HSS για δεδομένα αυθεντικοποίησης του χρήστη καθώς και ένα μήνυμα τύπου Challenge για το σκοπό αυτό.
- Η HSS αποστέλλει τα δεδομένα αυτά στον S-CSCF.
- Ο S-CSCF αποστέλλει ένα μήνυμα 401 Unauthorized στον I-CSCF το οποίο περιέχει το challenge.
- Ο I-CSCF προωθεί το 401 unauthorized στον P-CSCF.
- Ο P-CSCF στην συνέχεια αυτός με τη σειρά αφαιρεί τα δεδομένα του δικτύου (topology hiding) στο μήνυμα και το αποστέλλει στο UE.
- Το UE αφού λάβει το μήνυμα υπολογίζει το response με βάση το challenge που έλαβε και τον μοναδικό κωδικό του και το στέλνει πίσω στον P-CSCF.
- Το response φτάνει με την ίδια διαδικασία στον S-CSCF το προωθεί στην HSS.
- Η HSS κάνει έλεγχο του response και στέλνει στον S-CSCF το προφίλ του χρήστη όπου και αποθηκεύεται.
- Τέλος ακολουθείται η ίδια διαδικασία για να αποσταλεί το μήνυμα 200 OK στο UE και να ολοκληρωθεί η εγγραφή του χρήστη στο IMS.

Σε όλες τις παραπάνω διαδικασίες χρησιμοποιείται ένας internal DNS για την ανακάλυψη της διεύθυνσης IP κάθε κόμβου από το αντίστοιχο domain που γνωρίζουν.



Εικόνα 11. IMS registration

Πριν ξεκινήσει η διαδικασία εγγραφής του χρήστη στο δίκτυο το τερματικό λαμβάνει τα απαραίτητα στοιχεία για να προσχωρήσει σε αυτή. Τα στοιχεία αυτά είναι:

- URI (Uniform Resource Identifier)
- Δημόσια ταυτότητα χρήστη (Public User Identity)
- Προσωπική ταυτότητα χρήστη (Private User Identity)
- Η IP διεύθυνση

Στη συνέχεια δημιουργείται το πακέτο REGISTER για να χρησιμοποιηθεί κατά την εγγραφή του χρήστη στο δίκτυο IMS, όπως περιγράφηκε παραπάνω. Στην εικόνα 12 παρουσιάζεται η δομή ενός μηνύματος SIP REGISTER.

Αντίστοιχα μετά το πέρας της εγγραφής επιστρέφεται το μήνυμα 200 OK το οποίο φαίνεται στην εικόνα 13.

```
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:172.26.108.161;transport=tcp SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/TCP 172.28.54.45;branch=z9hG4bK65f9c779686AC908
    ⊞ From: "1259" <sip:1259@172.26.108.161>;tag=463BD640-57F82393
    ⊟ To: <sip:1259@172.26.108.161>
      ⊞ SIP to address: sip:1259@172.26.108.161
    ⊞ CSeq: 2 REGISTER
      Call-ID: 37d19404-2c1daac7-80b264de@172.28.54.45
    ⊟ Contact: <sip:1259@172.28.54.45;transport=tcp>;methods="INVITE, .
      ⊞ Contact-URI: sip:1259@172.28.54.45;transport=tcp
        Contact parameter: transport=tcp>
        Contact parameter: methods="INVITE,
      ⊞ Contact-URI: \n
      User-Agent: PolycomSoundStationIP-SSIP_6000-UA/4.0.2.11307
      Accept-Language: en
    ⊟ Authorization: Digest username="", realm="", nonce="7d3e9be050be
        Authentication Scheme: Digest
        username=""
        realm=""
        nonce="7d3e9be050be547e5f5ae0bd1be40038b0652023C1016ADC9B0A"
        uri="sip:172.26.108.161;transport=tcp"
        response="4169c069f48e90a2e316791381d24fee"
        algorithm=MD5
      Max-Forwards: 70
      Expires: 3600
      Content-Length: 0
```

Εικόνα 12. SIP REGISTER

```
Session Initiation Protocol
    Status line:   SIP/2.0 200 OK
    Status-Code:  200
    Message Header
     Via: SIP/2.0/UDP 12.194.224.134:5060;branch=z9hG4bKm
     Call-ID: SDopf0b01-9f4f824d3dc750fde8c2db1462d304ec-cgg1e32
    CSeq: 1 INVITE
    From: "full name"<sip:******9398@12.194.224.137>;tag=123456
    To: <sip:******0461@12.194.224.134:5060>;tag=468c0
    Contact:******0461<sip:******0461@192.168.1.188:5060
    Allow: REFER,UPDATE,INFO,MESSAGE,OPTIONS
    Content-Type: application/sdp
    Content-Length: 169
Session Description Protocol
    Session Description Protocol Version (v): 0
   Owner/Creator,  Session  Id  (o):  ******0461  0  0  IN  IP4
192.168.1.188
   …
   Connection Information (c): IN IP4 192.168.1.188
   …
   Media Description, name and address(m): audio 10000 RTP/AVP 2
100
```

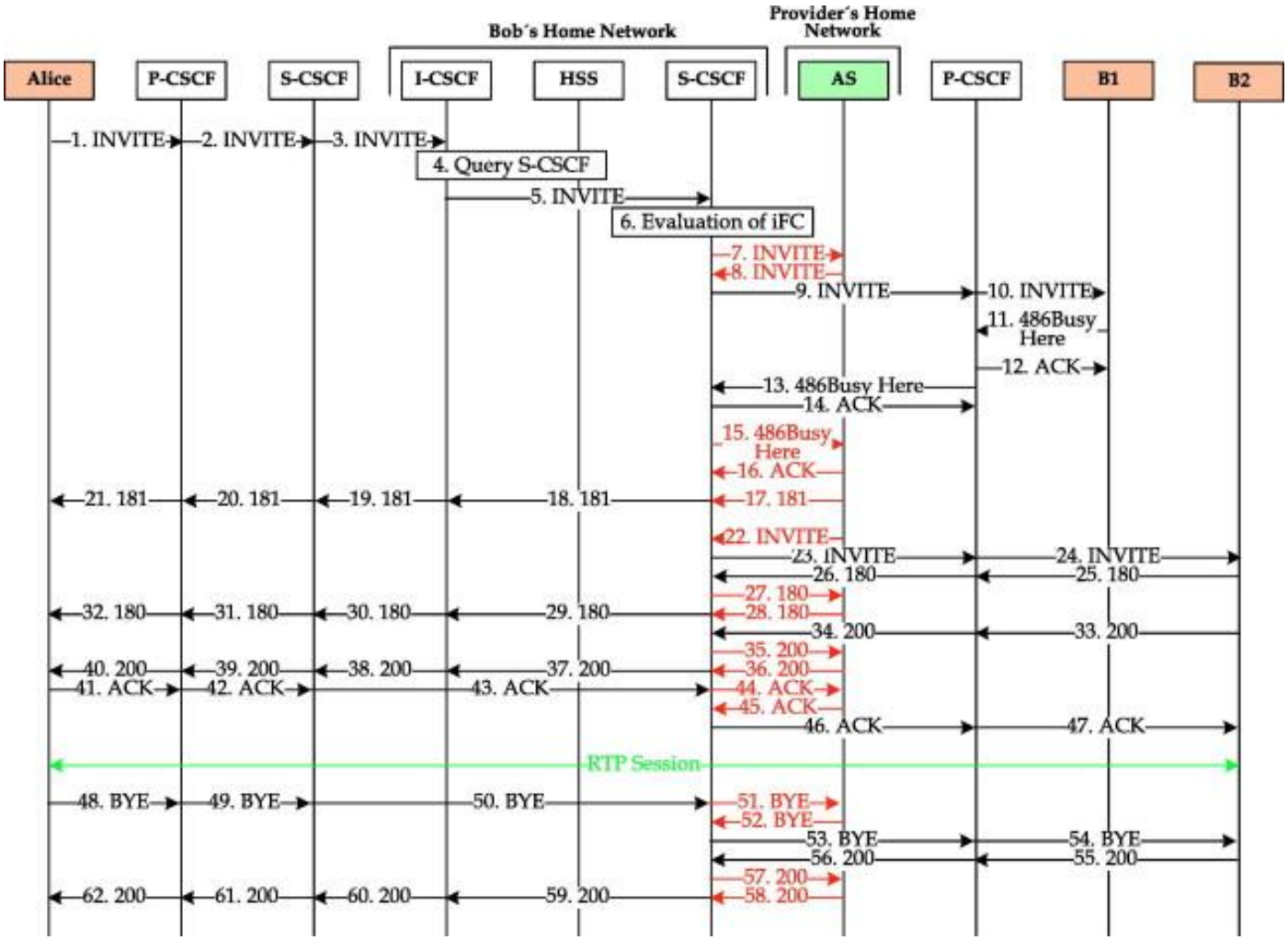
Εικόνα 13. SIP 200 OK

4.1.4 Πραγματοποίηση Κλήσης

Από την στιγμή που το τερματικό θα εγγραφεί στο δίκτυο, όπως περιγράφηκε στο προηγούμενο κεφάλαιο, είναι έτοιμο να πραγματοποιήσει κλήσεις προς άλλους χρήστες.

Μια κλήση ενός UE προς έναν συνδρομητή άλλου δικτύου ακολουθεί την παρακάτω διαδικασία (Εικόνα 14):

- Το UE ετοιμάζει και αποστέλλει το μήνυμα SIP Invite στο P-CSCF.
- Αντίστοιχα ο P-CSCF προωθεί κατάλληλα το μήνυμα στον S-CSCF που γνωρίζει από την διαδικασία του registration.
- Ο S-CSCF προωθεί το invite στον Application Server που υπάγεται ο χρήστης.
- Ο AS απαντά με ένα μήνυμα SIP 100 Trying, το οποίο προωθείται πίσω στο UE και με το invite.
- Το invite τελικά αποστέλλεται προς τον I-CSCF του άλλου δικτύου, αφού έχει συμβουλευτεί την ENUM/DNS και διαπιστώνει ότι το URI/τηλεφωνικός αριθμός δεν βρίσκεται στο home δίκτυο.
- Ο I-CSCF στέλνει μέσω Diameter αίτημα στην HSS για τον εντοπισμό του καλούμενου χρήστη.
- HSS αποκρίνεται κατάλληλα με τα δεδομένα του χρήστη και τελικά ο I-CSCF αποστέλλει το Invite στον S-CSCF.
- Ο S-CSCF αποστέλλει πίσω ένα μήνυμα 100 Trying και παράλληλα προωθεί το invite σταδιακά στον καλούμενο αντίστοιχα όπως περιγράφηκε προηγουμένως.
- Ο καλούμενος όταν παραλαμβάνει το Invite, εφόσον είναι διαθέσιμος, αποστέλλει ένα μήνυμα SIP 180 Ringing στον δικό του P-CSCF το οποίο προωθείται τελικά στον χρήστη που ξεκίνησε την κλήση.
- Αφού σηκώσει το ακουστικό ο χρήστης Β, τότε αποστέλλει ένα μήνυμα SIP 200 OK στον χρήστη Α, ο οποίος αποκρίνεται με ένα μήνυμα SIP ACK.
- Μετά την διαδικασία αυτή πραγματοποιείται η μεταφορά των πολυμέσων μέσω ενός RTP Session.
- Στην συνέχεια ένας από τους δύο χρήστες (πχ ο Α) κατεβάζει το ακουστικό του και αντίστοιχα το UE αποστέλλει ένα μήνυμα SIP BYE στον άλλο χρήστη.
- Τελικά ο χρήστης Β αποκρίνεται με ένα μήνυμα 200 OK και η κλήση τερματίζεται.



Εικόνα 14. Πραγματοποίηση Κλήσης μεταξύ τριών μερών

4.1.5 Προφίλ Χρηστών

Όπως αναφέρθηκε στα προηγούμενα υποκεφάλαια η HSS διατηρεί τα προφίλ των συνδρομητών (user profiles) και αλληλεπιδρά αντίστοιχα με τον S-CSCF με βάση αυτά τα προφίλ, όπως περιγράφηκε παραπάνω. Ο S-CSCF κατά την εγγραφή του χρήστη σε αυτόν, αιτείται και τελικά αποθηκεύει και αυτός τα προφίλ των συνδρομητών για τους οποίους είναι υπεύθυνος και διαχειρίζεται. Ένα προφίλ συνδρομητή έχει την μορφή που παρουσιάζεται στην εικόνα 15.

```
<ServiceProfile>
        <PublicIdentify>
           <Identity>sip: eric@ims.exemple.com</Identity>
        </PublicIdentity>
        <PublicIdentity>
           <Identity>tel:+33122334455</Identity>
        </PublicIdentity>
        <InitialFilterCriteria>
            <Priotity>0</Priority>
            <TriggerPoint>
                <ConditionTypeCNF>0</ConditionTypeCNF>
                <SPT>
                    <ConditionNegated>0</ConditionNegated>
                    <Group>0</Group>
                    <Method>INVITE</Method>
                </SPT>
                 <SPT>
                    <ConditionNegated>0</ConditionNegated>
                    <Group>0</Group>
                    <SessionCase>2</SessionCase>
                </SPT>
            </TriggerPoint>
            <ApplicationServer>
                 <ServerName>sip:vmail@ims.exemple.com</ServerName>
                 <DefaultHandling>1</DefaultHandling>
           </ApplicationServer>
        </InitialFilterCriteria>
</ServiceProfile>
```

Εικόνα 15. HSS user profile

4.2 Ασφάλεια στο IMS

Η ασφάλεια του δικτύου IMS χωρίζεται σε δύο άξονες. Την πιστοποίηση της αυθεντικότητας χρήστη/δικτύου και την ασφάλεια στο επίπεδο δικτύου, η οποία έχει να κάνει με την διασφάλιση της κίνησης που μεταδίδεται σε ευαίσθητα σημεία του δικτύου (εκτός IMS δηλαδή) ή και μεταξύ άλλων δικτύων που δεν μπορούν να θεωρηθούν έμπιστα. Το πρωτόκολλο που χρησιμοποιεί το IMS σε αυτές τις περιπτώσεις είναι το IPSec.

Το κομμάτι του δικτύου που πρέπει να προστατευτεί καθώς είναι εκτεθειμένο και μπορεί να πέσει θύμα επίθεσης είναι αυτό μεταξύ του τερματικού του χρήστη και του P-CSCF, που αποτελεί τον πρώτο κόμβο του IMS. Αυτό το κομμάτι μπορεί επίσης να βρίσκεται υπό την διαχείριση άλλου παρόχου οπότε πρέπει να εφαρμόσουμε ασφάλεια με σκοπό την μη αποκάλυψη της ταυτότητας του συνδρομητή. Όπως αναφέραμε παραπάνω σε αυτό το σημείο το IMS χρησιμοποιεί IPSec Security Associations διασφαλίζοντας ουσιαστικά το κομμάτι αυτό.

Όσον αφορά την αυθεντικοποίηση και την πιστοποίηση του χρήστη και του δικτύου το IMS χρησιμοποιεί την διαδικασία εγγραφής του χρήστη στο δίκτυο, όπως περιγράφηκε σε προηγούμενα κεφάλαια, με χρήση μηνυμάτων REGISTER. Η διαδικασία αυτή βασίζεται σε δύο βασικά σημεία. Την χρήση κάρτας SIM από μεριάς συνδρομητή ή την χρήση modem/router. Η πρώτη περίπτωση χρησιμοποιείται σε δίκτυα κινητής τηλεφωνίας και η δεύτερη σε δίκτυα σταθερής τηλεφωνίας. Η φιλοσοφία και των δύο τρόπων είναι η ίδια. Η ταυτότητα συνδρομητή αποθηκεύεται και στις δύο περιπτώσεις στο τερματικό (SIM ή modem/router). Έτσι η ταυτότητα αυτή χρησιμοποιείται για την δημιουργία του αρχικού μηνύματος REGISTER και την εγγραφή του χρήστη στο δίκτυο. Στην ουσία με αυτό τον τρόπο πιστοποιείται η αυθεντικότητα του χρήστη στο δίκτυο.

Αντίστοιχα χρειάζεται να πιστοποιηθεί και το δίκτυο στον χρήστη για λόγους ασφάλειας και μη αποκάλυψης των στοιχείων του χρήστη σε μη έμπιστες οντότητες. Τον ρόλο αυτό αναλαμβάνει η HSS η οποία κατά το provisioning των υπηρεσιών του χρήστη δημιουργεί το μοναδικό προφίλ του, στο οποίο βρίσκεται και το username/password. Έτσι κατά την λήψη του REGISTER από τον χρήστη δημιουργεί ένα μήνυμα digest χρησιμοποιώντας αυτές τις πληροφορίες έτσι ώστε ο χρήστης να χρησιμοποιήσει τον αντίστοιχο αλγόριθμο για να πιστοποιήσει το δίκτυο (challenge – response). Μετά αυτή την αμοιβαία διαδικασία ο χρήστης έχει αυθεντικοποιηθεί και πιστοποιηθεί να χρησιμοποιήσει το δίκτυο.

Από πλευράς ασφάλειας του πυρήνα του IMS, το βάρος πέφτει στον κόμβο που απαντά στα αιτήματα των συνδρομητών και αποτελεί τον αρχικό κόμβο επαφής του δικτύου κορμού με το δίκτυο του IMS. Αυτός σε πολλές περιπτώσεις είναι ο P-CSCF αλλά συνήθως στις περισσότερες υλοποιήσεις των παρόχων χρησιμοποιείται μπροστά από αυτόν ένας κόμβος SBC (Session Boarder Controller). Ο SBC χρησιμοποιείται στην ουσία ως τοίχος προστασίας του IMS ελέγχοντας όλες τις συνεδρίες που διαχειρίζεται το IMS. Όλη η εισερχόμενη και εξερχόμενη κίνηση του IMS περνά από αυτόν. Πέραν από τοίχος προστασίας, ο SBC εκτελεί και λειτουργίες topology hiding του IMS για μη αποκάλυψή της τοπολογίας σε επιτιθέμενους που βρίσκονται στο μη έμπιστο κομμάτι του δικτύου. Σε περίπτωση απουσίας του SBC τους ρόλους αυτούς εκτελεί ο P-CSCF. Εσωτερικά του IMS χρησιμοποιείται συνήθως ξεχωριστό τοίχος προστασίας αλλά και ζώνες προστασίας DMZ.

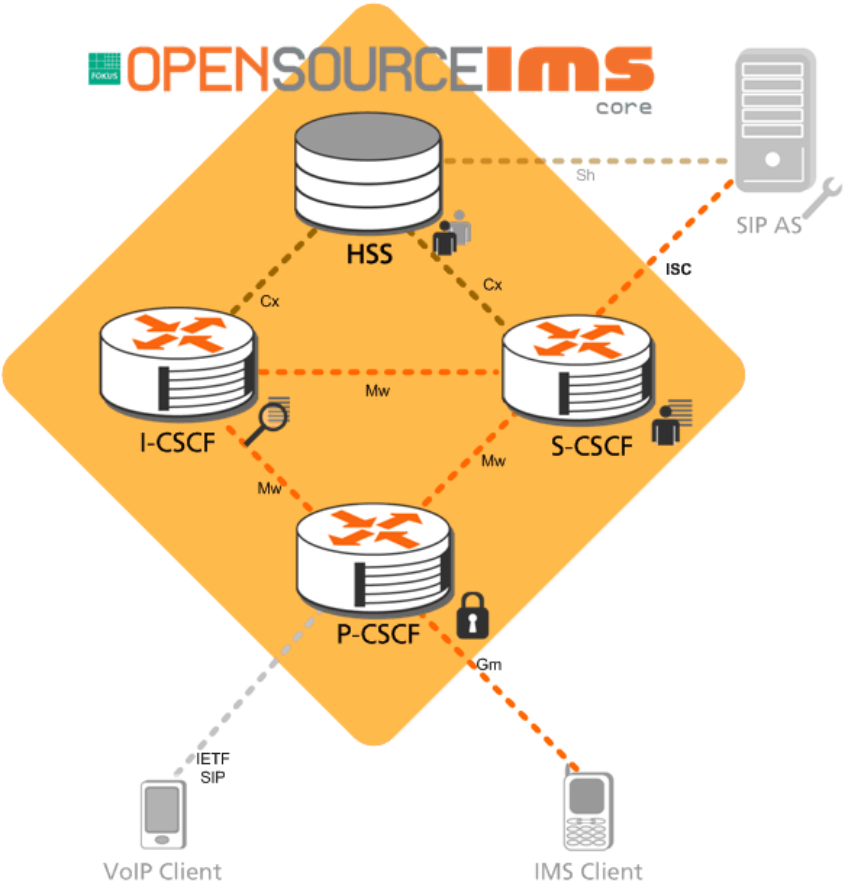
Κεφάλαιο 5

5.1 Πειραματική Διάταξη OpenIMS Core

Για την εφαρμογή των επιθέσεων, που θα παρουσιαστούν σε επόμενο κεφάλαιο, προς το δίκτυο IMS αλλά και των αντίμετρων που πρέπει να ληφθούν για την αντιμετώπισή τους, θα χρησιμοποιήσουμε την πειραματική διάταξη του OpenIMS Core. Η διάταξη αυτή έχει εξελιχθεί από τον οργανισμό FOKUS Open Source IMS Core και βασίζεται στο λειτουργικό σύστημα Linux.

Η διάταξη OpenIMS Core περιλαμβάνει τις παρακάτω οντότητες όπως ορίζονται από στο 3GPP:

- HSS
- P-CSCF
- I-CSCF
- S-CSCF



Εικόνα 16. Αρχιτεκτονική OpenIMS Core

Το OpenIMS Core αποτελεί στην ουσία ένα testbed και δεν προορίζεται για εμπορική χρήση. Συμμορφώνεται με όλες τις προδιαγραφές του δικτύου IMS όπως περιγράφονται στο 3GPP και για αυτό το λόγω ανταποκρίνεται σε πραγματικά σενάρια. Μπορεί να εγκατασταθεί σε οποιοδήποτε προσωπικό υπολογιστή που έχει λειτουργικό σύστημα linux και για αυτό το λόγο αποτελεί ιδανικό testbed για την εφαρμογή προσομοιώσεων επίθεσης σε IMS δίκτυα και λήψη αντίμετρων που ανταποκρίνονται σε πραγματικά σενάρια.

Ο πυρήνας του OpenIMS πάνω στον οποίο θα εφαρμόσουμε τα σενάρια επίθεσης αποτελείται από τους παρακάτω κόμβους (Εικόνα 16):

- P-CSCF
- I-CSCF
- S-CSCF
- HSS

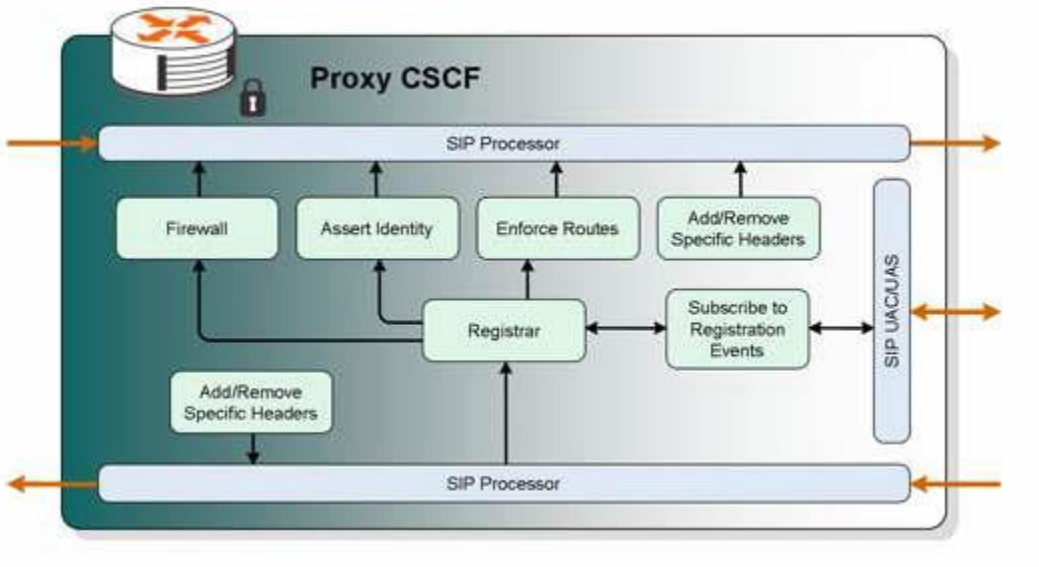
5.2 OpenIMS Core CSCFs

Οι ιδιότητες και λειτουργίες των κόμβων CSCF των δικτύων IMS παρουσιάστηκαν σε προηγούμενα κεφάλαια. Οι CSCFs του OpenIMS Core project έχουν ως σκοπό να προσαρμόζονται στα πρότυπα που ορίστηκαν από το 3GPP και να τα εφαρμόζουν στο δικό του περιβάλλον, καλύπτοντας όλες τις δυνατότητές τους.

Ένας ακόμα στόχος που πετυχαίνει το OpenIMS project, πέραν από της ρεαλιστικής απεικόνισης των CSCF, είναι η αποδοτική λειτουργία τους αλλά και η δυνατότητα εύκολης διαμόρφωσής τους σε διαφορετικά συστήματα ανάλογα με τις εκάστοτε ανάγκες.

5.2.1 OpenIMS Core P-CSCF

Ο P-CSCF του OpenIMS project λειτουργεί ως firewall για το core δίκτυο του IMS. Οι μόνοι χρήστες οι οποίοι έχουν την δυνατότητα να στέλνουν μηνύματα στον πυρήνα του IMS είναι αυτοί που έχουν εγγραφεί στο δίκτυο, βάση της διαδικασίας εγγραφής (registration) που περιγράφηκε σε προηγούμενα υποκεφάλαια. Επιπρόσθετα γίνονται οι κατάλληλες δρομολογήσεις βάση των μηνυμάτων που λαμβάνει από τους χρήστες ή από το δίκτυο.



Εικόνα 17. Αρχιτεκτονική OpenIMS Core P-CSCF

Τα βασικά χαρακτηριστικά του P-CSCF στην υλοποίηση OpenIMS Core είναι τα εξής:

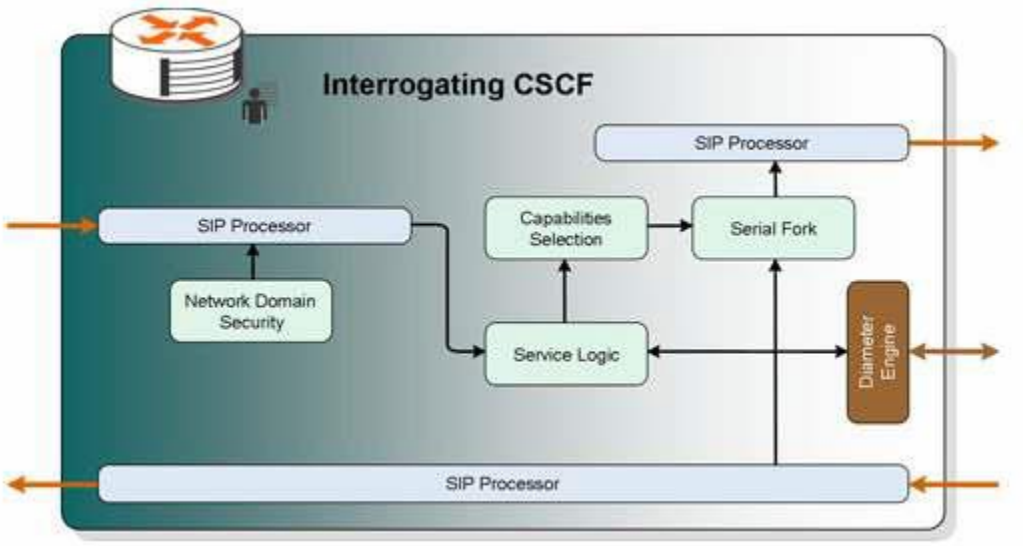
- Χειρισμός σηματοδοσίας SIP από και προς τα τερματικά.
- Λειτουργίες τοίχους προστασίας για τον πυρήνα του IMS.
- Έλεγχος SIP headers.
- Υλοποίηση NAT και topology hiding.
- Έλεγχος της κατάστασης των τερματικών, όλων των συνεδριών και την ανάγκη για εγγραφή τερματικού στο δίκτυο.
- Ρύθμιση IP-Sec.

5.2.2 OpenIMS Core I-CSCF

Ο I-CSCF του OpenIMS project λειτουργεί ως stateless proxy και στέλνει ερωτήματα στην HSS, μέσω της διεπαφής Cx που υλοποιεί, για έλεγχο της δημόσιας ταυτότητας του χρήστη από τον οποίο λαμβάνεται το μήνυμα και στη συνέχεια δρομολογεί κατάλληλα στον αντίστοιχο S-CSCF, μέσω των capabilities του χρήστη.

Τα βασικά χαρακτηριστικά του I-CSCF στην υλοποίηση OpenIMS Core είναι τα εξής:

- Υλοποίηση διεπαφής Cx
- Επιλογή S-CSCF βάση των capabilities του χρήστη.
- Topology hiding.



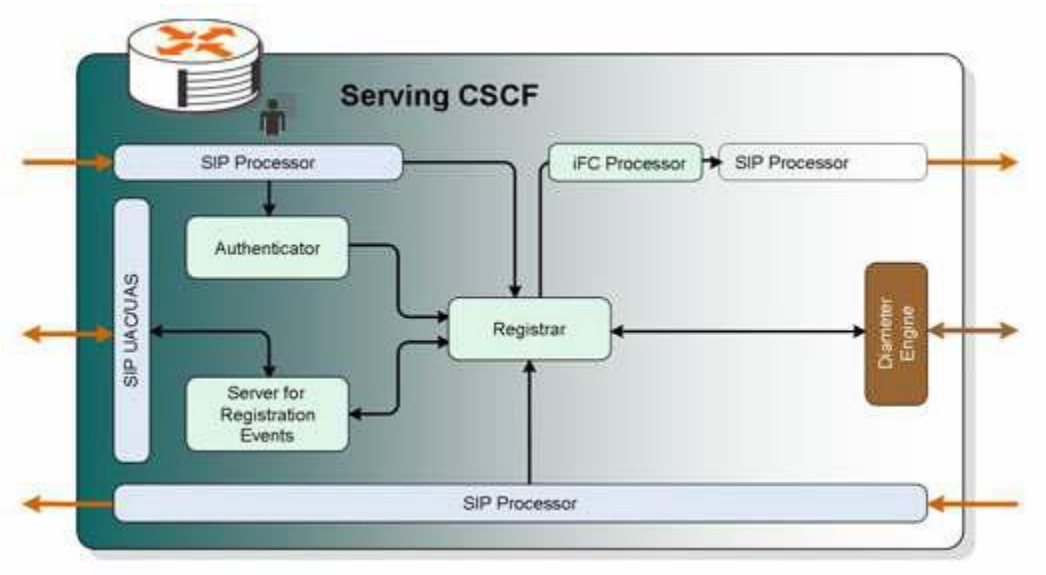
Εικόνα 18. Αρχιτεκτονική OpenIMS Core I-CSCF

5.2.3 OpenIMS Core S-CSCF

Ο S-CSCF του OpenIMS project επικοινωνεί με την HSS για να κατεβάσει το προφίλ του χρήστη μέσω της διεπαφής Cx που υλοποιεί. Υλοποιεί πιστοποίηση των χρηστών μέσω της διαδικασίας challenge-response που περιγράφηκε σε προηγούμενα υποκεφάλαια μέσω αλγορίθμων AKA v.1, v.2 MD5 και MD5.

Τα βασικά χαρακτηριστικά του S-CSCF στην υλοποίηση OpenIMS Core είναι τα εξής:

- Υλοποίηση της διεπαφής Cx.
- Πιστοποίηση μέσω αλγορίθμων AKA v.1, v.2 MD5 και MD5.
- Επεξεργασίας SIP header.
- Κατέβασμα user profile από την HSS.
- Έλεγχος όλων των συνεδριών που διαχειρίζεται.

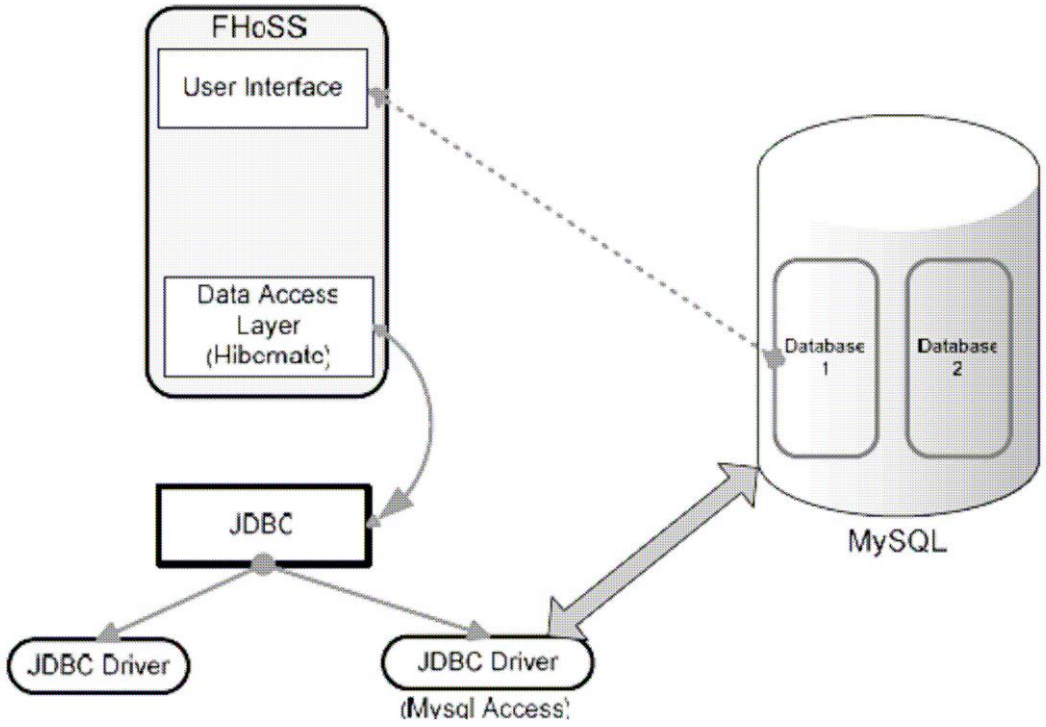


Εικόνα 19. Αρχιτεκτονική OpenIMS Core S-CSCF

5.3 OpenIMS Core FOKUS HSS (FHoSS)

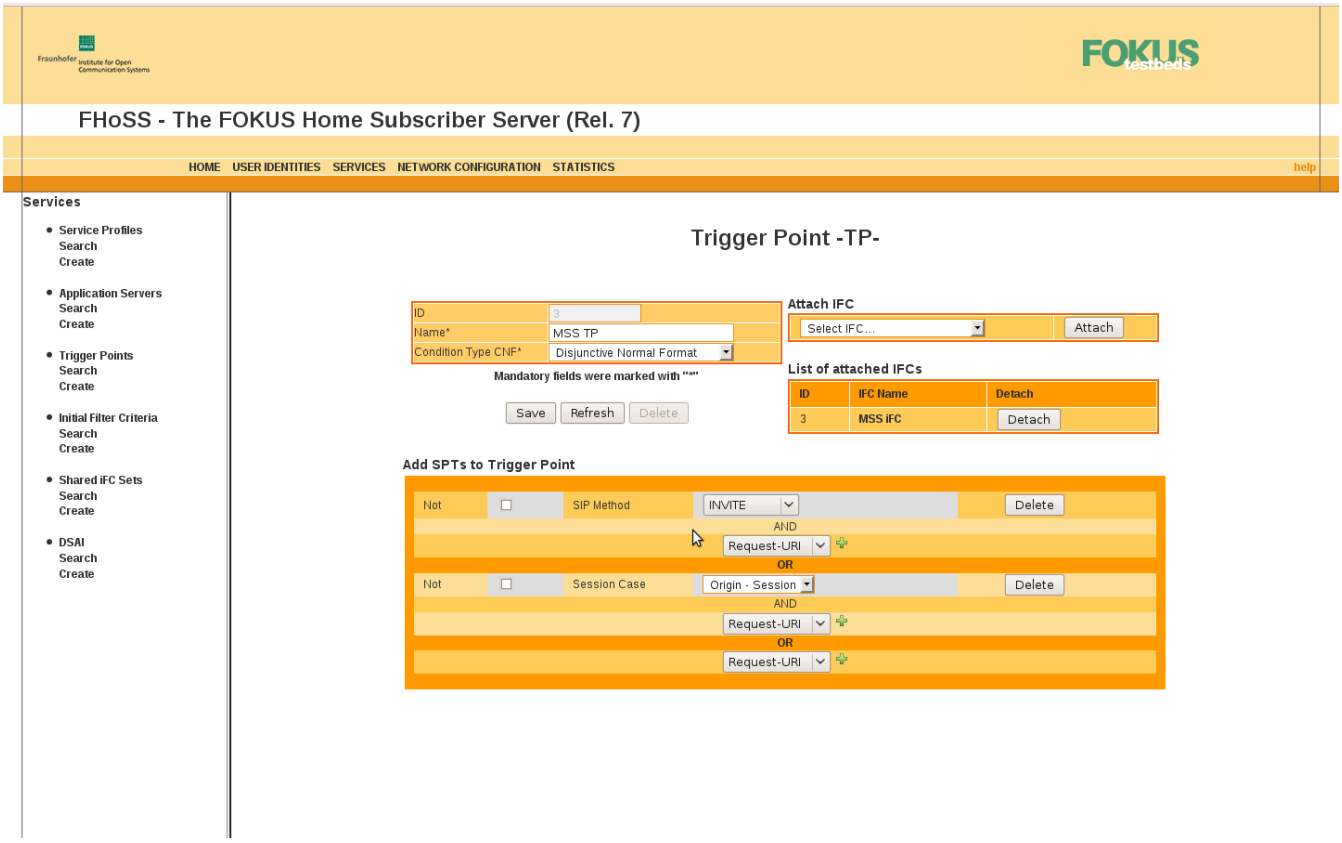
Το OpenIMS project έχει υλοποιήσει και χρησιμοποιεί την δικιά του HSS η οποία βασίζεται στην γλώσσα προγραμματισμού Java και ονομάζεται FOKUS Home Subscriber Server (FHoSS).

Η HSS αυτή χρησιμοποιεί για την αποθήκευση των χρηστών την βάση δεδομένων MySQL (Εικόνα 20). Στην ουσία αποτελεί ένα σημείο ελέγχου της βάσης δεδομένων που υλοποιεί παράλληλα τις διεπαφές diameter με τους I-CSCF και S-CSCF. Υποστηρίζεται πιστοποίηση βασισμένη στο πρωτόκολλο HTTP.



Εικόνα 20. Αρχιτεκτονική FHoSS

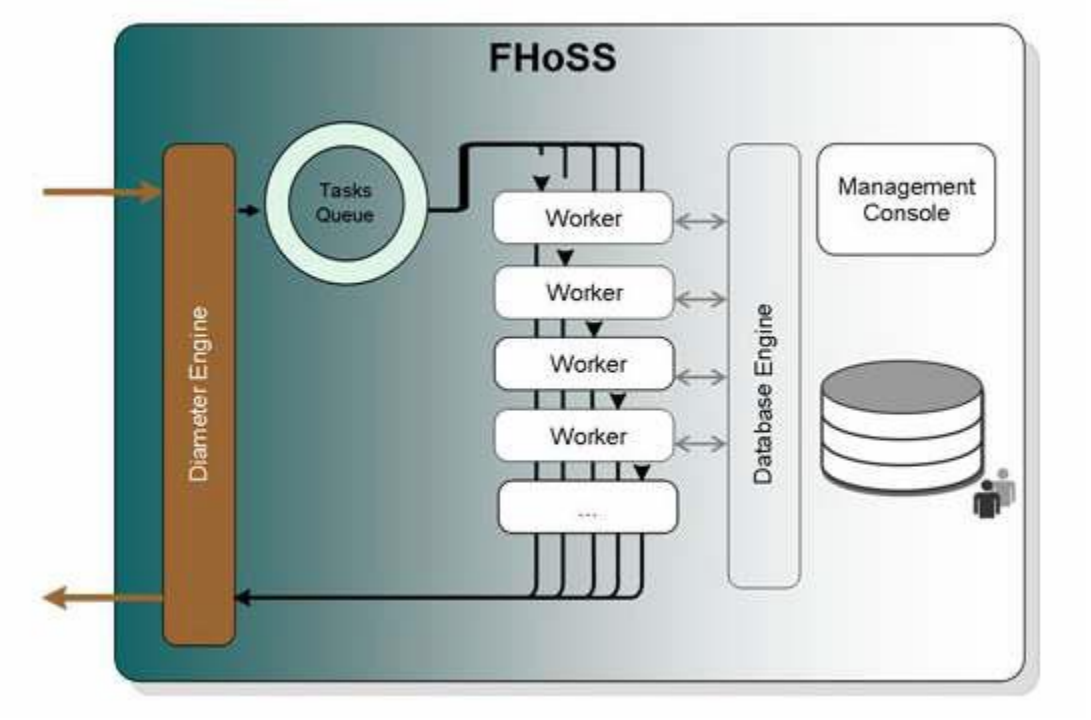
Έχει υλοποιηθεί και ένα web interface για την διαχείριση της FHoSS κατι των χρηστών του δικτύου το οποίο παρουσιάζεται στην εικόνα 21.



Εικόνα 21. Διαχείριση της HSS

Τα βασικά χαρακτηριστικά της HSS στην υλοποίηση OpenIMS Core είναι τα εξής:

- Υλοποίηση των διεπαφών Cx, Sh και Zh.
- Υλοποίηση πρωτοκόλλου Diameter βασισμένο στην Java.
- Λειτουργία AuC.
- Web interface διαχείρισης.



Εικόνα 22. Αρχιτεκτονική OpenIMS Core FHoSS

Κεφάλαιο 6

Εγκατάσταση του OpenIMS Core

Το λειτουργικό σύστημα που έχει επιλεγεί για να φιλοξενήσει το OpenIMS Core είναι το Linux Debian 6. Η επιλογή έγινε για λόγους λειτουργικότητας και απόδοσης του συστήματος.

Το λειτουργικό σύστημα φιλοξενείται σε μια εικονική μηχανή (Virtual Machine) σε σύστημα VMware Workstation 9, το οποίο αποτελεί ιδανικό τρόπο υλοποίησης δοκιμών, αξιοποιώντας ήδη υπάρχοντες υπολογιστικούς πόρους.

Για τον έλεγχο και την μελέτη της δικτυακής κίνησης τα χρησιμοποιήσουμε το λογισμικό ανάλυσης πρωτοκόλλων δικτύου Wireshark.

6.1 Λήψη του κώδικα

Αρχικά δημιουργούμε τους φακέλους που θα φιλοξενήσουν τον κώδικα του OpenIMS Core:

```
mkdir /opt/OpenIMSCore
cd /opt/OpenIMSCore
```

Στην συνέχεια κατεβάζουμε τον κώδικα για του CSCF και την HSS από τον ιστότοπο του OpenIMS Core Project στα κατάλληλα paths.

```
mkdir FHoSS
svn checkout
http://svn.berlios.de/svnroot/repos/openimscore/FHoSS/tru
nk FHoSS

mkdir ser_ims
svn checkout
http://svn.berlios.de/svnroot/repos/openimscore/ser_ims/t
runk ser_ims


cd FHoSS
ant compile deploy
cd ..
```

Για να καταφέρουμε να κάνουμε compile τον κώδικα που έχουμε κατεβάσει στο σύστημά μας απαιτείται η ύπαρξη μερικών packages στο σύστημά μας τα οποία και πρέπει να εγκαταστήσουμε. Αυτά είναι τα εξής:

- Sun-java-jdk
- Mysql-server
- Libmysqlclient15-dev
- Libxml2.dev
- Ant
- Bind9
- Flex
- Bison

Στην συνέχεια είμαστε έτοιμοι να κάνουμε compile τον κώδικα.

```
cd ser_ims
make install-libs all
cd ..
cd FHoSS
ant compile
ant deploy
cd ..
```

6.2 Ρύθμιση του περιβάλλοντος

Πλέον το OpenIMS Core βρίσκεται εγκατεστημένο στο σύστημά μας και είναι έτοιμο προς χρήση. Για να μπορέσει να λειτουργήσει όμως στο περιβάλλον μας πρέπει να γίνει το κατάλληλο configuration σε επίπεδο δικτύου.

Σε αυτό το σημείο το OpenIMS Core είναι εγκατεστημένο να λειτουργεί στην διεπαφή loopback (IP address 127.0.0.1) του εικονικού μηχανήματος με domain το open-ims.test. Η MySQL είναι εγκατεστημένη για χρήση σε τοπικό επίπεδο

6.2.1 Ρύθμιση του DNS

Για τον εντοπισμό των IPs των διάφορων κόμβων από τα τερματικά των χρηστών αλλά και από τους ίδιους κόμβους του IMS θα εγκαταστήσουμε και θα χρησιμοποιήσουμε τον DNS bind9.

```
sudo apt-get install bind9
```

Στην συνέχεια αντιγράφουμε το αρχείο DNS του OpenIMS στον φάκελο του bind9 ώστε να γίνει resolvable.

```
Sudo cp /opt/OpenIMSCore/ser_ims/cfg/open-ims.dnszone
/etc/bind/
```

Προσθέτουμε το domain στο configuration του bind.

```
sudo nano /etc/bind/named.conf

zone "open-ims.test"{

     type master;

     file "/etc/bind/open-ims.dnszone";

};
```

Στην συνέχεια επανεκκινούμε τον DNS server μας για να υλοποιηθούν οι αλλαγές που εισάγαμε.

```
sudo /etc/init.d/bind9 restart
```

Από τη στιγμή που ρυθμίσαμε τον DNS μας πρέπει να τον ορίσουμε ως επιλογή για το σύστημά μας ώστε να μπορεί να κάνει resolv μέσω αυτού.

```
sudo nano /etc/resolv.conf

nameserver 192.168.44.130
```

Ένας εύκολος τρόπος να ελέγξουμε αν λειτουργεί σωστά ο DNS είναι να κάνουμε reachability test σε κάποιο από τους κόμβους του IMS.

```
ping pcscf.open-ims.test

Pinging 192.168.44.130 with 32 bytes of data:

Reply from 192.168.44.130: bytes=32 time=2ms TTL=64

Reply from 192.168.44.130: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.44.130:

     Packets: Sent = 2, Received = 4, Lost = 0 (0% loss)
```

6.2.2 Ρύθμιση της MySQL

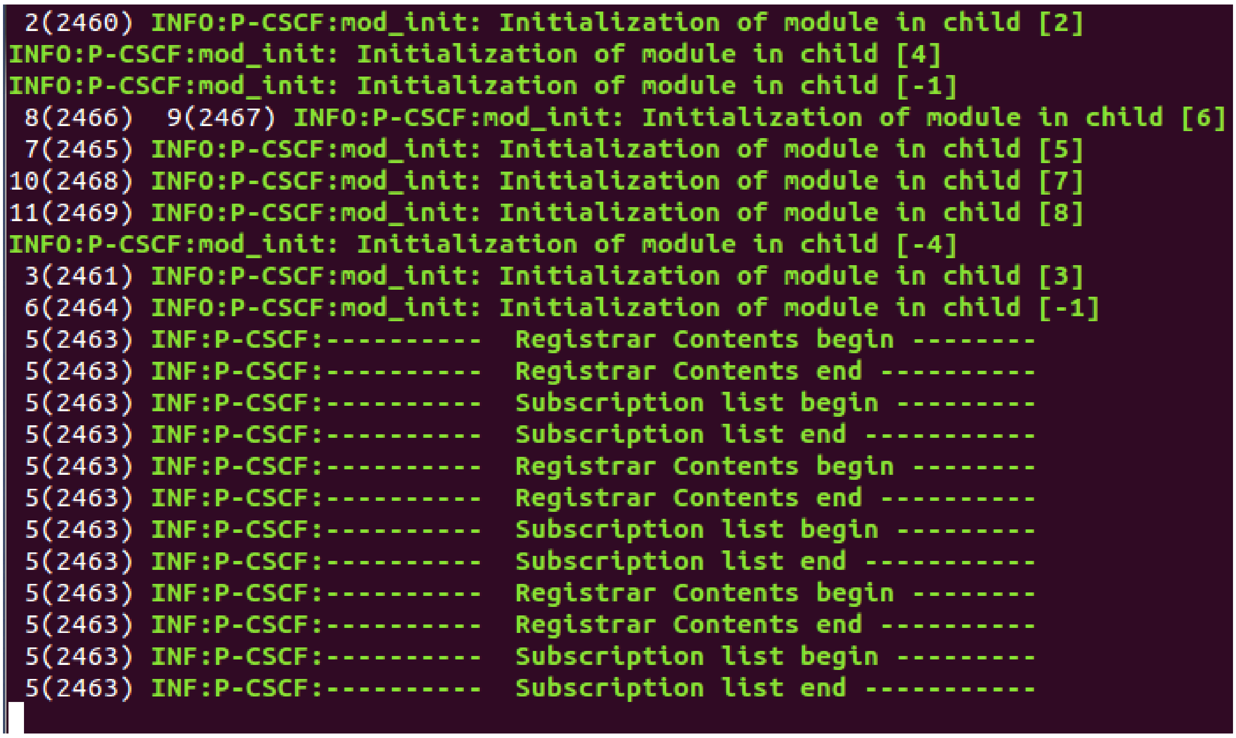
Σε αυτό το σημείο πρέπει να ρυθμίσουμε την βάση δεδομένων MySQL που θα χρησιμοποιήσει η HSS για να αποθηκεύει τα δεδομένα των χρηστών του δικτύου.

```
mysql -u root -p -h localhost < ser_ims/cfg/icscf.sql

mysql -u root -p -h localhost < FHoSS/scripts/hss_db.sql

mysql -u root -p -h localhost < FHoSS/scripts/userdata.sql
```

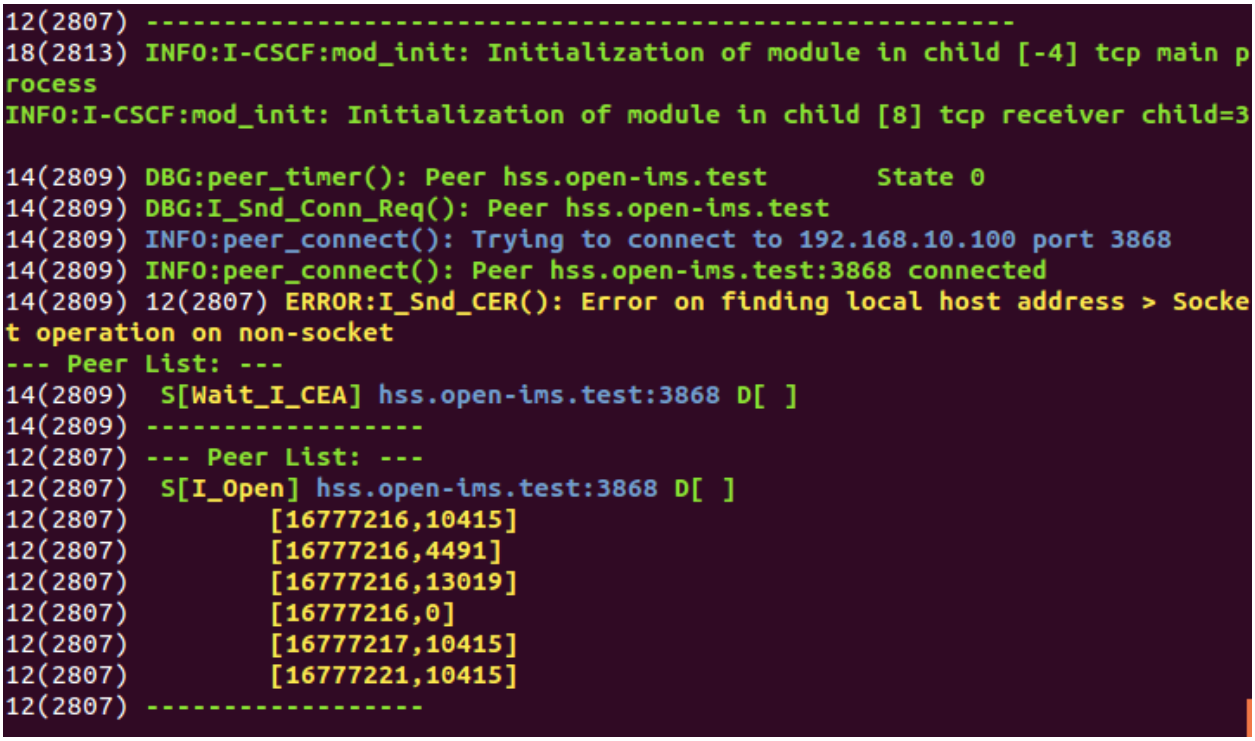
6.2.3 Εκτέλεση του OpenIMS Core

Εκτελούμε αρχικά του CSCF οι οποίοι πρέπει να τρέχουν παράλληλα για να λειτουργήσει το IMS μας.

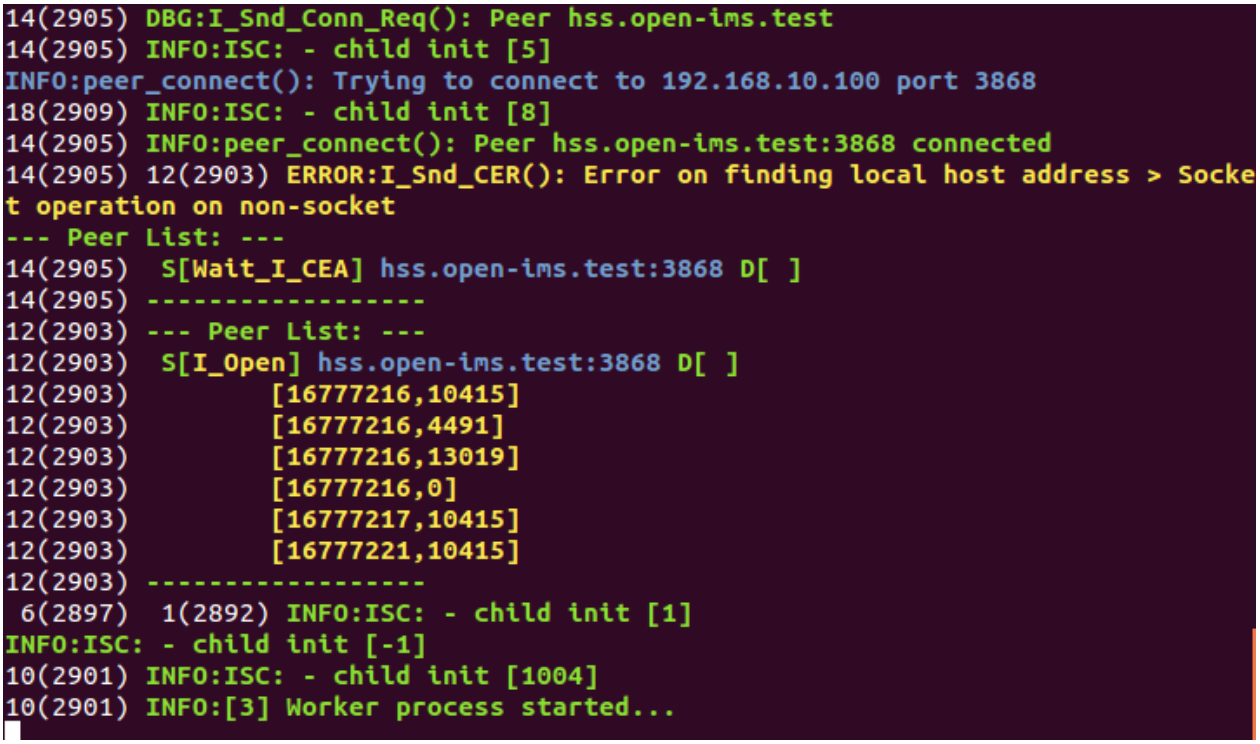
```
cd /opt/OpenIMSCore/

./pcscf

./icscf

./scscf
```



Εικόνα 23. Εκτέλεση του P-CSCF



Εικόνα 24. Εκτέλεση του I-CSCF



Εικόνα 25. Εκτέλεση του S-CSCF

Στην συνέχεια τρέχουμε και την HSS/

```
cd /opt/OpenIMSCore/FHoSS/deploy
```

```
./startup.sh
```

```
        at org.apache.catalina.core.StandardWrapper.loadServlet(StandardWrapper.
java:1091)
        at org.apache.catalina.core.StandardWrapper.load(StandardWrapper.java:92
5)
        at org.apache.catalina.core.StandardContext.loadOnStartup(StandardContex
t.java:3857)
        at org.apache.catalina.core.StandardContext.start(StandardContext.java:4
118)
        at org.apache.catalina.core.ContainerBase.addChildInternal(ContainerBase
.java:759)
        at org.apache.catalina.core.ContainerBase.addChild(ContainerBase.java:73
9)
        at org.apache.catalina.core.StandardHost.addChild(StandardHost.java:524)
        at de.fhg.fokus.hss.main.TomcatServer.startTomcat(TomcatServer.java:144)
        at de.fhg.fokus.hss.main.HSSContainer.<init>(HSSContainer.java:74)
        at de.fhg.fokus.hss.main.HSSContainer.main(HSSContainer.java:110)
log4j:ERROR Either File or DatePattern options are not set for appender [LOGFILE
2].
2013-05-18 22:16:52,575 FATAL org.apache.jasper.EmbeddedServletOptions - <init>
The scratchDir you specified: /opt/OpenIMSCore/FHoSS/deploy/work/null/192.168.10
.100/hss.web.console is unusable.
2013-05-18 22:16:52,628 INFO  de.fhg.fokus.hss.main.TomcatServer - startTomcat W
ebConsole of FHoSS was started !
```

Εικόνα 26. Εκτέλεση της HSS

Πλέον το IMS μας είναι έτοιμο για να εξυπηρετήσει υπηρεσίες και να κάνουμε τις δοκιμές μας πάνω σε επιθέσεις και αντίμετρα που πρέπει να ληφθούν για την ασφάλεια των χρηστών και του δικτύου.

Τα στοιχεία των κάθε κόμβου και των αντίστοιχων υπηρεσιών στην υλοποίησή μας φαίνονται στον παρακάτω πίνακα.

STATUS OF OpenIMS SERVICES (expected running on eth0)	
P-CSCF	192.168.44.130:4060 ------ LISTEN ------ 1584/ser
I-CSCF	192.168.44.130:5060 ------ LISTEN ------ 1526/ser
S-CSCF	192.168.44.130:6060 ------ LISTEN ------ 1588/ser
HSS	192.168.44.130:8080 ------ LISTEN ------ 1015/java
Diameter [3868]	192.168.44.130:3868 ------ LISTEN ------ 1015/java
Diameter [3869]	192.168.44.130:3869 ------ LISTEN ------ 1542/ser
Diameter [3870]	192.168.44.130:3870 ------ LISTEN ------ 1616/ser
DNS - Bind9	192.168.44.130:53 ------ LISTEN ------ 1175/named127.0.0.1:53 ------ LISTEN ------ 1175/named:::53 ------ LISTEN ------ 1175/named
Uctiptv as	0.0.0.0:8010 ------ 1648/uctiptv_as ------
SQL Database	127.0.0.1:3306 ------ LISTEN ------ 1394/mysqld

Εικόνα 27. Στοιχεία Κόμβων

Κεφάλαιο 7

Υλοποίηση Επιθέσεων στο IMS και Λήψη Αντιμέτρων

Στο σημείο αυτό και αφού έχουμε αναλύσει την αρχιτεκτονική και τον τρόπο λειτουργίας των IMS δικτύων, θα προχωρήσουμε σε εφαρμογή επιθέσεων στο testbed OpenIMS Core που έχουμε εγκαταστήσει, το οποίο προσομοιώνει με ακρίβεια τα πρότυπα των IMS δικτύων, όπως έχουν οριστεί από το 3GPP.

Οι επιθέσεις αυτές θα έχουν ως στόχο το δίκτυο τις υπηρεσίες που διέρχονται από αυτό και τους χρήστες που το χρησιμοποιούν, θέτοντας σε κίνδυνο την ιδιοτικότητα των συνομιλούντων μερών την αποκάλυψη της ταυτότητας τους αλλά και των στοιχείων επικοινωνίας τους.

Στην συνέχεια θα αναλυθούν και θα εκτιμηθούν οι μηχανισμοί ασφάλειας που πρέπει να εφαρμοστούν, ώστε να προστατευτεί η ιδιωτικότητα των χρηστών και η ακεραιότητα του δικτύου.

Καθώς το πρωτόκολλο SIP δεν διαθέτει δικό του μηχανισμό ασφάλειας, η διαδικτυακή τηλεφωνία VoIP αντιμετωπίζει προβλήματα ασφάλειας και χρήζει εφαρμογής κατάλληλων μηχανισμών για την διασφάλιση της επικοινωνίας.

Σκοπός των μηχανισμών ασφαλείας που θα παρουσιαστούν είναι κάλυψη των βασικών απαιτήσεων για την παροχή ασφαλών επικοινωνιών μέσω του IP δικτύου, όπως είναι η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα. Ταυτόχρονα, στόχος μας είναι μέσα από αυτήν την υλοποίηση να μην παραβιαστούν διαδικασίες αυθεντικοποίησης των μηνυμάτων του πρωτοκόλλου σηματοδοσίας καθώς επίσης να μην παραβιαστεί η ορθότητα και η εγκυρότητα των μηχανισμών χρέωσης.

7.1 Κίνδυνος Αποκάλυψης Ταυτότητας Χρηστών

Όπως αναφέρθηκε και προηγουμένως υπάρχει ζήτημα αποκάλυψης της ταυτότητας των χρηστών του IMS δικτύου, καθώς η επικοινωνία μπορεί να γίνεται πάνω από μη έμπιστα IP δίκτυα και μη έμπιστους κόμβους οι οποίοι διαχειρίζονται τα SIP μηνύματα. Αυτό είναι ένα πρόβλημα που πρέπει να αντιμετωπιστεί, καθώς η ιδέα του IMS βασίζεται σε πολλαπλά μέσα πρόσβασης και IP δίκτυα κορμού.

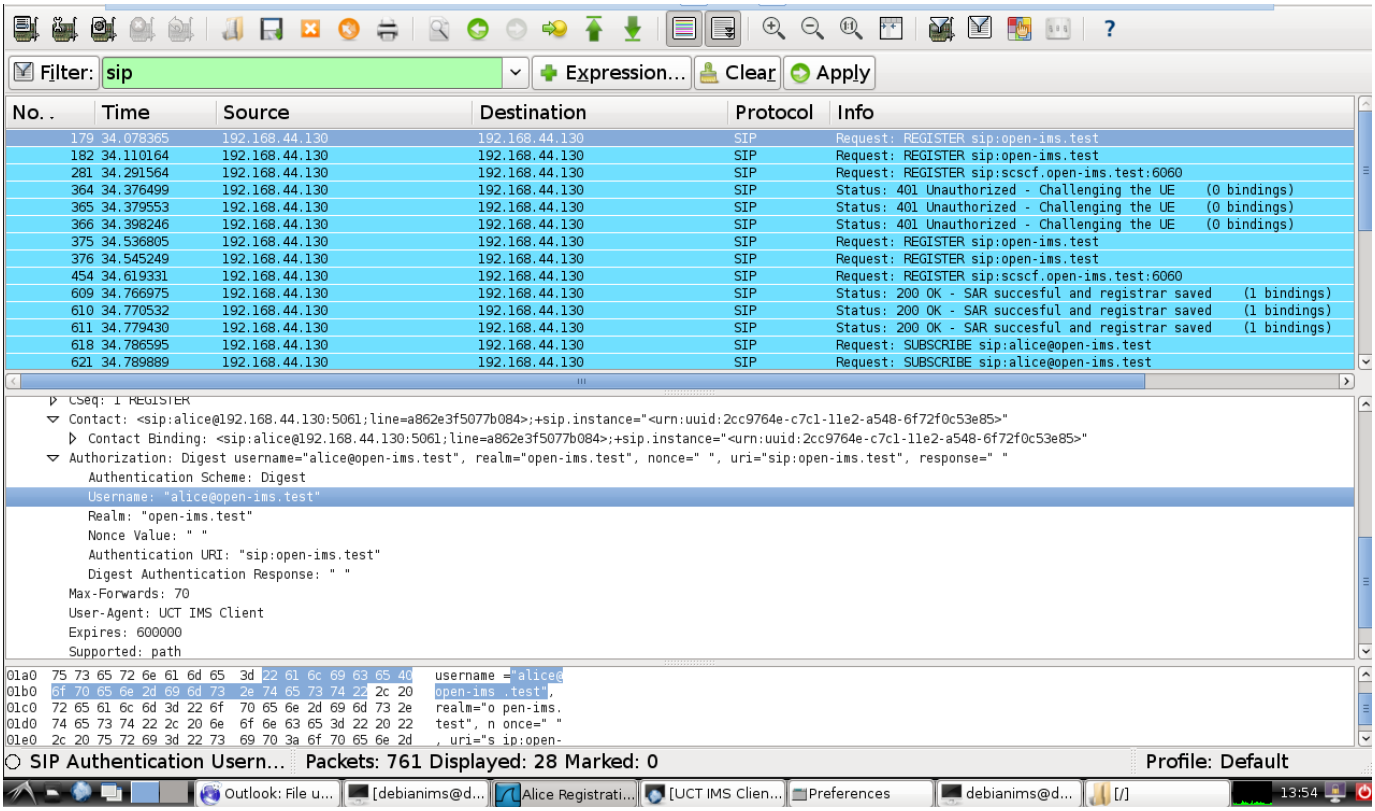
7.1.1 Επίθεση Υποκλοπής της Ταυτότητας του Χρήστη

Όπως αναφέρθηκε σε προηγούμενα κεφάλαια τα τερματικά κατά την ενεργοποίησή τους κινούν την διαδικασία της εγγραφής στο δίκτυο (registration). Το κομμάτι που είναι κυρίως ευάλωτο σε επιθέσεις είναι το IP δίκτυο κορμού από το τερματικό ως τον P-CSCF, όπου οι ενδιάμεσοι κόμβοι δεν είναι εύκολο να ελέγχονται.

Έτσι έχουμε στήσει ένα wireshark το οποίο είναι ένα πρόγραμμα traffic analysis και μπορούμε να πραγματοποιήσουμε επίθεση τύπου man-in-the-middle.

Το wireshark έχει ρυθμιστεί να λαμβάνει πακέτα από το IP δίκτυο πάνω από το οποίο πραγματοποιείται η μεταφορά των πακέτων από και προς τον χρήστη. Όταν ο χρήστη εκκινεί το τερματικό του τότε αποστέλλεται, όπως αναφέραμε, το μήνυμα REGISTER από το UE στον P-CSCF. Στην εικόνα 28 φαίνεται το πακέτο που υποκλέψαμε και μεταφέρει το αίτημα του χρήστη για εγγραφή στο IMS δίκτυο.

Όπως παρατηρούμε όλη η πληροφορία είναι σε καθαρό κείμενο και μπορούμε να αντλήσουμε πολλές πληροφορίες για τον χρήστη, όπως για παράδειγμα η IP διεύθυνσή του και ποιόν client χρησιμοποιεί.



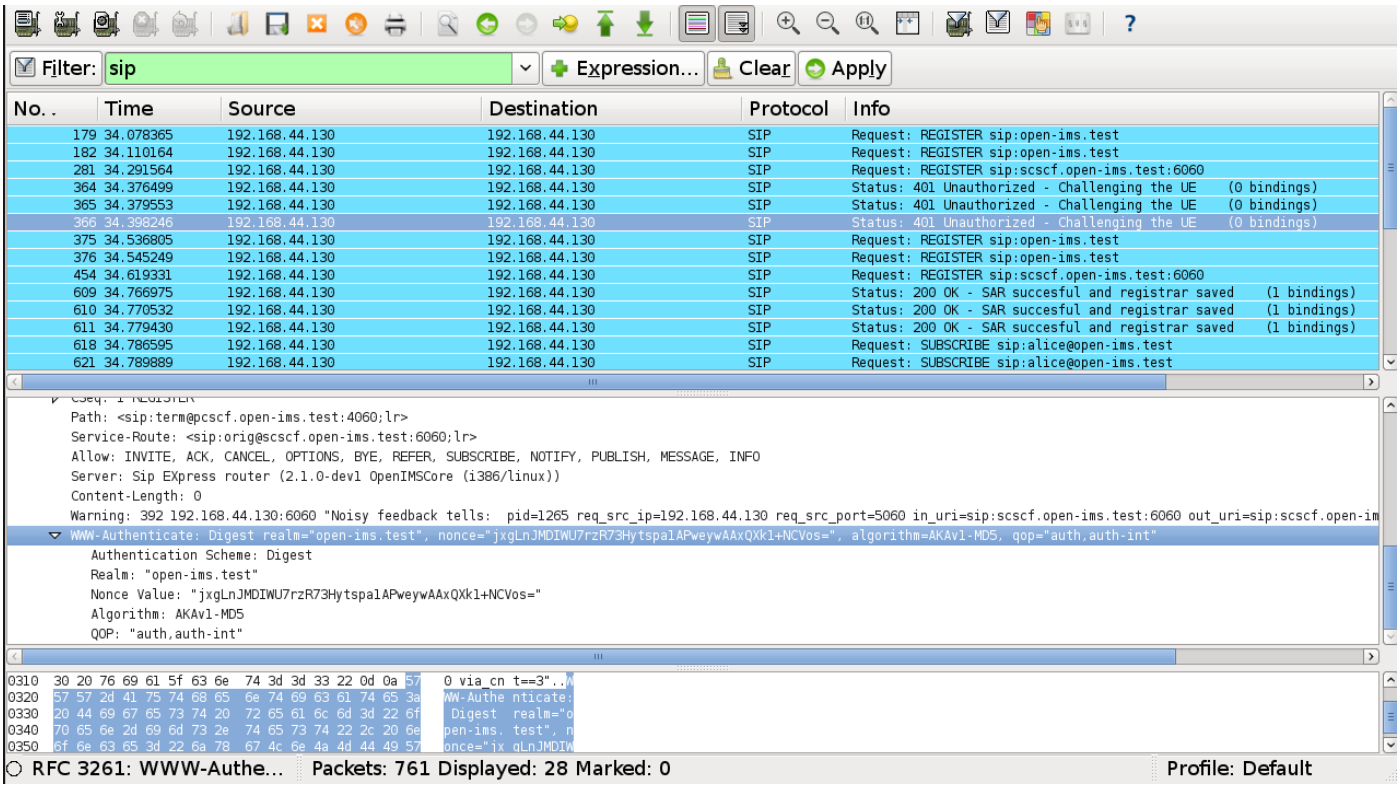
Εικόνα 28. Μήνυμα REGISTER από το UE

Αυτό όμως που είναι το πιο σημαντικό, αλλά και στόχος μας είναι η υποκλοπή της ταυτότητας του χρήστη, η οποία όπως βλέπουμε είναι εμφανής και είναι η

alice@open-ims.test. Οπότε ο στόχος του επιτιθέμενου για υποκλοπή ταυτότητας χρήστη του δικτύου IMS επιτεύχθηκε. Μια ακόμα χρήσιμη πληροφορία που αποσπάται είναι το domain των κόμβων του δικτύου, το οποίο μπορεί να αποσπαστεί από το SIP URI και είναι το open-ims.test. Η συγκεκριμένη πληροφορία μπορεί να χρησιμοποιηθεί σε διαφορετικού τύπου επιθέσεις.

Συνεχίζοντας την ανάλυση της επικοινωνίας παρατηρούμε ότι το IMS δίκτυο είναι έτοιμο να αυθεντικοποιήσει τον χρήστη μέσω της διαδικασίας challenge-response που περιγράφηκε προηγουμένως.

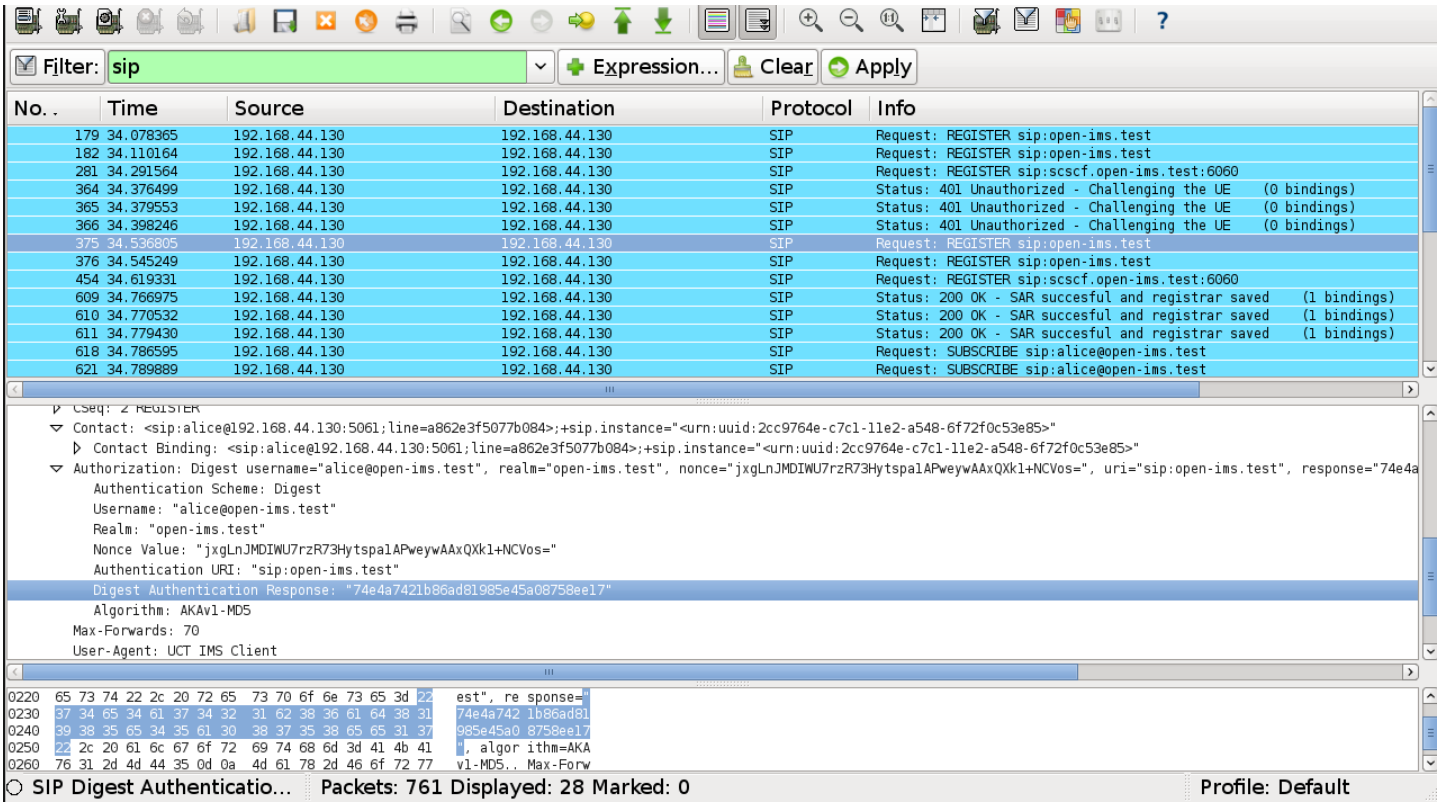
Το μήνυμα αυτό υποκλέπτεται επίσης από τον traffic analyzer που έχουμε στήσει στο IP δίκτυο (Εικόνα 29). Όπως παρατηρούμε και αυτό το μήνυμα είναι σε καθαρό κείμενο και η χρήση πληροφορία που αποσπάμε είναι η τιμή του Nonce και ο αλγόριθμος που χρησιμοποιείται και είναι ο AKAv1-MD5.



Εικόνα 29. Challenge του IMS προς το UE

Στην συνέχεια το τερματικό υπολογίζει το Digest Authentication Response, ώστε να γίνει η αυθεντικοποίηση του χρήστη. Ο υπολογισμός αυτός γίνεται με βάση το Digest που έλαβε το τερματικό από το δίκτυο και με τον κωδικό χρήστη που διαθέτει.

Η απόκριση αυτή του τερματικού λαμβάνεται από τον traffic analyzer και όπως στις προηγούμενες περιπτώσεις, έτσι και τώρα η απόκριση είναι σε καθαρό κείμενο και υποκλέπτεται.

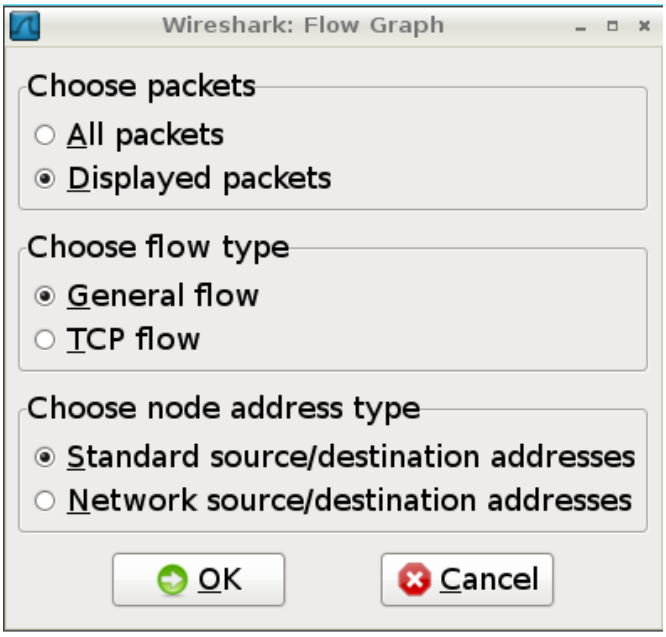


Εικόνα 30. Register από το UE προς τον P-CSCF με υπολογισμένο το digest

Την παραπάνω ανταλλαγή μηνυμάτων μπορούμε μέσω ειδικού εργαλείου του wireshark τα απεικονίσουμε και γραφικά.

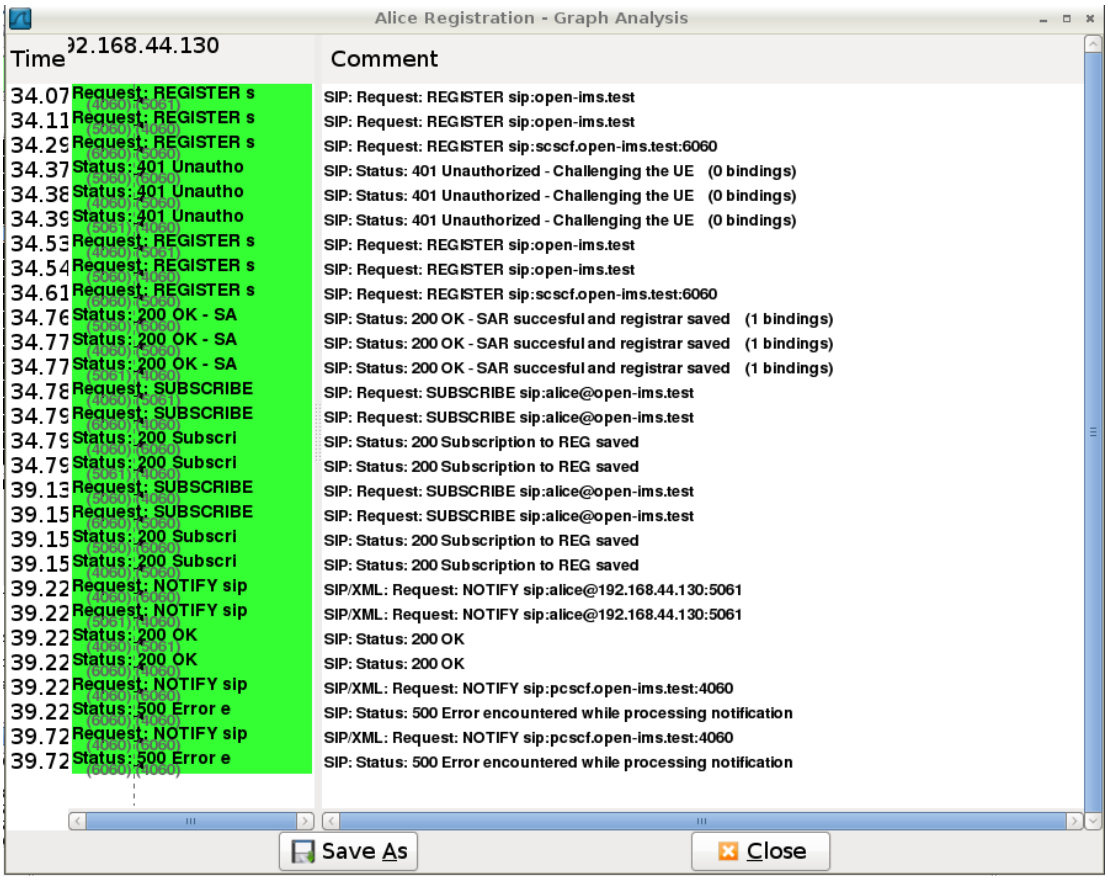
Πηγαίνοντας στο μενού Statistics/Flow Graph έχουμε την επιλογή να απεικονίσουμε σε ένα διάγραμμα ροής την ανταλλαγή των μηνυμάτων που έχουμε συλλάβει.

Επιλέγουμε αντίστοιχα να εμφανίσουμε τα πακέτα σύμφωνα με το φίλτρο που έχουμε εισάγει (SIP πακέτα μόνο), τον τύπο του διαγράμματος ροής που είναι ο γενικός και την βασική μορφή απεικόνισης δηλαδή source και destination διευθύνσεις των πακέτων (εικόνα 31).



Εικόνα 31. Επιλογές Διαγράμματος Ροής

Τελικά στην εικόνα 32 βλέπουμε το διάγραμμα ροής της εγγραφής του χρήστη Alice στο δίκτυο με όλα τα μηνύματα που ανταλλάχτηκαν με το IMS, όπως το συλλέξαμε με το wireshark, του κωδικούς SIP κάθε πακέτου, το domain, τους κόμβους που αποστέλλονται τα μηνύματα και την διάρκεια όλης της διαδικασία που είναι κοντά στα 5 δευτερόλεπτα.



Εικόνα 32. Διάγραμμα Ροής Registration Χρήστη Alice

Με την παραπάνω διαδικασία καταφέραμε να υποκλέψουμε:

- Την ταυτότητα του χρήστη.
- Η IP του χρήστη.
- Το domain του δικτύου.
- Το Digest που αποστέλλει το IMS.
- Το Digest Authentication Response που αποστέλλει το UE ως απάντηση στο αρχικό.
- Και τον αλγόριθμο που χρησιμοποιείται (AKAv1-MD5).

Με τις παραπάνω πληροφορίες έχει αφενός καταλυθεί η ιδιωτικότητα του χρήστη και αφετέρου μπορεί να ανακτηθεί και ο κωδικός του με χρήστη μεθόδων reverse engineering.

Έτσι θα είναι δυνατή η εγγραφή ενός ψεύτικου τερματικού στο δίκτυο και με αυτό τον τρόπο ο γνήσιος χρήστης δεν θα έχει υπηρεσίες αλλά παράλληλα θα χρεώνεται λανθασμένα.

7.1.1 Αντίμετρο στην Επίθεση Υποκλοπής της Ταυτότητας του Χρήστη

Για να αντιμετωπίσουμε παρόμοιες επιθέσεις που περιγράφηκε και πραγματοποιήθηκε στο προηγούμενο υποκεφάλαιο θα χρησιμοποιήσουμε τον μηχανισμό ασφαλείας TLS, που σκοπό του έχει να κρυπτογραφήσει την κίνηση σηματοδοσίας μεταξύ του τερματικού χρήστη και του P-CSCF, δηλαδή στην ουσία την επικοινωνία του UE με το IMS δίκτυο, στο οποίο κομμάτι τα δεδομένα των χρηστών και του δικτύου είναι ευάλωτα σε επιθέσεις.

Για να ενεργοποιήσουμε τον μηχανισμό ασφαλείας στο OpenIMS Core πρώτα από όλα πρέπει να κάνουμε compile το παρακάτω module:

```
cd /opt/OpenIMSCore/
make all include_modules=tls
```

Απαραίτητη προϋπόθεση είναι να έχουμε εγκατεστημένο στο λειτουργικό μας σύστημα το πακέτο OpenSSL. Στην συνέχεια κανουμε compile τις παρακάτω παραμέτρους:

```
make all include_modules=tls TLS_EXTRA_LIBS="-lz -lkrb5"
```

Στην συνέχεια πρέπει να ορίσουμε τα πιστοποιητικά που θα χρησιμοποιηθούν από το P-CSCF. Το OpenIMS Core έχει έτοιμο script για την δημιουργία πιστοποιητικών. Παρακάτω φαίνεται η εκτέλεση αυτού του script:

```
/opt/OpenIMSCore/ser_ims/cfg/tls_prepare.sh
```

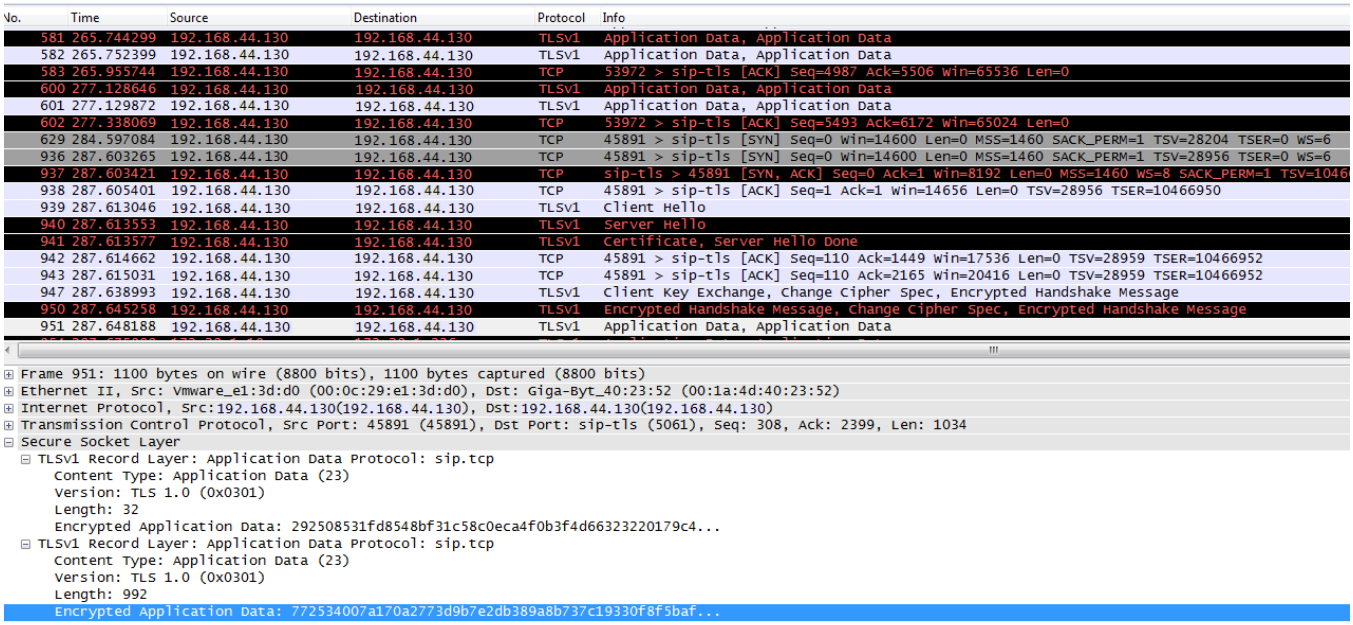
Στην συνέχεια πρέπει να κάνουμε κάποιες τροποποιήσεις στο κώδικα του P-CSCF ώστε να υποστηρίξει τον μηχανισμό ασφάλειας TLS. Ανοίγουμε τον κώδικα του P-CSCF και προσθέτουμε τα παρακάτω στοιχεία:

```
listen=tls:127.0.0.1

tls_port_no=4061

enable_tls=yes

...

modparam("pcscf","use_tls",1)

modparam("pcscf","tls_port",4061)

...

loadmodule "/opt/OpenIMSCore/ser_ims/modules/tls/tls.so"

modparam("tls", "tls_method", "TLSv1")

modparam("tls",                              "private_key",
"/opt/OpenIMSCore/PCSCF_CA/pcscf_private_key.pem")

modparam("tls",                              "certificate",
"/opt/OpenIMSCore/PCSCF_CA/pcscf_cert.pem")

modparam("tls",                                  "ca_list",
"/opt/OpenIMSCore/PCSCF_CA/pcscf_ca_list.pem")

modparam("tls", "verify_certificate", 1)

modparam("tls", "require_certificate", 0)

modparam("tls", "tls_disable_compression", 1)
```

Μετά από τις παραπάνω ρυθμίσεις είμαστε έτοιμοι να χρησιμοποιήσουμε τον μηχανισμό ασφάλειας TLS μεταξύ του τερματικού χρήστη και του P-CSCF (IMS δίκτυο), απλώς επιλέγοντας στον client να χρησιμοποιήσει TLS.

Αφού έχουμε κάνει τις προηγούμενες ενέργειες εκτελούμε εκ νέου το σενάριο επίθεσης man-in-the-middle με χρήστη του traffic analyzer wireshark. Και σε αυτή την περίπτωση το τερματικό κατά την εκκίνησή του προχωράει στην εγγραφή του στο δίκτυο με αποστολή του μηνύματος REGISTER.

Στην εικόνα 31 φαίνονται τα πακέτα που έχουμε κάνει capture ως επιτιθέμενοι. Είναι εμφανές ότι το συγκεκριμένο πακέτο, περάν από την IP διεύθυνση του χρήστη, δεν μπορεί να μας αποφέρει τίποτα το χρήσιμο, καθώς είναι κρυπτογραφημένο. Η IP διεύθυνση δεν θα μπορούσε να είναι κρυπτογραφημένη καθώς η πληροφορία αυτή χρειάζεται στους ενδιάμεσους κόμβους για λόγους δρομολόγησης.



Εικόνα 33. Μήνυμα REGISTER με χρήση TLS

Από την παραπάνω μελέτη που διεξήγαμε είναι εμφανές ότι ο μηχανισμός ασφάλειας TLS κρίνεται επιτυχημένος και αποτελεσματικός, καθώς προστατεύτηκε η ιδιωτικότητα του χρήστη που χρησιμοποιεί το πρωτόκολλο SIP για την μεταφορά της σηματοδοσίας πάνω από το IP δίκτυο.

Ο παραπάνω μηχανισμός έρχεται σε απόλυτη αρμονία με τον μηχανισμό αυθεντικοποίησης του χρήστη που χρησιμοποιεί το δίκτυο IMS μέσω της συνάρτησης σύνοψης AKAv.1-MD5 για την χρήση του μηχανισμού challenge-response.

Οι παραπάνω δύο μηχανισμοί κρίνονται συνδυαστικά άρτιοι και οι καταλληλότεροι για την προστασία της ιδιοτικότητας του χρήστη σε περιβάλλοντα IMS, τα οποία

χρησιμοποιούν μη έμπιστα IP δίκτυα κορμού, καθώς μπορεί να χρησιμοποιηθεί και hop-by-hop.

7.2 Κίνδυνος Συνακροάσεων

Ένας μεγάλος κίνδυνος που διατρέχει την ιδιωτικότητα των χρηστών υπηρεσιών VoIP είναι λήψη των πακέτων που μεταφέρουν την φωνή και η αποκάλυψή τους σε τρίτο κακόβουλο πρόσωπο, το οποίο μπορεί τελικά να κάνει ανάλυσή των πακέτων και να ακούσει την συνομιλία μεταξύ των δύο μερών.

Ο κίνδυνος αυτός αυξάνεται στα δίκτυα νέας τεχνολογίας που χρησιμοποιούν δίκτυα IP, όπως είναι και τα δίκτυα IMS που εξετάζουμε. Ο κίνδυνος σε αυτά τα δίκτυα είναι αυξημένος, λόγω της ελεύθερης φύσης των IP δικτύων και της αδυναμίας ελέγχου σε πολλούς ενδιάμεσους κόμβους, οι οποίοι μπορούν να είναι υπό τον έλεγχο κακόβουλων χρηστών και να οδηγήσουν σε επιθέσεις τύπου man-in-the-middle.

Παρακάτω θα πραγματοποιήσουμε μια επίθεση υποκλοπής συνομιλίας δύο χρηστών οι οποίοι χρησιμοποιούν υπηρεσίες τηλεφωνίας στο δίκτυο IMS, με την βοήθεια του OpenIMS Core που έχουμε υλοποιήσει και του wireshark traffic analyzer.

Στην συνέχεια θα προτείνουμε και θα εφαρμόσουμε τα κατάλληλα αντίμετρα για την διασφάλιση της ιδιωτικότητας των χρηστών του IMS δικτύου.

7.2.1 Επίθεση Υποκλοπής Συνομιλίας Χρηστών IMS

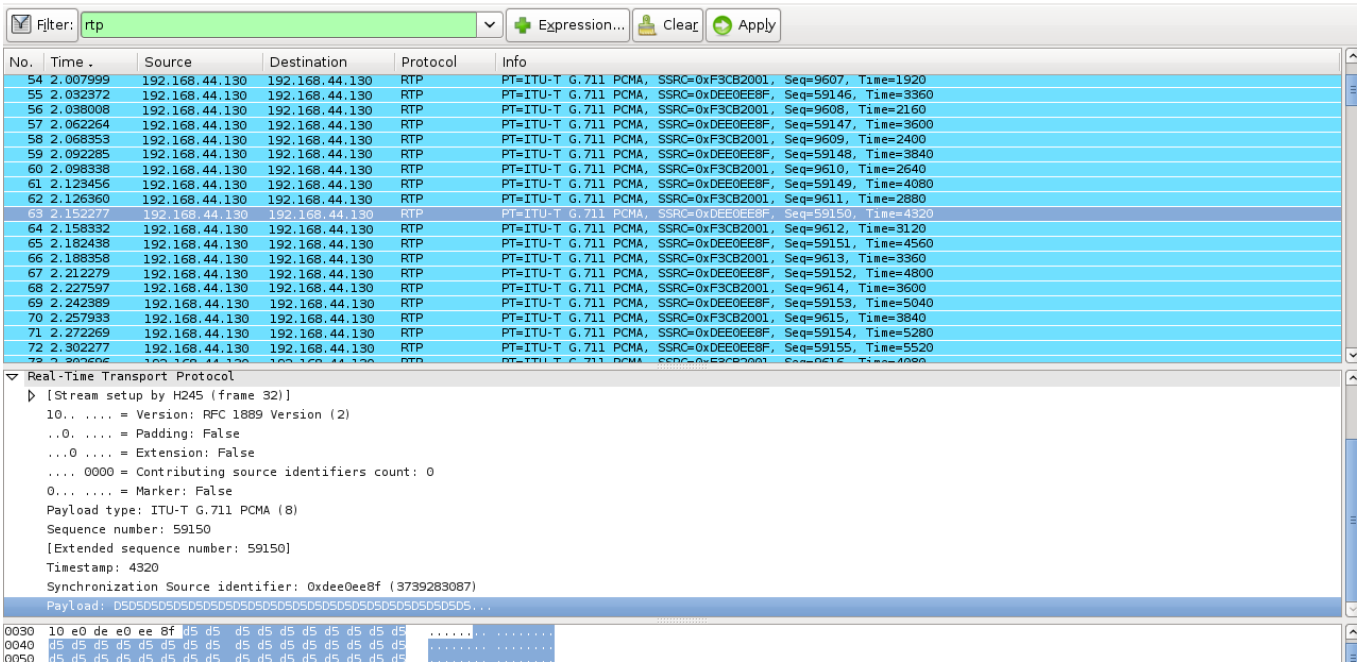
Όπως αναφέραμε και παραπάνω τα δίκτυα IMS χρησιμοποιούν για την μεταφορά των πολυμέσων το πρωτόκολλο RTP. Η χρησιμοποίηση της υποδομής IP δικτύων κάνουν δυνατή την λήψη του RTP Stream από κακόβουλους χρήστες με σκοπό την κατάλυση της ιδωτικότητας των συνομιλητών.

Έτσι με τον traffic analyzer wireshark που έχουμε στήσει στο IMS δίκτυο θα προσπαθήσουμε να πραγματοποιήσουμε επίθεση τύπου man-in-the-middle και να αναλύσουμε το RTP stream που θα λάβουμε.

Το wireshark έχει ρυθμιστεί να λαμβάνει πακέτα από το IP δίκτυο πάνω από το οποίο πραγματοποιείται η μεταφορά των πακέτων από και προς τον χρήστη. Στην υλοποίησή μας του OpenIMS Core διενεργούμε κλήση από τον χρήστη Alice προς τον χρήστη Bob. Όταν ολοκληρωθεί η ανταλλαγή της σηματοδοσίας SIP και γίνει η εγκαθίδρυση της σύνδεσης, αρχίζει η ανταλλαγή RTP πακέτων, όπως λαμβάνουμε και στο wireshark (Εικόνα 32).

Όπως παρατηρούμε βλέπουμε σε καθαρό κείμενο την κωδικοποίηση που χρησιμοποιείται στο payload του RTP πακέτου, που στην περίπτωσή μας είναι ο κώδικας G.711 και τελικά το ίδιο το payload του πακέτου (εικόνα 32).

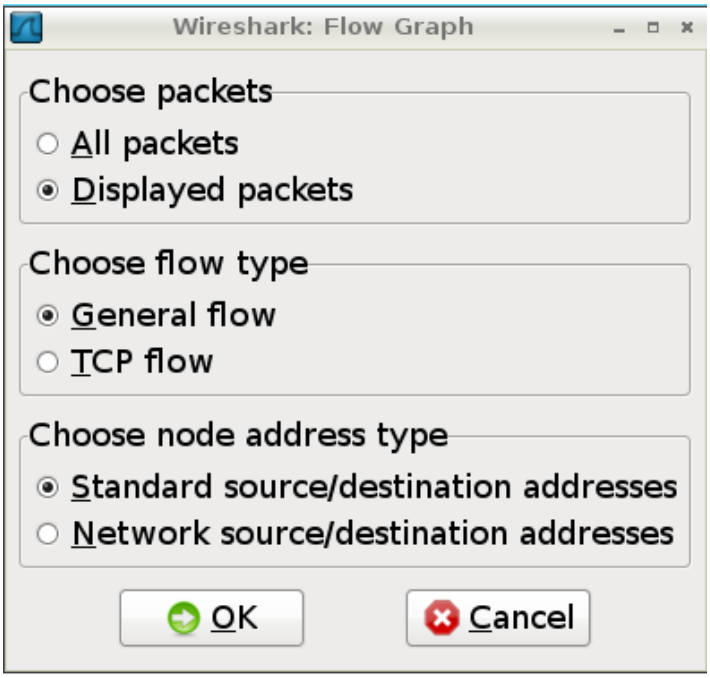
Έχοντας λάβει το RTP stream με την συνομιλία μεταξύ των χρηστών Alice και Bob θα προσπαθήσουμε να αναλύσουμε τα δεδομένα αυτά.



Εικόνα 34. Υποκλοπή πακέτων RTP

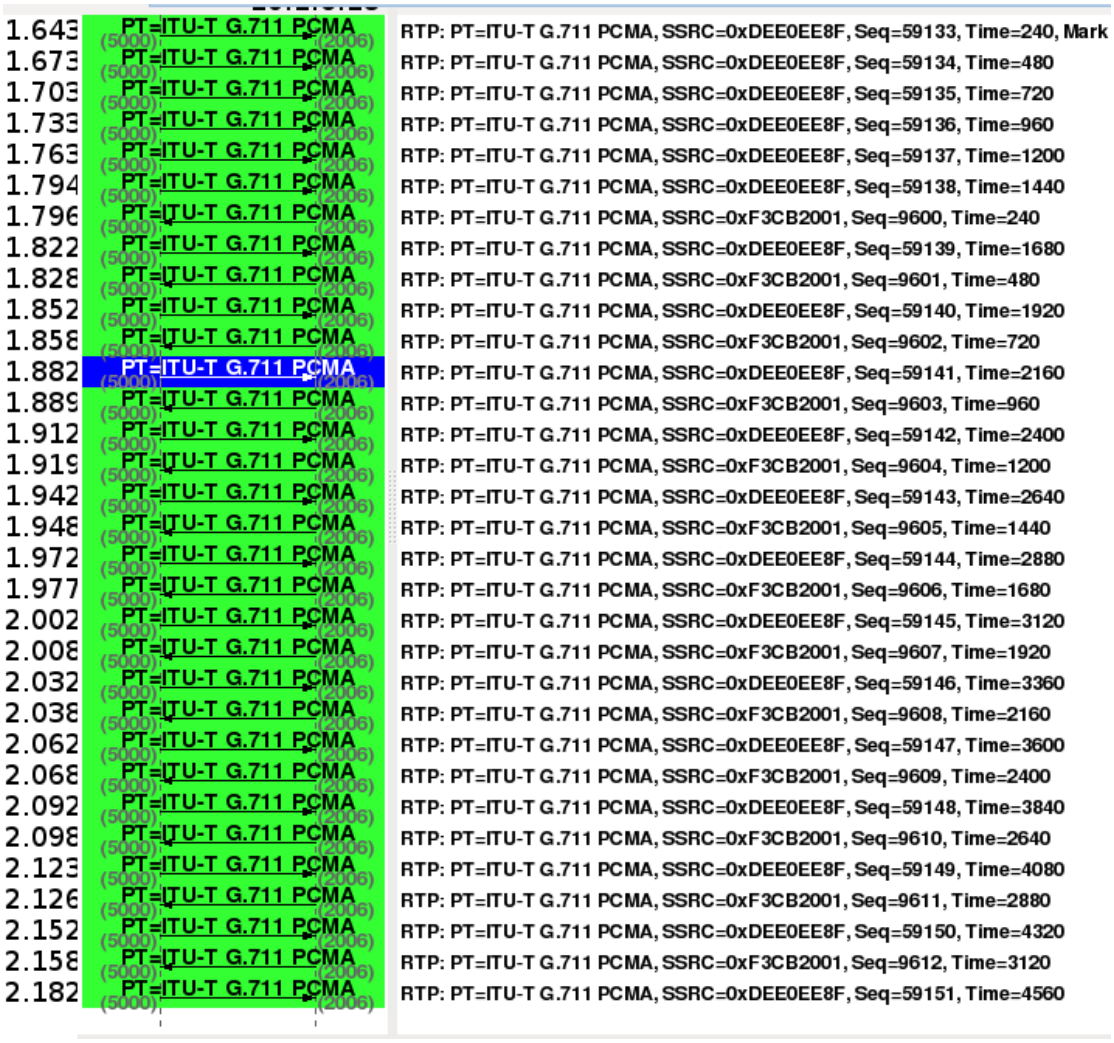
Χρησιμοποιώντας το εργαλείο wireshark και πηγαίνοντας στο μενού Statistics/Flow Graph έχουμε την επιλογή να απεικονίσουμε σε ένα διάγραμμα ροής την ανταλλαγή των μηνυμάτων που έχουμε συλλάβει.

Επιλέγουμε αντίστοιχα να εμφανίσουμε τα πακέτα σύμφωνα με το φίλτρο που έχουμε εισάγει (RTP πακέτα μόνο), τον τύπο του διαγράμματος ροής που είναι ο γενικός και την βασική μορφή απεικόνισης δηλαδή source και destination διευθύνσεις των πακέτων (εικόνα 33).



Εικόνα 35. Επιλογές Διαγράμματος Ροής

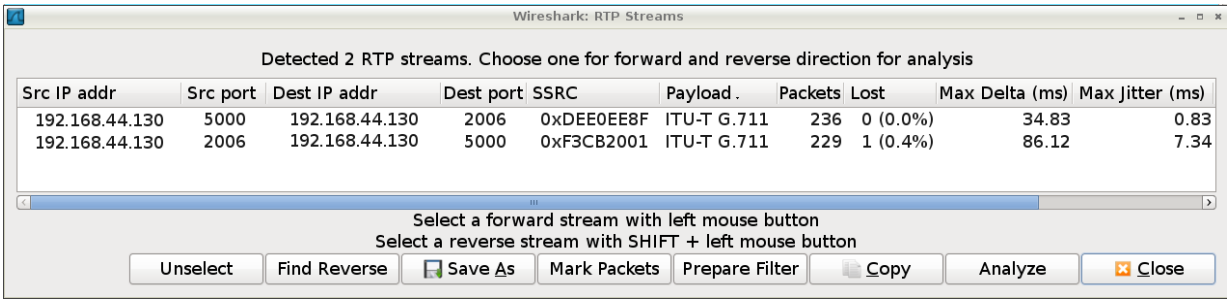
Τελικά στην εικόνα 34 βλέπουμε το διάγραμμα ροής του RTP stream που ανταλλάχτηκε, όπως το συλλέξαμε με το wireshark, την κωδικοποίηση κάθε πακέτου και τον χρόνο της κλήσης, που βλέπουμε ότι είναι κοντά στα 7 δευτερόλεπτα.



Εικόνα 36. Διάγραμμα ροής RTP Stream

Σε αυτό το σημείο θα ξεχωρίσουμε τις ροές και θα προσπαθήσουμε να τις αποκωδικοποιήσουμε με σκοπό τελικά να ακούσουμε την συνομιλία των δύο μερών.

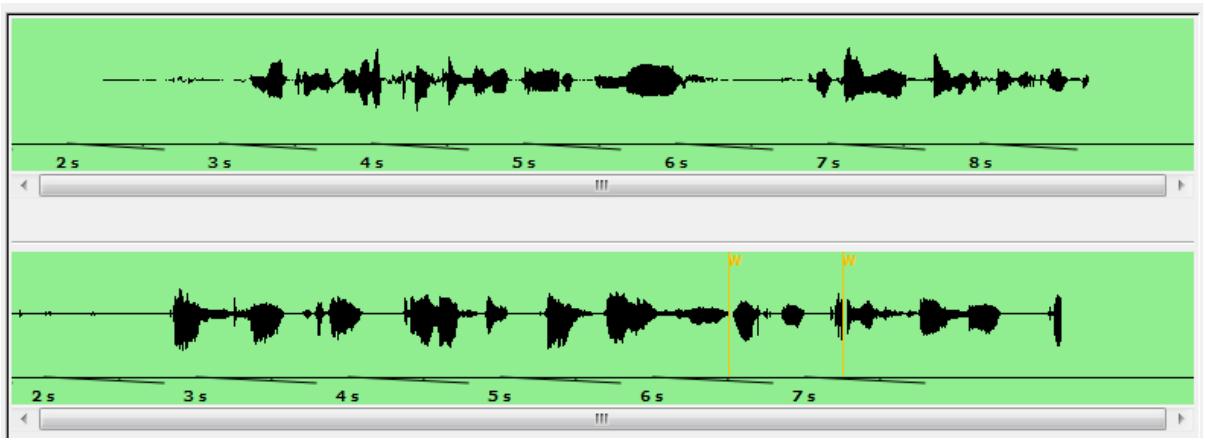
Στο wireshark, έχοντας την ροή δεδομένων RTP, επιλέγουμε το αντίστοιχο εργαλείο στο μενού Telephony/RTP/Show all streams. Στην εικόνα 35 βλέπουμε τις δύο ροές δεδομένων που έχουμε κάνει capture, μία από τον χρήστη Alice και μία από την χρήστη Bob.



Εικόνα 37. Οι ροές RTP των χρηστών Alice/Bob

Χρησιμοποιώντας αντίστοιχο εργαλείο του wireshark επιλέγουμε Telephony/RTP/Stream Analysis και επιλέγουμε να κάνουμε decode τις δύο ροές δεδομένων RTP. Τα αποτελέσματα του decode φαίνονται στην εικόνα 36, με αποτέλεσμα να μπορούμε να ακούσουμε την συνομιλία της Alice και του Bob.

Με αυτό τον τρόπο έγινε μια επιτυχής επίθεση υποκλοπής συνομιλίας στο δίκτυο IMS.



Εικόνα 38. Η φωνή που μεταδόθηκε από την Alice και τον Bob

7.2.2 Αντίμετρο στην Επίθεση Υποκλοπής Συνομιλίας Χρηστών IMS

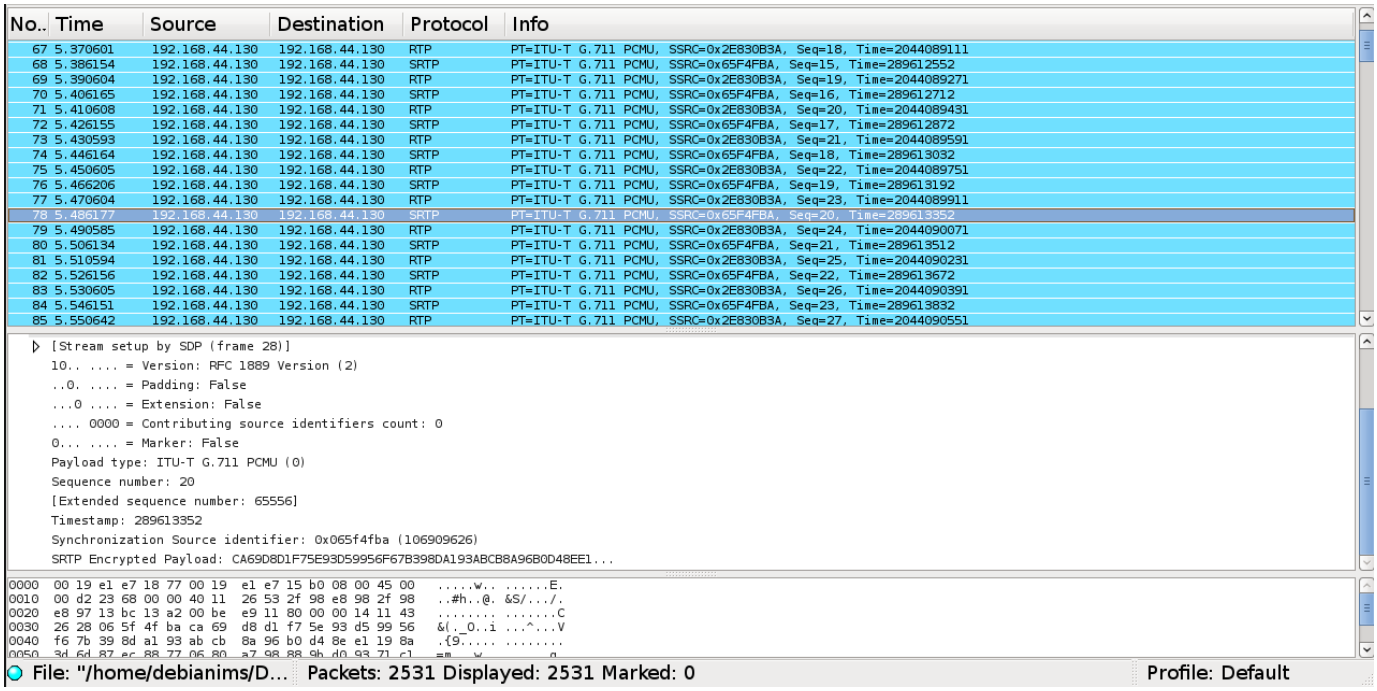
Μετά την επιτυχημένη επίθεση υποκλοπής της συνομιλίας χρηστών του δικτύου IMS που εκτελέσαμε στο προηγούμενο υποκεφάλαιο θα προτείνουμε αντίμετρο για να αντιμετωπιστούν παρόμοιες επιθέσεις στα δίκτυα αυτά.

Για τον σκοπό αυτό θα χρησιμοποιήσουμε το πρωτόκολλο SRTP (Secure RTP) στα δύο τερματικά άκρα και θα εκτελέσουμε εκ νέου την κλήση μεταξύ των χρηστών Alice και Bob. Στην συνέχεια θα δοκιμάσουμε να υποκλέψουμε την συνομιλία και να αξιολογήσουμε τελικά την αποτελεσματικότητα του αντίμετρου.

Το πρωτόκολλο SRTP αποτελεί την επέκταση του πρωτοκόλλου RTP, με στόχο την ασφάλεια της ροής δεδομένων. Χρησιμοποιεί την κρυπτογράφηση των πακέτων της ροής με σκοπό να επιτύχει την ακεραιότητα των μηνυμάτων αλλά, την αυθεντικότητά τους και τελικά την ιδιωτικότητα των τερματικών χρηστών.

Αφού εφαρμόσουμε SRTP στα άκρα, διενεργούμε στο OpenIMS Core που έχουμε στήσει την κλήση μεταξύ των χρηστών Alice και Bob και όπως κινηθήκαμε και προηγουμένως, υποκλέπτουμε τα πακέτα της συνομιλίας.

Απομονώνουμε τελικά μέσω των φίλτρων του wireshark το SRTP stream και τα αποτελέσματα φαίνονται στην εικόνα 37.



Εικόνα 39. Υποκλοπή πακέτων SRTP

Όπως παρατηρούμε τα πακέτα που έχουμε κάνει capture περιέχουν πληροφορία σε κρυπτογραφημένη και ακατάληπτη μορφή με αποτέλεσμα να μην υπάρχει κάποιο χρήσιμο δεδομένο για ανάλυση από τον επιτιθέμενο.

Προσπαθώντας να κάνουμε decode τα πακέτα που λάβαμε, όπως στην προηγούμενη περίπτωση με το RTP, δεν καταφέρνουμε να ανακτήσουμε και να ακούσουμε την φωνή των συνομιλητών.

Από την παραπάνω μελέτη που διεξήγαμε είναι εμφανές ότι ο μηχανισμός ασφάλειας SRTP κρίνεται επιτυχημένος και αποτελεσματικός, καθώς προστατεύτηκε η ιδιωτικότητα του χρήστη που χρησιμοποιεί το πρωτόκολλο RTP για την μεταφορά της φωνής πάνω από το IP δίκτυο.

Ο παραπάνω μηχανισμός έρχεται σε συνεργασία με την ασφάλεια TLS που αναλύσαμε σε προηγούμενο υποκεφάλαιο αλλά και τον μηχανισμό αυθεντικοποίησης του χρήστη που χρησιμοποιεί το δίκτυο IMS μέσω της συνάρτησης σύνοψης AKAv.1-MD5 για την χρήση του μηχανισμού challenge-response αποτελούν ένα ολοκληρωμένο πακέτο ασφάλειας για τα IMS δίκτυα και την εξασφάλιση της ιδιωτικότητας των χρηστών τους.

7.3 Κίνδυνος Επίθεσης στο Δίκτυο του IMS

Αφού εφαρμόσαμε στα προηγούμενα υποκεφάλαια επιθέσεις που έθιξαν την ιδιωτικότητα των χρηστών με επιθέσεις πάνω στην σηματοδοσία και την ροή των πολυμέσων των χρηστών, θα μελετήσουμε την δυνατότητα επίθεσης στο ίδιο το IMS δίκτυο, στοχεύοντας στην διαθεσιμότητά του.

Όπως αναφέραμε προηγουμένως οι κόμβοι του IMS είναι αποκλεισμένοι και καλά προστατευμένοι από το εξωτερικό περιβάλλον, όπου βρίσκονται οι χρήστες. Ο P-CSCF μας παρέχει κάποιες υπηρεσίες ασφάλειας για το IMS δίκτυο όπως για παράδειγμα απόκρυψη της τοπολογίας του δικτύου και γενικά αποτελεί τον διαμεσολαβητή μεταξύ του IP δικτύου κορμού και του δικτύου κορμού του IMS. Επίσης πολλά δίκτυα εφαρμόζουν στην αρχιτεκτονική τους για έξτρα ασφάλεια την εγκατάσταση κόμβου SGC, οποίος αποτελεί ένα τοίχος προστασίας για το δίκτυο.

Όλα τα παραπάνω καθιστούν πολύ δύσκολη την επίθεση στους κόμβους του IMS. Υπάρχει όμως ένας έμμεσος τρόπος επίθεσης στο IMS Core, η οποία θα οδηγήσει στην μη διαθεσιμότητα του δικτύου και πάνω σε αυτή θα βασιστούμε για την εφαρμογή επίθεσης στο δίκτυο του IMS.

Το IMS χρησιμοποιεί για την ανακάλυψη και τελικά την επικοινωνία χρήστη-IMS αλλά την μεταξύ των κόμβων του IMS επικοινωνία έναν ή περισσότερους εξυπηρετητές DNS.

Οι εξυπηρετητές DNS, λόγω της ανάγκης να αποδέχονται αιτήματα των πελατών αλλά και των κόμβων του IMS είναι ανοιχτοί και εξωτερικά και εσωτερικά του IMS. Μια λανθασμένη ρύθμιση σε αυτούς ή μια γνωστή αδυναμία τους (exploit) μπορεί να τους κάνει ευάλωτους σε επιθέσεις.

Μια επιτυχημένη επίθεση σε εξυπηρετητή DNS μπορεί να οδηγήσει σε κατάρρευση του IMS δικτύου καθώς δεν θα είναι δυνατή η αντιστοίχηση των domains που γνωρίζουν οι κόμβοι αλλά και οι χρήστες με IP διευθύνσεις έτσι ώστε να καταστεί τελικά δυνατή επικοινωνία.

Παρακάτω θα δοκιμάσουμε να εφαρμόσουμε μια τέτοιου τύπου επίθεση στην διάταξή του OpenIMS Core που έχουμε υλοποιήσει και θα μελετήσουμε και κατάλληλους τρόπους αντιμετώπισής τους.

7.3.1 Επίθεση DNS Cache Poisoning

Οι επιθέσεις τύπου DNS Cache poisoning έχουν ως στόχο την επίθεση στην προσωρινή βάση δεδομένων (cache database) των εξυπηρετητών DNS και έχουν ως αποτέλεσμα να επιστρέφονται λανθασμένες IP διευθύνσεις στους χρήστες που διενεργούν ερωτήματα με αποτέλεσμα να επιτυγχάνεται εκτροπή της κίνησης σε κακόβουλους κόμβους. Στην περίπτωση που μελετάμε, μια επίθεση DNS Cache Poisoning θα έχει ως αποτέλεσμα την εκτροπή της σηματοδοσίας του IMS δικτύου

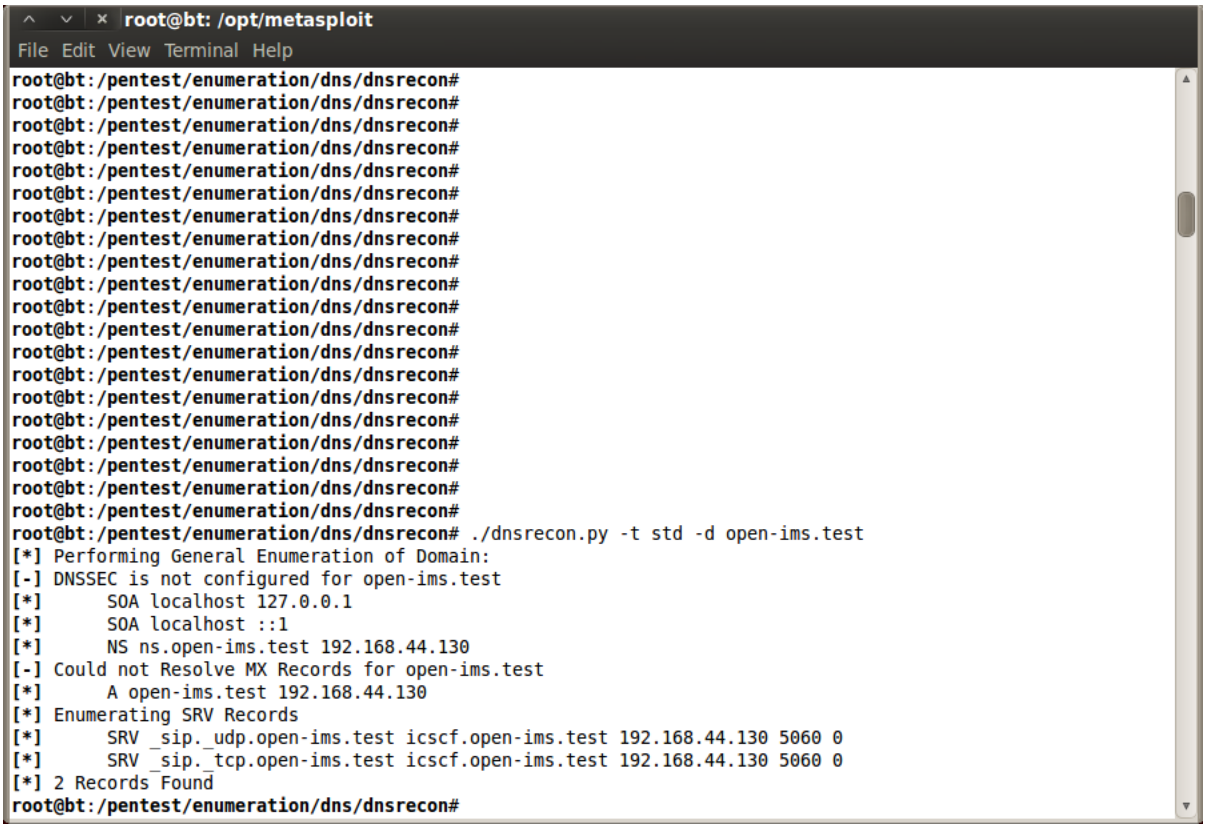
σε κόμβο που δεν θα μπορεί να την εξυπηρετήσει, με αποτέλεσμα να χαθεί η διαθεσιμότητα του δικτύου και των υπηρεσιών του.

Το IMS που έχουμε υλοποιήσει χρησιμοποιεί για το δίκτυό του έναν εξυπηρετητή DNS και συγκεκριμένα τον bind9. Για να πραγματοποιήσουμε μια επίθεση DNS Cache Poisoning θα προσπαθήσουμε να ανακαλύψουμε κάποια αδυναμία του bind9, την οποία μπορούμε να εκμεταλλευτούμε προς όφελός μας και να εκτρέψουμε την σηματοδοσία σε λάθος κόμβο.

Για τους σκοπούς της επίθεσης θα χρησιμοποιήσουμε έναν ξεχωριστό υπολογιστή που χρησιμοποιεί το λειτουργικό σύστημα Linux Backtrack 5 R3 και εκτελείται στο περιβάλλον μας μέσω της βοήθειας του VMware workstation 9.

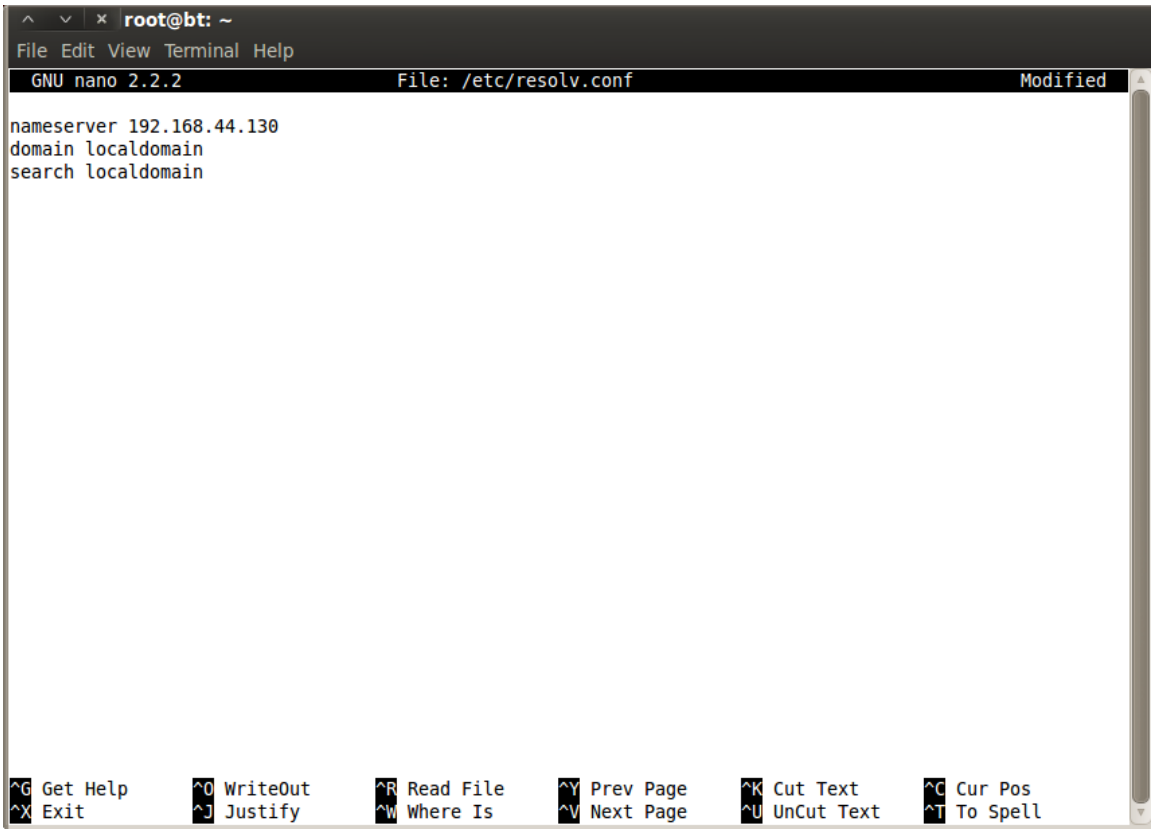
Από τις προηγούμενες επιθέσεις που εκτελέσαμε με τον traffic analyzer και την λήψη πακέτων σηματοδοσίας γνωρίζουμε το domain που χρησιμοποιεί το IMS δίκτυο το οποίο είναι το open-ims.test.

Από την στιγμή που γνωρίζουμε το domain του IMS δικτύου μπορούμε να χρησιμοποιήσουμε το εργαλείο του backtrack DNSrecon που βρίσκεται στην σουίτα DNS Analysis του Network Analysis στο Backtrack. Το αποτέλεσμα θα είναι να ανακαλύψουμε την IP διεύθυνση του DNS που θέλουμε να επιτεθούμε και είναι η 192.168.44.130 (Εικόνα 40). Ακόμα από την πρώτη ανάλυση του DNS που κάναμε ανακαλύπτουμε ότι ο DNS δεν εφαρμόζει τον μηχανισμό ασφάλειας DNSSec με αποτέλεσμα να έχουμε μια πρώτη αδυναμία του.



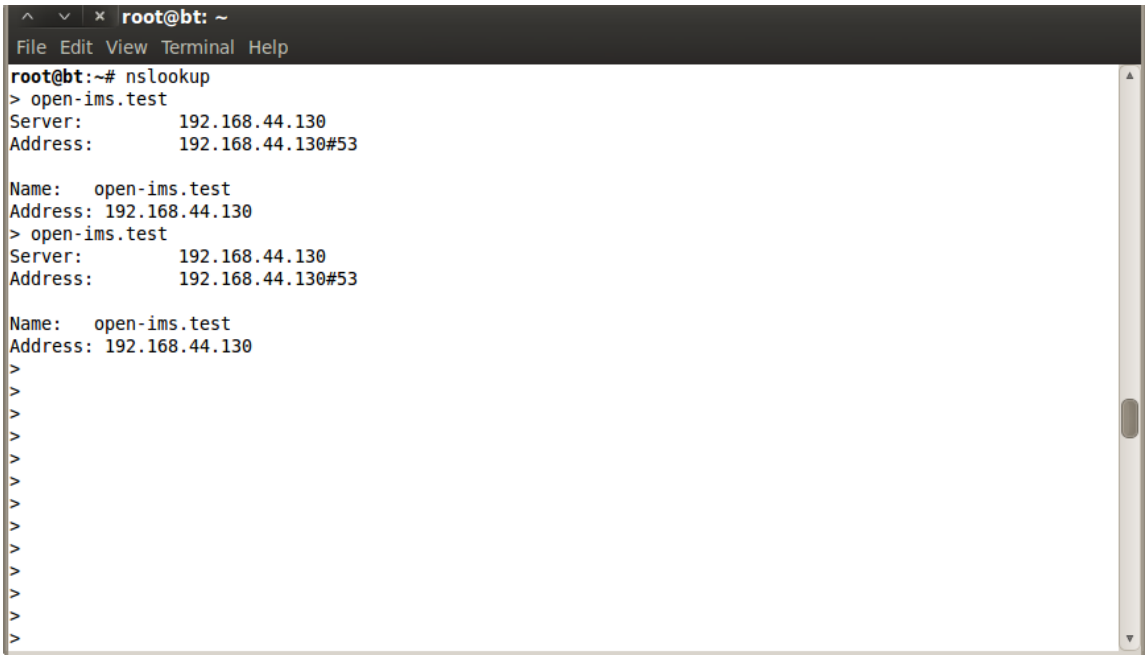
Εικόνα 40. DNSrecon Analysis

Από την στιγμή που γνωρίζουμε την IP διεύθυνση του DNS που θέλουμε να επιτεθούμε ρυθμίζουμε τον υπολογιστή μας να αποστέλλει τα DNS ερωτήματά του σε αυτόν (Εικόνα 41) και παράλληλα ρυθμίζουμε την IP διεύθυνση του υπολογιστή μας στο ίδιο υποδίκτυο με αυτό του DNS.



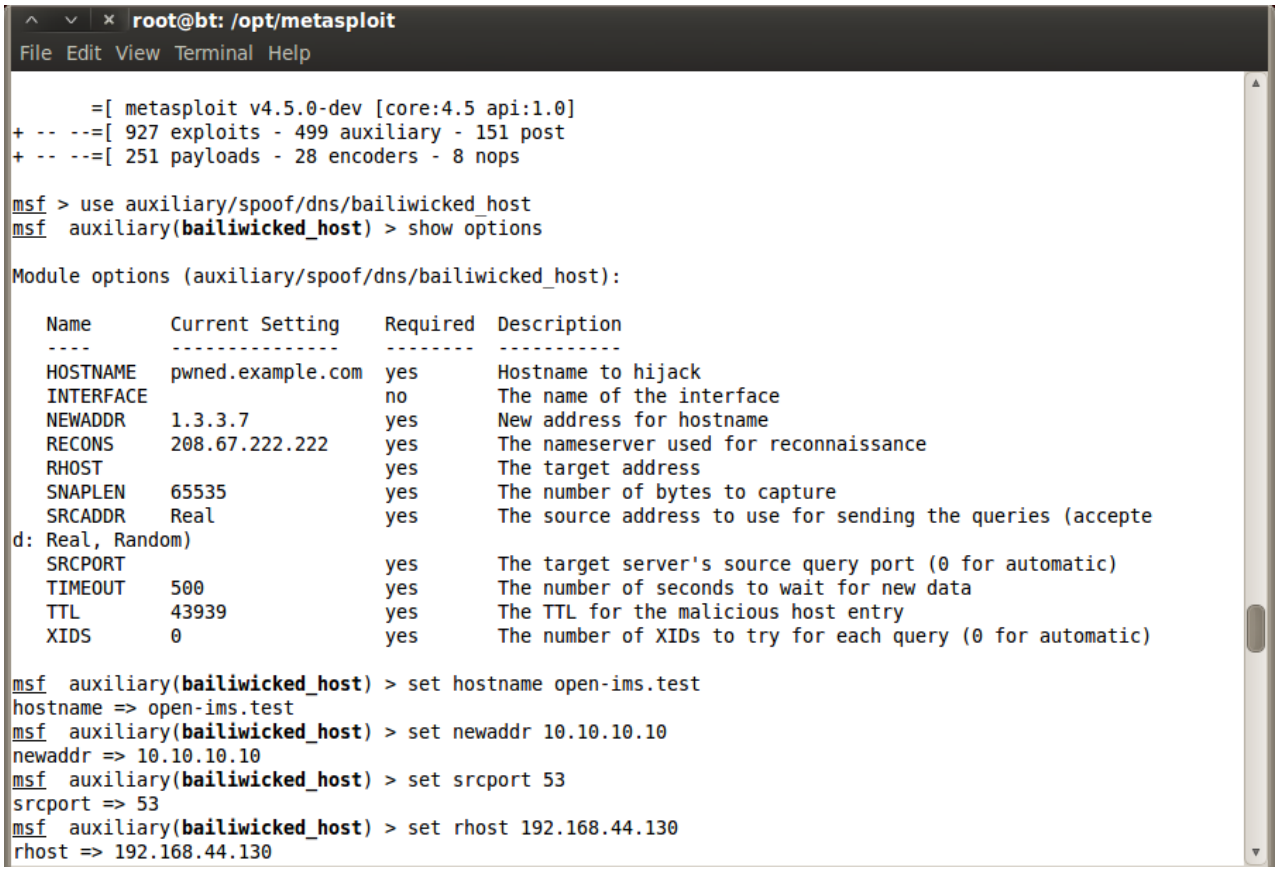
Εικόνα 41. Ρύθμιση του resolv.conf

Μέσω nslookup επιβεβαιώνουμε την ορθή λειτουργία του συστήματος (Εικόνα 42).



Εικόνα 42. Επιβεβαίωση ορθής λειτουργίας DNS

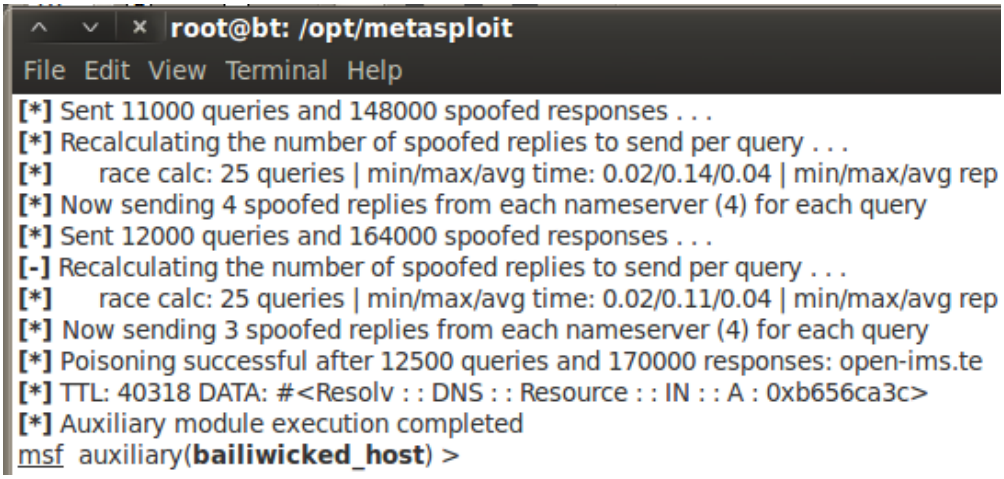
Στην συνέχεια ρυθμίζουμε το metasploit ώστε να πραγματοποιήσει το DNS cache poisoning για το domain open-ims.test εισάγοντας την λανθασμένη IP 10.10.10.10 ώστε να μην μπορεί να γίνει η δρομολόγηση προς τους κόμβους του IMS αλλά και την IP/πόρτα του εξυπηρετητή DNS (εικόνα 43).



Εικόνα 43. Ρύθμιση metasploit

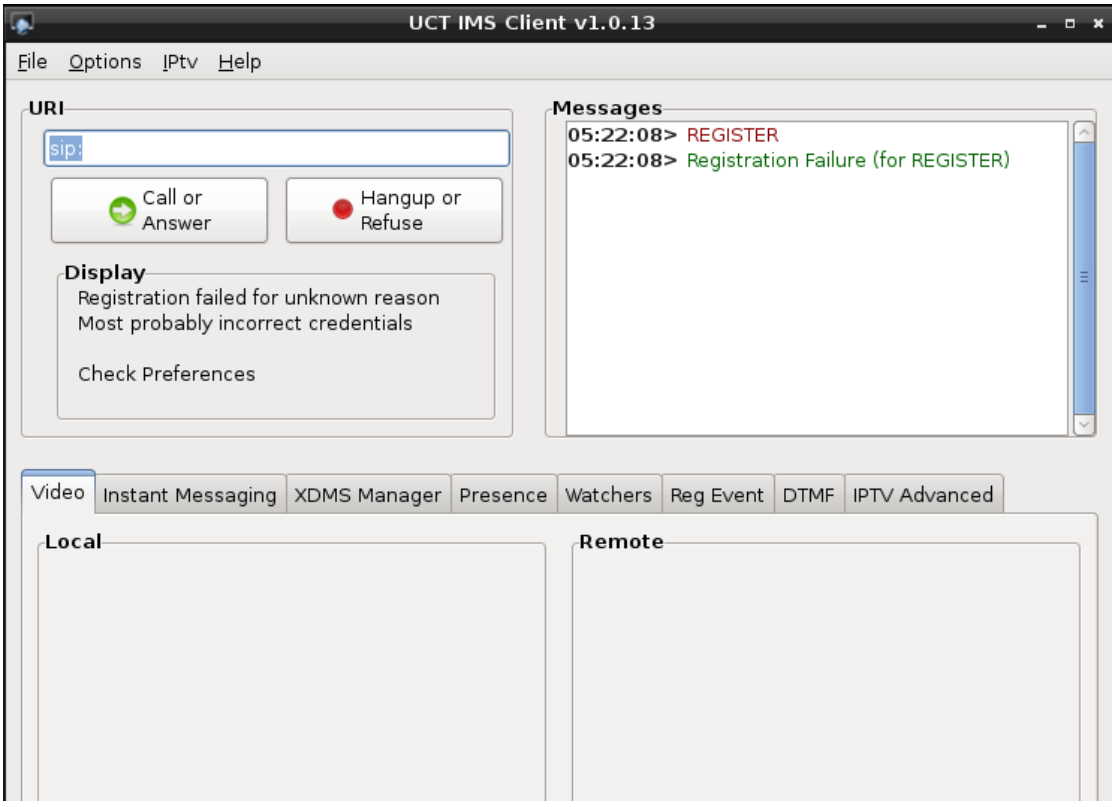
Μετά από τις παραπάνω ρυθμίσεις είμαστε έτοιμοι να εκτελέσουμε το exploit εις βάρος του εξυπηρετητή DNS του IMS core εκτελώντας την εντολή run (Εικόνα 44). Η εκτέλεση μπορεί να πάρει αρκετή ώρα μέχρι να ολοκληρωθεί καθώς πρέπει να λήξει η εγγραφή του DNS για το συγκεκριμένο domain ώστε να εισαχθεί η λανθασμένη IP στην συνέχεια.

Όπως φαίνεται στην εκτέλεση του script έχουμε τα spoofed πακέτα που ανεστάλησαν στον στόχο μας, τους σχετικούς χρόνους απόκρισης αλλά και τα πακέτα απόκρισης.



Εικόνα 44. Επιτυχής εκτέλεση του exploit

Τώρα θα προσπαθήσουμε να πραγματοποιήσουμε μια εγγραφή του χρήστη Alice στο IMS Δίκτυο για να δούμε τα αποτελέσματα της επίθεσής μας.



Εικόνα 45. Αποτυχημένη εγγραφή χρήστη στο IMS

Όπως φαίνεται από την εικόνα 45 η εγγραφή του χρήστη Alice το IMS δίκτυο απέτυχε. Ο λόγος της αποτυχίας είναι το γεγονός ότι ο DNS server που εξυπηρετεί το IMS δίκτυό μας κατευθύνει σε λανθασμένη IP (10.10.10.10) η οποία δεν υπάρχει

και δεν μπορεί να εξυπηρετήσει τα SIP αιτήματα που στέλνει το τερματικό του χρήστη.

Με αυτό τον τρόπο έχουμε επιτύχει μια επίθεση άρνησης υπηρεσίας (denial of service – DoS) αλλά παράλληλα έχει καταρρεύσει και η επικοινωνία μεταξύ των ίδιων των κόμβων του IMS οι οποίοι εξυπηρετούνται από τον ίδιο εξυπηρετητή DNS.

7.3.2 Αντίμετρο στην Επίθεση DNS Cache Poisoning

Για να αντιμετωπίσουμε επιθέσεις τύπου DNS Cache Poisoning θα ρυθμίσουμε κατάλληλα τον DNS που εξυπηρετεί το δίκτυο IMS που έχουμε υλοποιήσει, ώστε να δέχεται αιτήματα μόνο από έμπιστους κόμβους.

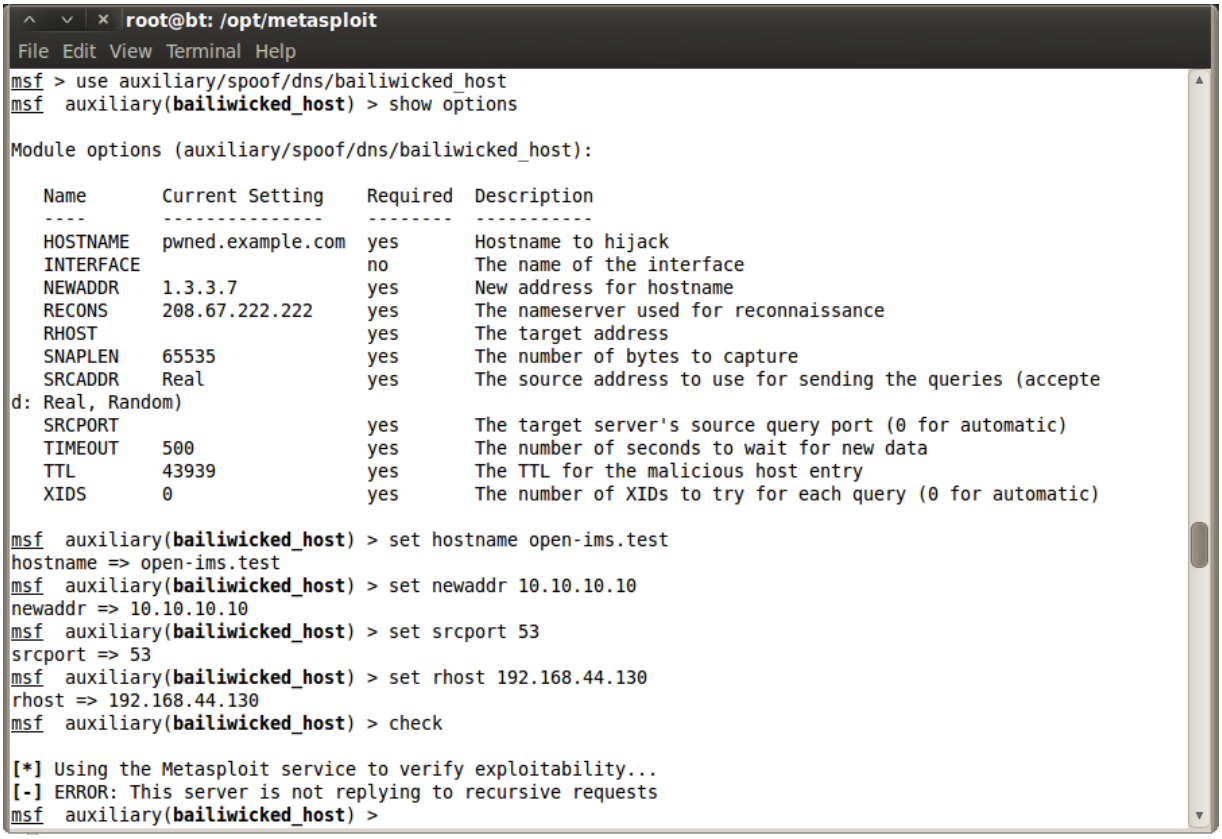
Το παραπάνω δεν θα μας επιφέρει κάποιο πρόβλημα στην λειτουργία του δικτύου καθώς ο συγκεκριμένος DNS δεν εξυπηρετεί διαδίκτυο και δεν υπάρχει λόγος να απαντά αιτήματα από μη έμπιστους κόμβους για domain που δεν εξυπηρετεί.

Για να κάνουμε την παραπάνω ρύθμιση που περιγράψαμε στον DNS μας προσθέτουμε στο αρχείο /etc/bind/named.conf.option τον παρακάτω κώδικα.

```
acl "trusted" {
      192.168.44.0/24;
      192.168.44.130; //Έμπιστη στατική IP
      localhost;
      localnets;
}
allow-query { any; };
allow-recursion { trusted; };
allow-query-cache { trusted; };
```

Τώρα θα προσπαθήσουμε να εκτελέσουμε εκ νέου την επίθεση για να δούμε τα αποτελέσματα. Εκτελούμε όπως περιγράψαμε στο προηγούμενο υποκεφάλαιο την επίθεση με χρήση του metasploit και παρατηρούμε ότι αυτή αποτυγχάνει καθώς δεν μπορεί ο μη έμπιστος εξοπλισμός που χρησιμοποιούμε ως επιτιθέμενοι να στείλει ερωτήματα στον DNS (εικόνα 46). Αντίθετα οι χρήστες αλλά και οι κόμβοι του IMS εξυπηρετούνται κανονικά.

Έτσι το αντίμετρο που χρησιμοποιήσαμε για την αντιμετώπιση της επίθεσης DNS cache poisoning κρίνεται επιτυχημένο.



Εικόνα 46. Επιτυχής αντιμετώπιση επίθεσης DNS Cache Poisoning

Πέραν της παραπάνω εφαρμογής για την αντιμετώπιση γενικότερων επιθέσεων στους DNS του IMS δικτύου θα πρέπει να γίνεται ένας γενικότερος σχεδιασμός όσον αφορά την ασφάλεια που να περιλαμβάνει χρήση πολλαπλών DNS Servers σε αρχιτεκτονική κατάλληλη ώστε ξεχωριστοί DNS να εξυπηρετεί τους χρήστες και ξεχωριστοί το δίκτυο. Με αυτό τον τρόπο ελαχιστοποιούνται οι πιθανότητες να δεχθεί επίθεση ένας εσωτερικός DNS αλλά παράλληλα την επίπτωση μιας επίθεσης σε έναν DNS που εξυπηρετεί χρήστες θα είναι περιορισμένη και ελεγχόμενη.

Ακόμα γενικότερη καλή τακτική ασφάλειας στα IMS δίκτυα είναι η εφαρμογή κόμβου SBC (Session Boarder Controller), οποίος όπως αναφέρθηκε παρέχει υπηρεσίες τοίχους προστασίας στο IMS και παρέχει μια ολοκληρωμένη ασφάλειας στο δίκτυο σε συνδυασμό με τις τακτικές που περιγράφηκαν στην παρούσα διπλωματική.

Κεφάλαιο 8

Συμπεράσματα

Έπειτα από την ανάλυση που έγινε στην παρούσα διπλωματική εργασία οι μηχανισμοί ασφάλειας TLS και SRTP κρίνονται αποτελεσματικοί για την διασφάλιση της ιδιωτικότητας και της εμπιστευτικότητας των χρηστών του δικτύου. Οι κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται είναι ισχυροί και επιτυγχάνουν την ιδιωτικότητα τόσο για τη σηματοδοσία όσο και τα πολυμέσα του δικτύου. Επίσης η χρήση της συνάρτησης σύνοψης AKA-MD5 με τη χρήση του μηχανισμού challenge/response για την αυθεντικοποίηση των χρηστών, προσδίδει ένα επιπλέον αρκετά ασφαλή μηχανισμό ταυτοποίησης του χρήστη.

Οι μηχανισμοί ασφάλειας TLS και SRTP όπως φάνηκε από την ανάλυση που έγινε λειτουργούν συμπληρωματικά και θα πρέπει να αντιμετωπίζονται σαν ένας μηχανισμός ασφάλειας. Η κρυπτογράφηση μόνο της σηματοδοσίας και η αποστολή των πολυμέσων σε καθαρή μορφή και αντίστροφα δεν μας επιφέρει ολοκληρωμένη ασφάλειας στην επικοινωνία χρήστη-IMS. Στην πρώτη περίπτωση που τα πολυμέσα μεταδίδεται σε καθαρή μορφή, επιτρέπει σε ένα κακόβουλο χρήση να υποκλέψει την συνομιλία. Στην δεύτερη περίπτωση, μέσω της σηματοδοσίας μεταφέρονται τα κρυπτογραφικά κλειδιά για το SRTP αλλά και άλλες χρήσιμες πληροφορίες για το δίκτυο, πράγμα που σημαίνει ότι με την υποκλοπή των δεδομένων αυτών είναι δυνατή η αποκρυπτογράφηση της φωνής. Έτσι θα πρέπει να γίνεται εφαρμογή και των δύο μηχανισμών ασφάλειας για να έχουμε ολοκληρωμένη ασφάλεια στο δίκτυό μας.

Ακόμα προσοχή πρέπει να γίνεται και στο δικτυακό επίπεδο καθώς όπως παρατηρήσαμε είναι εμφανής ο κίνδυνος εμφάνισης έμμεσης επίθεσης στην διαθεσιμότητα του IMS μέσω εξυπηρετητών όπως ο DNS, που σε πολλές περιπτώσεις αντιμετωπίζουν κενά ασφαλείας λόγω της φύσης τους.

Έτσι η ασφάλειας των δικτύων IMS απαιτεί μια σφαιρική μελέτη και εφαρμογή καθώς γίνεται χρήση πολλών σύγχρονων τεχνολογιών αιχμής για να προσφερθεί η τελική υπηρεσία στους χρήστες. Αυτή η χρήση πολλών τεχνολογιών στο IMS αποτελεί το όπλο του και χάρης αυτές γνωρίζει μεγάλη άνθηση αλλά απαιτεί παράλληλα μεγάλη προσοχή στην εφαρμογή σωστών μηχανισμών ασφάλειας σε όλους τους τομείς.

Βιβλιογραφία

[1] Alan B. Johnston, SIP: Understanding the Session Initiation Protocol, Second Edition, Artech House, 2004.

[2] David Endler & Mark Collier, Hacking VoIP Exposed: Voice Over IP Security Secrets and Solutions, McGraw-Hill Professional Publishing, 2007.

[3] Gonzalo Camarillo, Miguel A. Garcia-Martin, 3G IP Multimedia subsystem IMS – Merging the Internet and the Cellular Worlds, Second Edition, John Wiley & Sons LTD, 2006.

[4] Is-Haka Mkwawa, Emmanuel Jammeh, Lingfen Sun, Asiya Khan and Emmanuel Ifeachor, Open IMS Core with VoIP Quality Adaptation, University of Plymouth, 2009.

[5] Khalid Al-Begain, Chitra Balakrisha, Luis Angel Galindo & David Moro, The IMS: A Development and Deployment Perspective, John Wiley & Sons LTD, 2009.

[6] Miikka Poikselka & Georg Mayer, The IMS: IP Multimedia Concepts and Services, Third Edition, John Wiley & Sons LTD, 2009.

[7] Zhibi Wang & Alcatel-Lucent, IMS Security Framework, Version: 2.0 , 3GPP, 2008.

[8] http://www.3gpp.org/Technologies/Keywords-Acronyms/article/ims, last accessed 10/6/2013.

[9] https://en.wikipedia.org/wiki/IP_Multimedia_Subsystem, last accessed 10/6/2013.

[10] https://en.wikipedia.org/wiki/Session_Initiation_Protocol, last accessed 10/6/2013.

[11] https://kb.isc.org/article/AA-00913/0/BIND-9-Security-Vulnerability-Matrix.html, last accessed 10/6/2013.

[12] http://pic.dhe.ibm.com/infocenter/aix/v6r1/index.jsp?topic=%2Fcom.ibm.aix.commadmn%2Fdoc%2Fcommadmndita%2Fbind9.htm, last accessed 10/6/2013.

[13] http://uctimsclient.berlios.de/, last accessed 10/6/2013.

[14] http://www.debian.org/support, last accessed 10/6/2013.

[15] http://www.debian.org/security/2013/dsa-2656, last accessed 10/6/2013.

[16] http://www.eventhelix.com/ims/#.UbdVeOenAZl, last accessed 10/6/2013.

[17] http://www.openimscore.org/doc, last accessed 10/6/2013.