Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Ασφάλεια σε VOIP

Μπάκουλη Άννα

1/11/2012

Επιβλέπων καθηγητής :Λαμπρινουδάκης Κ.

ΕΥΧΑΡΙΣΤΙΕΣ

Κατά την διάρκεια της εκπόνησης της Διπλωματικής μου εργασίας υπήρξαν αρκετοί άνθρωποι που ο καθένας με τον δικό του τρόπο συνέβαλλαν σε αυτό και με βοήθησαν να φτάσω στο σημείο όπου η εργασία έχει φτάσει στο τέλος της και μπορώ πλέον να ευχαριστήσω τον καθένα ξεχωριστά.

Θα ξεκινήσω ευχαριστώντας τον καθηγητή μου κ. Λαμπρινουδάκη και όχι επειδή έτσι συνηθίζεται στις Διπλωματικές εργασίες αλλά επειδή είναι ένας εξαιρετικός καθηγητής και άνθρωπος και είχα την τιμή και την χαρά να τον γνωρίσω και να συνεργαστώ μαζί του. Θα ήθελα να του εκφράσω την εκτίμηση και την ευγνωμοσύνη μου για την καθοδήγηση και την κατανόηση καθ' όλη την διάρκεια την συνεργασίας μας. Ελπίζω στο μέλλον να μου δοθεί η ευκαιρία να συνεργαστώ ξανά μαζί του .

Από τις ευχαριστίες δεν θα μπορούσε να λείπει η οικογένεια μου, η μητέρα μου Αλεξάνδρα και τα αδέρφια μου Μαρία και Αποστόλης με την στήριξη και την υπομονή των οποίων κατάφερα να φτάσω στο σημείο που έχω φτάσει έως σήμερα . Τους ευχαριστώ πολύ για όλα αυτά που μου προσέφεραν και συνεχίζουν να μου προσφέρουν, χωρίς αυτούς σίγουρα δεν θα ήταν δυνατή η εκπόνηση της εργασίας.

Θα ήθελα να ευχαριστήσω ιδιαιτέρως τον Αντώνη Κορακή για την ανιδιοτελή βοήθεια του η οποία ήταν απαραίτητη για την εκπόνηση της εργασίας, για την στήριξη του και για τις συμβουλές του την στιγμή που αντιμετώπισα την μεγαλύτερη δυσκολία κατά την διάρκεια της εργασίας. Θα ήθελα να τον ευχαριστήσω επίσης για τις γνώσεις του τις οποίες μοιράστηκε μαζί μου, για το κουράγιο που μου έδινε τις στιγμές που αγχωνόμουν και το άγχος που μου δημιουργούσε τις στιγμές που επαναπαυόμουν.

Τέλος θέλω να ευχαριστήσω τον Νίκο Βρανά για τις αρχικές οδηγίες που μου παρείχε και την απαραίτητη καθοδήγηση.

ΠΕΡΙΛΗΨΗ

Το VoIP αναφέρεται σε πρωτόκολλα επικοινωνίας, τεχνολογίες, μεθοδολογίες και τεχνικές μετάδοσης οι οποίες εμπλέκονται στην μετάδοση επικοινωνιών φωνής και συνόδους πολυμέσων πάνω από δίκτυα που κάνουν χρήση πρωτοκόλλου Internet. Το SIP (Session Initiation Protocol) είναι ένα πρωτόκολλο σηματοδοσίας ορισμένο από την IETF για VoIP και άλλες συνόδους πολυμέσων ή κειμένου.

Το SIP πρωτόκολλο είναι το πλέον διαδεδομένο πρωτόκολλο σηματοδοσίας με αποτέλεσμα θέματα που αφορούν την ασφάλεια σχετικά με αυτό να χρήζουν προσοχής. Ένα από τα θέματα αυτά έχει να κάνει με την απόκρυψη της ταυτότητας του χρήστη κατά την διάρκεια εγγραφής του στο IMS δίκτυο. Στην παρούσα διπλωματική μελετήθηκαν δύο τρόποι διαφύλαξης του ονόματος χρήστη με χρήση δύο διαφορετικών κρυπτογραφικών αλγορίθμων AES και RSA.

ΓΛΩΣΣΑΡΙ ΟΡΩΝ

Αγγλικός Όρος	**Απόδοση**
Voice over IP	Υπηρεσία Φωνής μέσω IP Δικτύων
Internet	Διαδίκτυο
IP Multimedia Subsystem	Υποσύστημα Πολυμέσων IP
Denial of Service	Άρνηση Παροχής Υπηρεσίας
Circuit Switching	Μεταγωγή Κυκλώματος
Packet Switching	Μεταγωγή Πακέτων
Header	Κεφαλίδες
Signalling Protocols	Πρωτόκολλα Σηματοδοσίας
Request	Αίτηση
Client	Πελάτης
Server	Εξυπηρέτης/ Εξυπηρετητής/ Διακομιστής
Response	Απόκριση
Start- Line	Αρχική Γραμμή
Message Body	Κύριο Μέρος Μηνύματος

Request-Line	Γραμμή Αίτησης
Status-Line	Γραμμή Κατάστασης
Contact Address	Διευθύνσεων Επαφής
User Agents	Πράκτορες Χρήστη
Registrar	Εξυπηρέτης Εγγραφής
Proxy	Πληρεξούσιος Εξυπηρέτης
Redirect	Εξυπηρέτης Ανακατεύθυνσης
Gateway	Εξυπηρέτης Πύλη
Stateless Mode	Κατάσταση Χωρίς Μνήμη
Stateful Mode	Κατάσταση με Μνήμη
Domain	Τομέας
Unauthorized Access	Μη Εξουσιοδοτημένη Πρόσβαση
Toll Frauds Call	Απάτη Χρέωσης Κλήσης
Impersonation	Πλαστοπροσωπία
Eavesdropping	Υποκλοπή Επικοινωνίας
Confidentiality	Εμπιστευτικότητα
Integrity	Ακεραιότητα
Authenticity	Αυθεντικότητα
Man-in-the-Middle Attack	Επιθέσεις Ενδιάμεσου
Flooding Attacks	Επιθέσεις Πλημμύρας
Termination	Τερματισμό
Cancellation	Ακύρωση
Redirection	Ανακατεύθυνση
Challenge-Response	Πρόκληση-Απάντηση
Spoofing	Απόκρυψη Ταυτότητας

Περιεχόμενα

Πίνακας Εικόνων

Κεφάλαιο 1 Εισαγωγή

1.1 Εισαγωγή

Το PSTN (Public Switch Telephone Network) θεωρείται ως το μεγαλύτερο αναπτυγμένο τηλεπικοινωνιακό δίκτυο παγκοσμίως. Το PSTN χρησιμοποιεί την τεχνική μεταγωγής κυκλώματος, σύμφωνα με την οποία το επικοινωνιακό κανάλι που απαιτείται για την μετάδοση των δεδομένων μεταξύ δύο ή περισσότερων οντοτήτων , δεσμεύεται αποκλειστικά για την συγκεκριμένη επικοινωνία, χωρίς να υπάρχει η δυνατότητα διαμοιρασμού του από άλλες οντότητες, ανεξαρτήτως του ποσοστού χρήσης καθ' όλη την διάρκεια της επικοινωνίας. Συνέπεια αυτής της τεχνικής είναι η αξιοποίηση του δεσμευμένου καναλιού μόνο κατά το 10%-25% του συνολικού όγκου των δεδομένων που θα μπορούσαν να μεταδοθούν μέσω αυτού. Για την αποκατάσταση μια σύνδεσης, άρα και της δέσμευσης της γραμμής απαιτείται η αξιοποίηση των κατάλληλων συστημάτων σηματοδοσίας. Αρχικά αυτά τα συστήματα ήταν εσωζωνικά (in-band) και απαιτούσαν την αρχική δέσμευση του καναλιού και όλων των απαραίτητων πόρων για την πραγματοποίηση της επικοινωνίας. Εξαιτίας όμως της αναξιοπιστίας και των προβλημάτων ασφάλειας αυτών των συστημάτων προτάθηκε και τελικά επικράτησε η εξωζωνική (out-of band) μετάδοση των σημάτων σηματοδοσίας, δηλαδή η χρήση διαφορετικού καναλιού και όχι μέσω του καναλιού μετάδοσης φωνής. Συνεπώς δεν είναι απαραίτητη η αρχική δέσμευση του καναλιού αλλά το δίκτυο σηματοδοσίας είναι επιφορτισμένο με το εντοπισμό του καλούμενου και αν ο καλούμενος είναι διαθέσιμος τότε πραγματοποιείται η δέσμευση του καναλιού για την επίτευξη της επικοινωνίας. Το εξωζωνικό σύστημα που χρησιμοποιείται ευρέως είναι το SS7 (Signaling System 7) το οποίο είναι ένα σύνολο από προδιαγραφές και πρωτόκολλα τα οποία απαιτούνται για την σωστή λειτουργία του τηλεφωνικού συστήματος PSTN. Όμως παρά την ύπαρξη συστημάτων όπως το SS7 δεν λύθηκαν όλα τα προβλήματα. Ένα τέτοιου είδους σύστημα συμβάλλει στην σωστή λειτουργία του τηλεφωνικού συστήματος και συμβάλλει στην δυνάτητα ύπαρξης νέων υπηρεσιών αλλά εξακολουθεί να απατείται δίκτυα, πρότυπα και εξοπλισμός κλειστής

αρχιτεκτονικής. Συνεπώς απαιτείται αυξημένο κόστος για την ανάπτυξη νέων υπηρεσιών.

Λόγω αυτού του αυξημένου κόστους δημιουργήθηκε η ανάγκη για την έυρεση νέων εναλλακτικών τρόπων παροχής υπηρεσιών τηλεφωνίας. Το ενδιαφερόν για υπηρεσίες τηλεφωνίας χαμηλού κόστους απο την μία και η ραγδαία εξέλιξη του ίντερνετ από την άλλη είχαν ως αποτέλεσμα την μετάδοση φωνής μέσω ανοιχτών δικτύων δεδομένων. Το πρωτόκολλο αυτών των δίκτυων ήταν όπως και σήμερα το πρωτόκολλο IP και η μεταδόση φωνής μέσω αυτών των δικτύων είναι γνωστή εως VOIP (Voice Over IP). Η υπηρεσία VOIP όπως και το δίκτυο PSTN χρησιμοποιεί διαφορετικά πρωτόκολλα για την σηματοδοσία και την μεταφορά των δεδομένων. Στην IP τηλεφωνία δεν μπορεί να αξιοποιηθεί το σύστημα σηματοδοσίας SS7 λόγω της μη συμβατότητας των πρωτοκόλλων των κατώτερων επιπέδων παρότι έχουν προταθεί λύσεις δεν έχουν εφαρμοστεί ευρέως και με επιτυχία. Πέραν των σημάτων σηματοδοσίας όμως στο διαδίκτυο δεν υπάρχει κανάλι που να αξιοποιείται εξολοκλήρου για την φωνή. Η μετάδοση δεδομένων φωνής μεταδίδεται μέσω του δικτύου δεδομένων που όμως είμαι αναξιόπιστο για την μετάδοση δεδομένων πραγματικού χρόνου. Επίσης η αρχιτεκτονική του διαδικτύου είναι δεδομένη και συνεπώς οι αλλαγές καθίστανται ανέφικτες. Για όλους τους παραπάνω λόγους η ανάπτυξη νέων πρωτοκόλλων τόσο για την διαχείριση των κλήσεων όσο και για την μεταφορά των πολυμεσικών δεδομένων ήταν απαραίτητη. Έτσι στην IP τηλεφωνία συναντάμε τριών ειδών πρωτόκολλα. Τα πρωτόκολλα σηματοδοσίας τα οποία διαχειρίζονται τις κλήσεις δηλαδή την εγκατάσταση τροποποίηση και τερματισμό των κλήσεων μεταξύ των οντοτήτων που επικοινωνούν (SIP, H.323). Τα πρωτόκολλα πολυμέσων για την μετάδοση των πολυμεσικών δεδομένων μεταξύ των οντοτήτων που έχει ήδη εγκατασταθεί κανάλι επικοινωνίας(RTP). Τα βοηθητικά πρωτόκολλα τα οποία χρησιμοποιούνται ήδη στις υπηρεσίες διαδικτύου και ενσωματώνονται στην αρχιτεκτονική της IP τηλεφωνίας για την παροχή ολοκληρωμένων υπηρεσιών(DNS).

Η IP τηλεφωνία συνεχώς κερδίζει έδαφος και όλο και περίσσοτεροι χρήστες αλλά και πάροχοι τηλεπικοινωνιακών υπηρεσίων την εφαρμόζουν λόγω του χαμηλού

κόστους και της ανάπτυξης υπηρεσιών οι οποίες απαιτούν λιγότερα έξοδα και βασίζονται στην αξιοποίηση του διαδικτύου. Η πρόκληση για την IP τηλεφωνία είναι να καταφέρει να υποστηρίξει υπηρεσίας με υψηλές απαιτήσεις διαθεσιμότητας, αξιοπιστίας και ασφάλειας όπως έχει αποδείξει το PSTN κατά την εξέλιξη του στα χρόνια λειτουργίας του. Είναι εμφανές πως σε ένα περιβάλλον όπβς αυτό του διαδικτύου όπου οι απειλές και οι ευπάθειες μεταφέρονται κατευθείαν στις υπηρεσίες που το αξιοποιούν ως μέσο ένας τέτοιος στόχος είναι δύσκολος και η επίτευξη του πολύ σημαντική.

1.2 Περιγραφή και σημαντικότητα του Προβλήματος

Όπως προαναφέρθηκε στις VOIP υπηρεσίες αξιοποιείται το πρωτόκολλο σηματοδοσίας SIP. Το SIP είναι ένα ανοιχτό πρωτόκολλο σηματοδοσίας το οποίο αναπτύχθηκε από την Internet Engineering Task Force (IETF) προκειμένου να δημιουργηθεί ένα πρωτόκολλο το οποίο να εγκαθιστά, να διαχειρίζεται και να τερματίζει επικοινωνία πραγματικού χρόνου πάνω σε δίκτυα IP. Το SIP αποτελεί ένα peer-to-peer πρωτόκολλο επικοινωνίας , επιπέδου εφαρμογής. Ένας από τους σκοπούς της δημιουργίας του συγκεκριμένου πρωτοκόλλου ήταν η ικανότητα να υποστηρίζει όλους τους τύπους της επικοινωνίας ανεξαρτήτως του μέσου. Συνεπώς διαφορετικά είδη επικοινωνίας όπως φωνή, κείμενο, ή βίντεο είναι δυνατόν να πραγματοποιηθούν με χρήση οποιασδήποτε συσκευής συμβατή με SIP όπως ένα μικρόφωνο σε ένα laptop υπολογιστή, ένα PDA, κινητό τηλέφωνο, ή ένα IP τηλέφωνο με δυνατότητες βιντεοδιάσκεψης. Επιπλέον το SIP έχει αρκετά κοινά χαρακτηριστικά με δύο πρωτόκολλα που είχαν ήδη εφαρμοστεί επιτυχώς στο διαδίκτυο το HTTP και το SMTP , είναι πρωτόκολλο κειμένου (τα μηνύματα κωδικοποιούνται σε μορφή κειμένου) όπως το πρώτο και η σύνταξη και η δομή του έχει ομοιότητες και με τα δύο.

Για την σηματοδοσία λοιπόν το πρωτόκολλο SIP στέλνει μηνύματα σε διαφορετικούς servers ανάλογα με το είδος του μηνύματος. Το πρώτο μήνυμα που αποστέλλει το SIP είναι το μήνυμα εγγραφής του χρήστη σε κάποιον server. Η

διαδικασία εγγραφής δεν έχει μόνο ως αποτέλεσμα την καταγραφή μιας νέας IP διεύθυνσης στο δίκτυο, αποτελεί και μια ευκαιρία για την αυθεντικοποίηση των χρηστών που έχουν πρόσβαση σε αυτό. Κάθε χρήστης έχει την φυσική διεύθυνση και την δημόσια, η δημόσια είναι για παράδειγμα όπως η διεύθυνση του ηλεκτρονικού ταχυδρομείου βάσει με την οποία μπορούν άλλοι χρήστες να επικοινωνήσουν μαζί μας. Αυτή την αντιστοιχία ανάμεσα στη δημόσια διεύθυνση URI και στην φυσική IP διεύθυνση αναλαμβάνει στο πρωτόκολλο SIP μια οντότητα η οποία ονομάζεται Registar. Όπως θα δούμε αναλυτικά και στο παρακάτω κεφάλαιο σε αυτή την οντότητα απευθύνονται και οι πληρεξούσιοι servers προκειμένου να βρουν ποιά είναι η φυσική διεύθυνση στην οποία θα δρομολογήσουν τις κλήσεις. Αυτό το χαρακτηριστικό ανέδειξε το Skype σε τόσο δημοφιλή VOIP εφαρμογή αφού αρκούσε να το εγκαταστήσει κάποιος στο laptop του και να έχει την δυνατότητα να καλεί αλλά και να προωθούνται οι κλήσεις σε αυτόν οπουδήποτε και αν βρίσκεται. Παρέχεται λοιπόν η δυνατότητα επικοινωνίας όπου και αν βρίσκεται ο χρήστης χωρίς οι καλούντες να πρέπει να γνωρίζουν την φυσική του διεύθυνση και χωρίς επιπλέον χρέωση λόγω της απόστασης.

Το SIP πρέπει να αντιμετωπίσει απειλές που έχουν σχέση με το ίδιο το περιβάλλον VOIP εξ' αιτίας της εύκολης πρόσβασης στο κανάλι επικοινωνίας αλλά και αυτές που σχετίζονται με το γεγονός πως πρόκειται για ένα πρωτόκολλο απλού κειμένου (text based). Συγκεκριμένα κατά την διαδικασία εγγραφής η οποία ξεκινά όταν ο συνδρομητής αποκτήσει πρόσβαση στο IP δίκτυο και του δοθεί μια διεύθυνση IP, το μήνυμα εγγραφής που στέλνεται είναι σε μορφή κείμενου (text based) χωρίς απόκρυψη των στοιχείων του χρήστη όπως user name και URI. Το γεγονός της μη απόκρυψης των συγκεκριμένων πληροφοριών αποτελεί αδυναμία του πρωτοκόλλου καθώς είναι δυνατή η εκμετάλλευση της από επιθέσεις όπως “eavesdropping” της οποίας την επίτευξη βοηθά και η ύπαρξη αυτοματοποιημένων εργαλείων που κυκλοφορούν στο διαδίκτυο και αναλύουν VOIP κίνηση. Επιπλέον η μορφή των μηνυμάτων θεωρείται πως δίνει ευκαιρίες για επιθέσεις όπως spoofing, hijacking και αλλοίωση μηνυμάτων. Η χρήση κακόβουλων SIP μηνυμάτων μπορεί να οδηγήσει σε επίθεση άρνησης υπηρεσιών ή σε μη εξουσιοδοτημένη πρόσβαση στην υπηρεσία.

Η εύκολη πρόσβαση στα IP δίκτυα, η ύπαρξη αυτοματοποιήμενων εργαλείων ανάλυσης κίνησης και επιθέσεων αλλά και η φύση του ίδιου του πρωτοκόλλου, εγείρει την ανάγκη για την υλοποίηση μεθόδων προς την κατεύθυνση της ασφάλειας. Τα δεδομένα σηματοδοσίας μεταδίδονται σε καθαρό κείμενο (plain text) συνεπώς κάποιος επιτιθέμενος μπορεί να γνωρίζει τις οντότητες που επικοινωνούν μεταξύ τους αλλά και τις παραμέτρους της μιας συνόδου. Οι παράμετροι αυτοί είναι πιθανό να χρησιμοποιηθούν σε άλλου είδους επιθέσεις, επίσης η τροποποίηση τους η οποία βλάπτει την ακεραιότητα του μηνύματος είναι δυνατόν να οδηγήσει σε αδυναμία αποκατάστασης συνόδου μεταξύ των οντοτήτων ή δρομολόγηση σε μη εξουσιοδοτημένες οντότητες. Επιπλέον όπως προαναφέρθηκε η δημιουργία απρόσμενης κίνησης μπορεί να οδηγήσει σε εξάντληση των υπολογιστικών πόρων άρα αδυναμία εξυπηρέτησης των νόμιμων χρηστών. Τέτοιου είδους προβλήματα είναι μη ανεκτά από τους χρήστες δεδομένης της μόνιμα διαθέσιμης τηλεφωνίας PSTN, ειδικά όταν αυτά τα προβλήματα συσχετίζονται και με άλλες υπηρεσίες όπως αυτή των χρεώσεων.

1.3 Στόχος της Διπλωματικής Εργασίας

Στόχος της διπλωματικής εργασίας είναι η εύρεση του καταλληλότερου αλγόριθμου και η εφαρμογή του με σκοπό την απόκρυψη των στοιχείων του χρήστη κατά την εγγραφή του στους εξυπηρετητές εγγραφής ενός IMS δικτύου. Συγκεκριμένα και για να επιτευχθεί αυτός ο στόχος, αρχικά πρέπει να αποτιμηθούν οι κίνδυνοι που αφορούν σε αυτή την ευπάθεια και να συγκριθούν οι αλγόριθμοι που είναι πιθανό να εφαρμοστούν ώστε αυτός που θα επιλεχθεί να δημιουργεί τις μικρότερες καθυστερήσεις και να εφαρμόζεται χωρίς να είναι αναγκαία η αλλαγή σε κανένα σημείο του πρωτοκόλλου SIP. Μέσα από την εφαρμογή των μεθόδων για την επίτευξη του σκοπού θα μπορεί να γίνει και η αξιολόγηση ανάλογα με τις συνέπειες και τα προβλήματα που προκύπτουν σε κάθε περίπτωση.

1.4 Μεθοδολογία

Η μεθοδολογία που ακολουθήθηκε με σκοπό να επιτευχθεί ο στόχος της διπλωματικής εργασίας αποτελείται από τα παρακάτω βήματα. Αρχικά έγινε μελέτη του πρωτοκόλλου σηματοδοσίας SIP, στην συνέχεια μελετήθηκαν τα προβλήματα ασφαλείας, οι ευπάθειες και οι υπάρχοντες μηχανισμοί ασφαλείας. Σε αυτό το στάδιο δόθηκε ιδιαίτερη σημασία στα προβλήματα ιδιωτικότητας που σχετίζονται με το πρωτόκολλο. Στο τελευταίο στάδιο της διπλωματικής σχεδιάστηκαν και υλοποιήθηκαν δύο προτεινόμενες λύσεις ώστε να μην είναι εφικτή πιθανή παραβίαση της ιδιωτικότητας.

1.5 Δομή Διπλωματικής Εργασίας

Στο κεφάλαιο που ακολουθεί περιγράφεται η Αρχιτεκτονική του δικτύου, του SIP πρωτοκόλλου και των SIP μηνυμάτων. Το τρίτο κεφάλαιο αναφέρεται αποκλειστικά στα προβλήματα ασφαλείας που αντιμετωπίζει το συγκεκριμένο πρωτόκολλο και στους ήδη υπάρχοντες μηχανισμούς ασφάλειας, παραθέτοντας στο τέλος μια σύγκριση αυτών των μηχανισμών. Το τέταρτο και τελευταίο κεφάλαιο σχετίζεται με την υλοποίηση, περιγράφονται οι αλγόριθμοι που έχουν επιλεχθεί για την υλοποίηση, η μεθοδολογία και τα εργαλεία που ακολουθήθηκαν, καθώς τα προβλήματα που αντιμετωπίστηκαν κατά την διάρκεια εφαρμογής τους.

Κεφάλαιο 2 Αρχιτεκτονική Δικτύου και Πρωτοκόλλου

2.1 Εισαγωγή

Το SIP έχει επικρατήσει μεταξύ των πρωτοκόλλων διαχείρισης σηματοδοσίας διότι εξειδικεύεται στην αρχιτεκτονική του διαδικτύου και έχει ενσωματωθεί ως πρωτόκολλο σηματοδοσίας στην αρχιτεκτονική 3ης γενιάς κινητών επικοινωνιών στο υποσύστημα πολυμέσων IP (Multimedia Subsystem IP-IMS) .

Οι πρώτοι που εφάρμοσαν το Voice Over IP είχαν να αντιμετωπίσουν πολλές προκλήσεις σε ένα περιβάλλον το οποίο είχε αρχικά δημιουργηθεί για μεταφορά δεδομένων. Σε ένα περιβάλλον για μεταφορά δεδομένων δεν αποτελεί προτεραιότητα η παράδοση σε πραγματικό χρόνο εάν σε μια επικοινωνία με ανταλλαγή άμεσων μηνυμάτων η απάντηση δεν ληφθεί για κάποια λεπτά δεν θα τελειώσει η συζήτηση, διότι μια τέτοια καθυστέρηση θεωρείται αναμενόμενη. Σε αντίθεση με την επικοινωνία φωνής η οποία από την φύση της είναι εφαρμογή πραγματικού χρόνου. Καθυστερήσεις στην παράδοση των πακέτων φωνής δεν είναι ανεκτά και για αυτό το λόγο η IETF (Internet Engineering Task Force) ξεκίνησε τον σχεδιασμό ενός πρωτοκόλλου ειδικά για τον έλεγχο πραγματικού χρόνου επικοινωνίας πολυμέσων. Σκοπός ήταν η δημιουργία ενός πρωτοκόλλου ελέγχου συνόδων ικανό να υποστηρίζει όλους τους τύπους επικοινωνίας ανεξαρτήτως του τύπου.

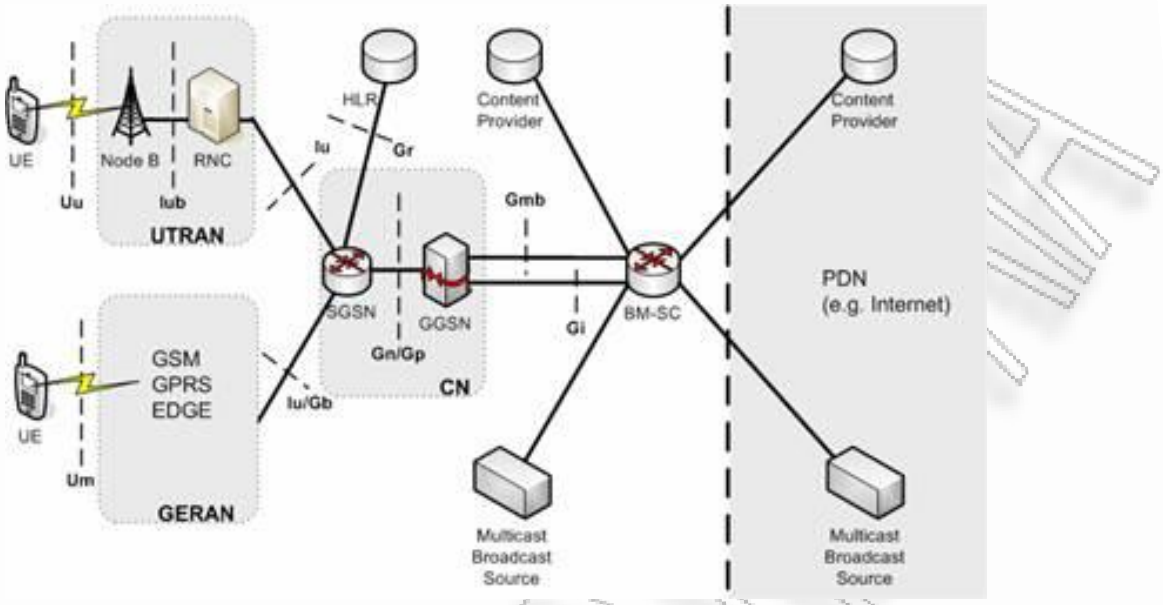
Στο παρόν κεφάλαιο περιγράφεται η αρχιτεκτονική του UMTS και του IMS δικτύου για την δημιουργία πλήρης εικόνας της λειτουργία του SIP πρωτοκόλλου. Στην συνέχεια του κεφαλαίου αναλύεται η αρχιτεκτονική του πρωτοκόλλου και δίνεται ιδιαίτερη έμφαση στα είδη των μηνυμάτων που αποτελούν στην ουσία το πρωτόκολλο. Είναι σημαντικό να κατανοηθεί πως όταν στην ανάλυση της αρχιτεκτονικής του SIP αναφερόμαστε σε οντότητες δεν εννοούμε φυσικές οντότητες. Οι SIP οντότητες είναι λογικές, στην πραγματικότητα μια φυσική οντότητα όπως ένας διακομιστής μπορεί να υποστηρίζει αρκετές λογικές οντότητες. (Russell)

2.1 Αρχιτεκτονική UMTS

Το UMTS (Universal Mobile Telecommunications System) αποτελεί το σύστημα που προτυποποιήθηκε από την 3GPP (3rd Generation Partnership Project), παρακάτω παρουσιάζονται τα βασικά στοιχεία της αρχιτεκτονικής του. Αποτελείται από τρία κύρια μέρη :

- Εξοπλισμός χρήστη (User Equipment,UE), είναι το τερματικό του χρήστη το οποίο διαθέτει ασύρματη πρόσβαση στο ράδιο-δίκτυο (Radio Access Network, RAN) του παρόχου υπηρεσιών.
- Το δίκτυο κορμού (Core Network) του παρόχου το οποίο αποτελείται από δύο υποσυστήματα. Το υποσύστημα μεταγωγής κυκλώματος (circuit switched, CS) και το υποσύστημα μεταγωγής πακέτων (packet switched)
- Οι διεπαφές (interfaces) μεταξύ των οντοτήτων.

Πριν συνεχίσουμε με την ανάλυση των οντοτήτων και της αρχιτεκτονικής πρέπει να σημειωθούν ορισμένα νέα στοιχεία που αφορούν στο UMTS σε σχέση με το προγενέστερο GSM. Το τερματικό του χρήστη αποτελείται από τον φορητό εξοπλισμό (Mobile Equipment, ME) και από την UICC (Universal Integrated Circuit Chip) αντί της κάρτας SIM που υπήρχε στο GSM. Στο δίκτυο κορμού το CS αποτελεί εξέλιξη του CS GSM δικτύου με το MSC (Mobile Switching Centre) να είναι το βασικότερο στοιχείο του , όμως από την έκδοση UMTS 5 και μετά το CS υποσύστημα έχει καταργηθεί. Το PS αποτελεί εξέλιξη του GSM GPRS και τα βασικότερα στοιχεία του είναι το SGSN και το GPRS Support Node (GGSN). Το νέο δίκτυο πρόσβασης του UMTS καλείται UMTS Terrstrial Radio Access Network (UTRAN) και βασίζεται στην τεχνολογία W-CDMA.



Εικόνα 1 Αρχιτεκτονική UMTS

Αναλυτικότερα το δίκτυο UTRAN αποτελείται από τον ελεγκτή ασύρματης πρόσβασης (Radio Network Controller, RNC) και το Node B το οποίο αποτελεί την βάση που παρέχει κάλυψη στην αντίστοιχη κυψέλη. Περισσότερες από μια κεραίες (Node Bs) μπορεί να ελέγχονται από ένα RNC. Το Node B συνδέεται με τον εξοπλισμό του χρήστη μέσω της διεπαφής Uu και με το RNC μέσω της διεπαφής Iub.

Οι οντότητες που αποτελούν το δίκτυο πυρήνα του UMTS είναι οι MSC, G-MSC, HLR, VLR οι οποίες προϋπήρχαν στο δίκτυο GSM. Οι κόμβοι αυτοί αποτελούν δίκτυο μεταγωγής κυκλώματος που αποτελεί υποσύνολο του δικτύου πυρήνα. Οι κόμβοι που προστέθηκαν όπως αναφέρθηκε και παραπάνω είναι οι SGSN και GGSN. Το στοιχείο MSC (Mobile Services Switching Center) επικοινωνεί ή περιέχει μια βάση δεδομένων των χρηστών που κινούνται στην περιοχή που ελέγχεται από το συγκεκριμένο MSC. Η βάση δεδομένων ονομάζεται VLR (Visitor Location Register). Το στοιχείο G-MSC (Gateway-MSC) αποτελεί πύλη εξόδου προς το PSTN δίκτυο. Στο PS υποσύστημα, το ρόλο των MSC/VLR παίζει το SGSN και αντίστοιχα η πύλη εξόδου προς τις IP υπηρεσίες παρέχεται από το GGSN. Το SGSN συνδέεται με το GGSN μέσω της διεπαφής Gn και με το UTRAN μέσω της διεπαφής Iu. (Γ. Καμπουράκης) (Π.Αντωνίου, 2005)

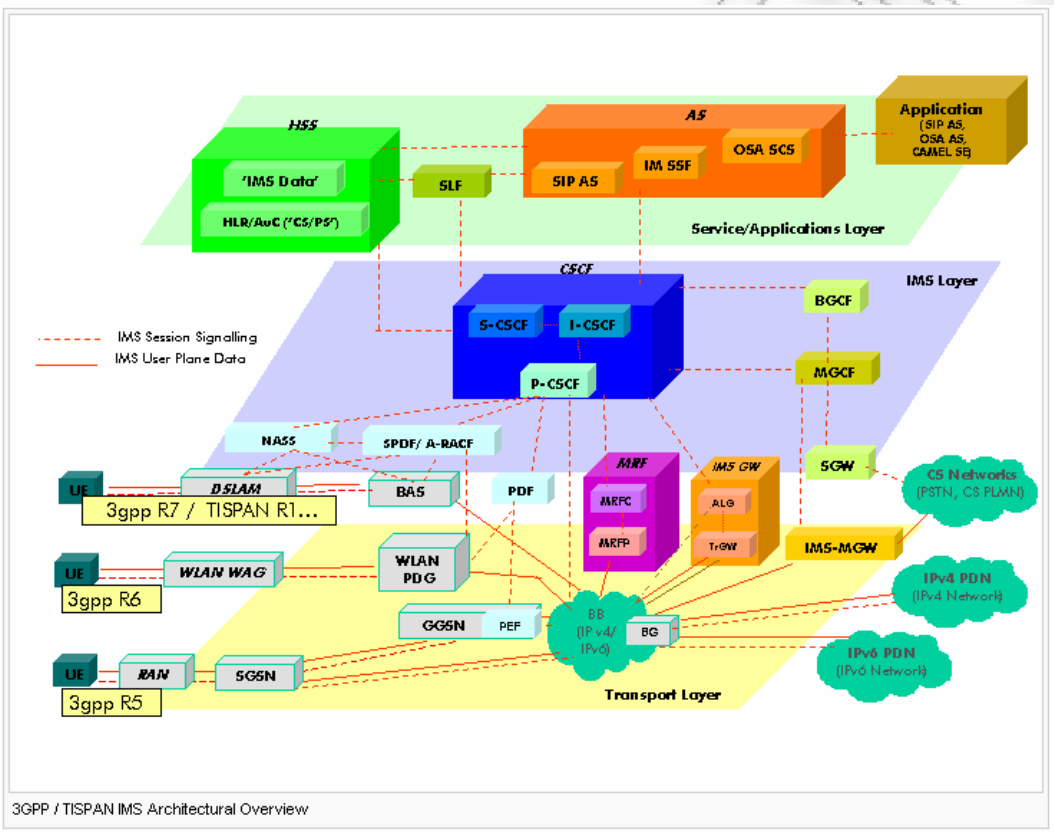
2.2 Αρχιτεκτονική IMS Δικτύου

Το IMS (IP Multimedia Subsystem) αποτέλεσε μια αλλαγή στο υπάρχον δίκτυο με σκοπό την ικανοποίηση των νέων αναγκών της αγοράς. Εισάγει μια αρχιτεκτονική η οποία εξυπηρετεί υπηρεσίες οι οποίες βασίζονται στο IP. Σχεδιάστηκε από την 3GPP με στόχο την εξέλιξη των δικτύων κινητής τηλεφωνίας πέρα από το GSM. Για να διευκολύνει την ενσωμάτωση με το ίντερνετ, το IMS χρησιμοποιεί IETF πρωτόκολλα όπου είναι δυνατόν π.χ SIP. Σύμφωνα με την 3GPP το IMS δεν προορίζεται για την προτυποποίηση εφαρμογών αλλά για να διευκολύνει στην πρόσβαση των πολυμέσων και των εφαρμογών φωνής από ασύρματα και ενσύρματα τερματικά. Για να επιτύχει όλα τα παράπανω το IMS εφαρμόζει οριζόντια επίπεδο ελέγχου το οποίο απομονώνει την πρόσβαση στο διαδίκτυο από το επίπεδο υπηρεσιών. Με αυτόν τον τρόπο αρχιτεκτονικά οι υπηρεσίες δεν χρειάζεται να έχουν τις δικές τους συναρτήσεις ελέγχου, αφού ως επίπεδο ελέγχου υπάρχει ένα κοινό οριζόντιο επίπεδο. (Wikipedia)

Πυρήνα του IMS (IP Multimedia Subsystem) δικτύου αποτελούν το CSCF (Call Session Control Function) και το HSS (Home Subscriber Server) στοιχείο. Το CSCF είναι υπεύθυνο για την επεξεργασία της σηματοδοσίας μέσω του SIP πρωτοκόλλου. Η κύρια λειτουργία του CSCF είναι να παρέχει έλεγχο των συνόδων για τα τερματικά και τις εφαρμογές χρησιμοποιώντας το IMS δίκτυο. Ο έλεγχος των συνόδων περιέχει την ασφαλή δρομολόγηση των SIP μηνυμάτων, έλεγχο των SIP συνόδων και επικοινωνία με την πολιτική για την υποστήριξη των εξουσιοδοτήσεων. Επίσης το CSCF έχει την ευθύνη για την αλληλεπίδραση με το HSS. Κάθε CSCF στοιχείο ανήκει σε μια από τιε τρεις παρακάτω κατηγορίες, τον Proxy-CSCF (P-CSCF), τον Serving-CSCF (S-CSCF) και τον Interrogating-CSCF (I-CSCF), καθένα από τα οποία έχει διαφορετική λειτουργία μέσα στο IMS δίκτυο. (mobilein.com)

Το HSS αποτελεί την κύρια βάση δεδομένων η οποία περιέχει πληροφορίες για τους συνδρομητές ώστε οι οντότητες του δικτύου να είναι σε θέση επικοινωνώντας με το HSS να διαχειριστούν τις κλήσεις και τις συνόδους. Παρέχει λειτουργίες που στηρίζουν τις υπηρεσίες αναγνώρισης των χρηστών, εξουσιοδότησης και αυθεντικοποίησης. Όταν ένας χρήστης εγγράφεται στο IMS domain, το προφίλ του

χρήστη (δηλαδή σχετικές πληροφορίες με τις υπηρεσίες που παρέχονται στον χρήστη) στέλνονται από το στοιχείο HSS στο CSCF. Για την εγκαθίδρυση μιας συνόδου το HSS παρέχει πληροφορίες σε όποιο CSCF εκείνη την χρονική στιγμή εξυπηρετεί τον χρήστη. Όταν περισσότερα από ένα HSS υπάρχουν στο δίκτυο, η οντότητα SLF (Subscriber Location Function) αναλαμβάνει να εντοπίσει το HSS που διατηρεί τα δεδομένα συνδρομής για τον εκάστοτε χρήστη.



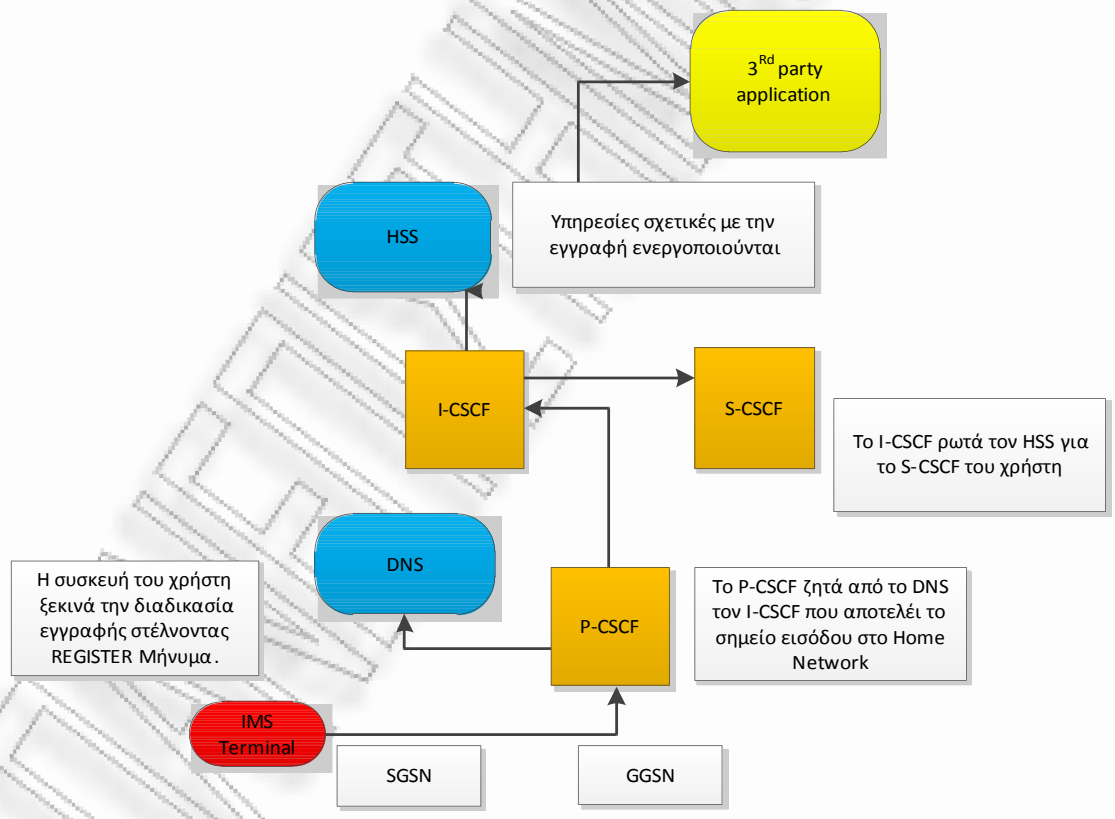
3GPP / TISPAN IMS Architectural Overview

Εικόνα 2 Αρχιτεκτονική IMS

2.3Διαδικασία εγγραφής χρήστη στο IMS δίκτυο

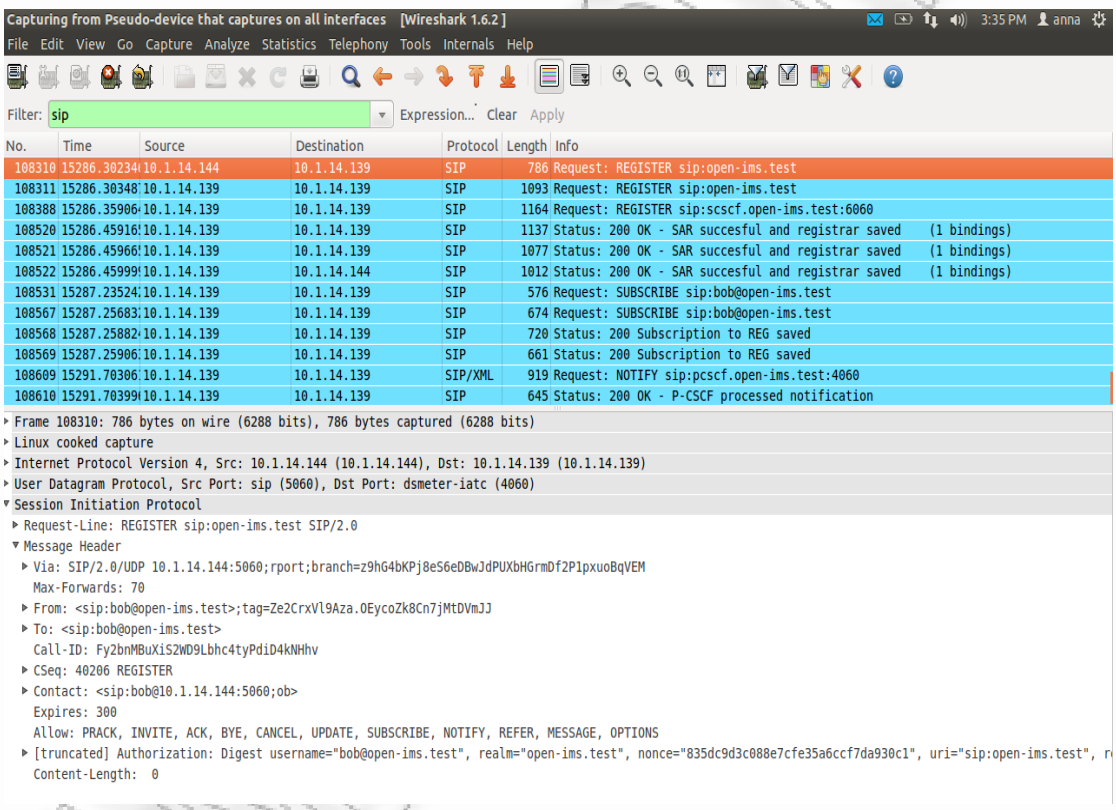
Μετά την αναφορά όλων των παραπάνω μπορούμε να μελετήσουμε την διαδικασία εγγραφής κάποιου χρήστη αναλυτικά. Το τερματικό του χρήστη ξεκινάει την διαδικασία εγγραφής στέλνοντας ένα μήνυμα εγγραφής (REGISTER message), ο (P-CSCF) είναι ένας SIP proxy και αποτελεί το πρώτο σημείο διαχείρισης του μηνύματος. Ο P-CSCF είναι ο πληρεξούσιος για όλα τα SIP μηνύματα ανάμεσα στο

τερματικό του χρήστη και στο υπόλοιπο IMS δίκτυο. Ο P-CSCF ζητά από το DNS την τοποθεσία του SIP εξυπηρετητή (I-CSCF) προκειμένου να στείλει το SIP μήνυμα. Όταν το I-CSCF λάβει το μήνυμα ζητά από το HSS να του καθορίσει ποίο S-CSCF εξυπηρετεί τον συγκεκριμένο χρήστη, λαμβάνοντας αυτή την πληροφορία προωθεί το μήνυμα στο κατάλληλο S-CSCF. Το τελευταίο στοιχείο είναι υπεύθυνο για την διασύνδεση με τους εξυπηρετητές εφαρμογών (Application Servers). Ζητά από το HSS να εγγράψει πως το συγκεκριμένο τερματικό εξυπηρετήθηκε από το συγκεκριμένο S-CSCF, κάτι το οποίο είναι πολύ χρήσιμο διότι στην εγκατάσταση της συνόδου απαιτείται να είναι γνωστό ποιό S-CSCF είναι υπεύθυνο για τον έλεγχο της συνόδου αυτού του τερματικού. Μέρος της διαδικασίας εγγραφής αποτελεί η χρήση διαπιστευτηρίων τα οποία το S-CSCF βρίσκει από το HSS με σκοπό να εκδώσει ένα μήνυμα πρόκληση (challenge) το οποίο και θα στείλει στο P-CSCF το οποίο ξεκίνησε την διαδικασία εγγραφής ώστε να αυθεντικοποιηθεί το τερματικό.



Εικόνα 3 Διαδικασία Εγγραφής

Με την χρήση του εργαλείου Wireshark αποτυπώνονται στην παρακάτω εικόνα τα πακέτα που ανταλλάσσονται μεταξύ του χρήστη και του IMS δικτύου προκείμενου να γίνει η εγγραφή, περισσότερες λεπτομέρειες για την εγγραφή αναπτύσσονται στο παρακάτω κεφάλαιο. Το Wireshark είναι ελεύθερο και ανοιχτού κώδικα λογισμικό ανάλυσης πρωτοκόλλων δικτύου. Χρησιμοποιείται για την ανάλυση και παρακολούθηση δικτύου, εντοπισμό και αντιμετώπιση προβλημάτων . Στην παρακάτω εικόνα φαίνονται τα πακέτα που ανταλλάχθηκαν μεταξύ του Client και του IMS δικτύου. Σε επόμενο κεφάλαιο θα γίνει εκτενής αναφορά στην ανταλλαγή μηνυμάτων, στην προκειμένη περίπτωση όμως κατανοούμε το μήνυμα Register που στέλνει ο client και το 200 Οκ που απαντά ο P-CSCF. (Wireshark)



Εικόνα 4 Πακέτα Εγγραφής

2.4 Η Αρχιτεκτονική του SIP

2.4.1 Οντότητες Δικτύου σε ένα Voice over IP Network

Σε αυτό το υποκεφάλαιο καταγράφονται κάποιες από τις οντότητες ενός δικτύου Voice over IP.

Media Gateway (MG)

Η Media Gateway οντότητα ελέγχεται από το MGCF με χρήση του H.248 πρωτοκόλλου, παρέχει συνεργασία της ροής των μέσων ανάμεσα σε διαφορετικά δίκτυα. Επίσης είναι η υπεύθυνη οντότητα για την επίτευχση συμβατότητας ανάμεσα σε διαφορετικές μορφές μεταφοράς, RTP/UDP/IP και TDM όπως επίσης και για την επανακωδικοποίηση φωνής και βίντεο όπου αυτό κρίνεται απαραίτητο.

Media Gateway Control Function (MGCF)

Ο MGCF είναι ο κεντρικός κόμβος του PSTN δικτύου. Σχεδιάστηκε για να ενσωματώσει το PSTN και τις παραδοσιακές υπηρεσίας τηλεφωφνίας. Το MGCF είναι υπεύθυνο για τον έλεγχο των πόρων των μέσων που χρησιμοποιούνται όταν η κίνηση πρέπει να διέρχεται ανάμεσα σε δίκτυα που χρησιμοποιούν διαφορερικά μέσα, ως επί των πλείστον ανάμεσα σε δίκτυα πολυπλεξίας διαίρεσης χρόνου (TDM time division multiplex) και δίκτυα βασισμένα σε IP. Αλληλεπιδρά με τις λειτουργίες ελέγχου κλήσεων και συνόδου χρησιμοποιώντας SIP, με το Media Gateway χρησιμοποιώντας το H.248 πρωτόκολλο και με το επίπεδο ελέγχου του GSTN χρησιμοποιώντας ISUP.

H.248 media control protocols

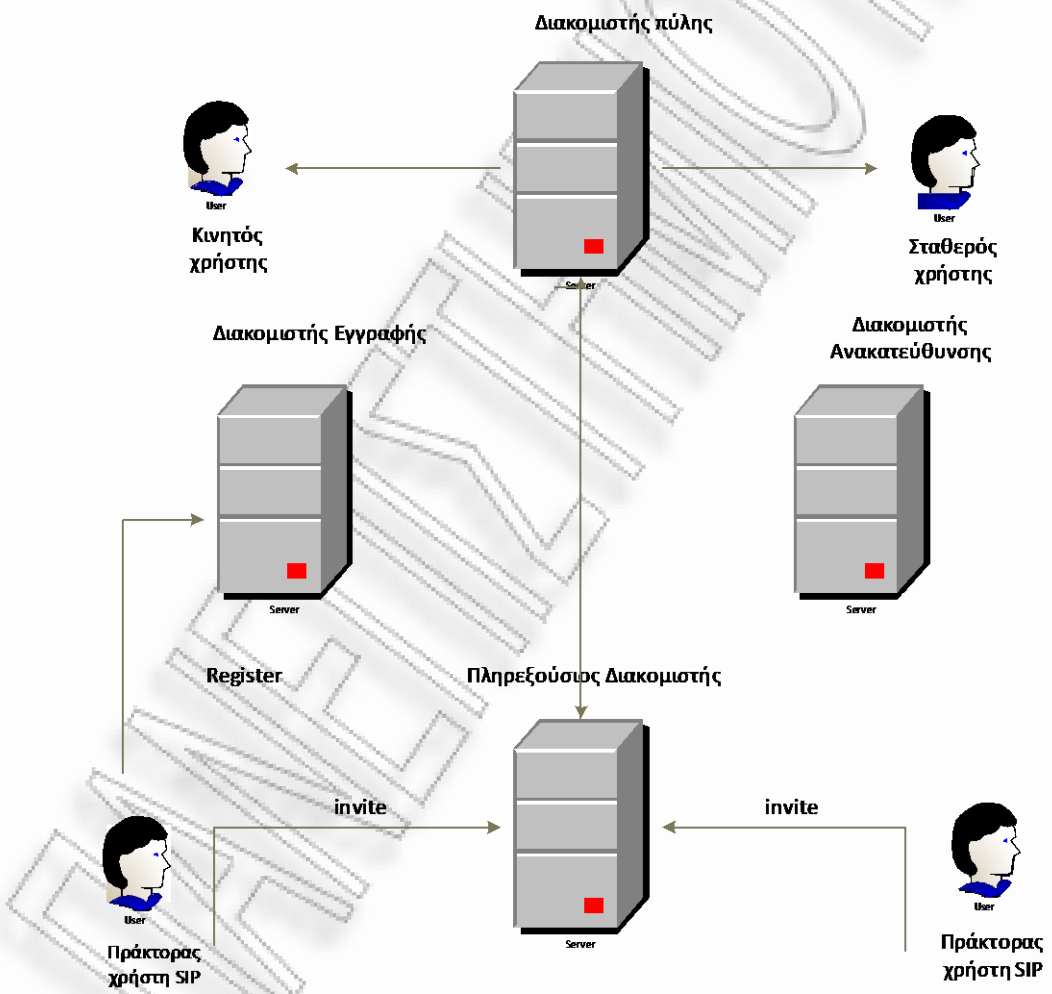
Το H.248 είναι ένα πρωτόκολλο ελέγχου το οποίο χρησιμοποιείται ανάμεσα στις συναρτήσεις ελέγχου των μέσων και στους πόρους των μέσων. Παραδείγματα κόμβων με συναρτήσεις ελέγχου μέσων είναι οι MGCF και MRFC (Media Resource Function Controller). Τυπικοί πόροι μέσων είναι οι MG και MRFP (Media Resource Function Processor).

Signaling Gateway (SG)

Η SG οντότητα είναι διεπαφή ανάμεσα στο SS7 δίκτυο και στο SIP. Μπορεί βέβαια να αποτελέσει διεπαφή και για άλλα μη SIP VoIP δίκτυα όπως H.323. (Ericsson, 2012)

2.4.2 Αρχιτεκτονική SIP

Οι οντότητες που απαρτίζουν ένα δίκτυο SIP είναι οι πράκτορες χρήστη (User Agent) και εξυπηρετητές (Servers).



Εικόνα 5 Αρχιτεκτονική SIP

Application server

Ο εξυπηρετητής εφαρμογής (Application server, **AS**) είναι μια SIP οντότητα η οποία παρέχει υπηρεσίες στο διαδίκτυο καθώς επίσης και στους συνδρομητές. Έχει την ικανότητα να δημιουργεί αιτήσεις και να ξεκινά διαλόγους ενεργώντας ως πράκτορας χρήστη έχοντας την ιδιότητα του πελάτη (client) και του εξυπηρετητή (server).

Πράκτορες χρήστη (User Agents)

Ο πράκτορας χρήστη είναι λογισμικό ενσωματωμένο στην συσκευή του χρήστη και έχει την ιδιότητα να δημιουργεί τις αιτήσεις (User Client) και να στέλνει τις κατάλληλες αποκρίσεις σε εισερχόμενα αιτήματα που δέχεται (User Server). Συνεπώς δύο ειδών πράκτορες χρήστη υπάρχουν στο τερματικό του χρήστη οι οποίες παρέχουν διαφορετικές λειτουργίες. Σε κάθε διάλογο που δημιουργείται ένας UA αντενεργεί με κάποιον άλλον.

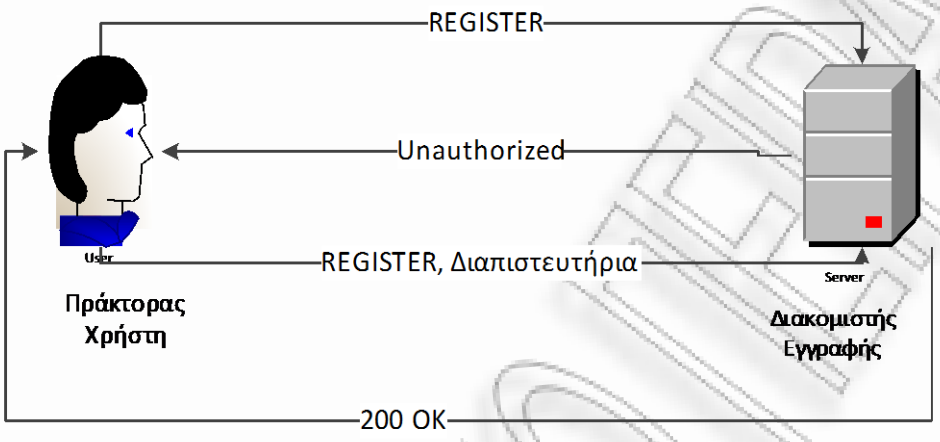
Εξυπηρετητές (Servers)

Οι εξυπηρετητές στην αρχιτεκτονική του SIP είναι ενδιάμεσες οντότητες που παρέχουν επιπρόσθετες υπηρεσίες για την παροχή ολοκληρωμένων λύσων και υπηρεσιών τηλεφωνίας στο διαδίκτυο. Παρακάτω περιγράφονται οι εξυπηρετητές που αξιοποιούνται από την αρχιτεκτονική SIP και οι λειτουργίες τους.

Εξυπηρετητής Εγγραφής (Registrar)

Ο εξυπηρετητής εγγραφής είναι υπεύθυνος για την διαχείριση και επεξεργασία των αιτήσεων εγγραφών. Οι αιτήσεις εγγραφής περιέχουν όλες εκείνες τις πληροφορίες που απαιτούνται για τον εντοπισμό και την προώθηση των αιτημάτων και των αποκρίσεων που απευθύνονται σε έναν συγκεκριμένο χρήστη. Κάθε φορά που μία συσκευή ανοίγει ή αλλάζει τοποθεσία στέλνει ένα μήνυμα εγγραφής (Register message) στο SIP δίκτυο για να του παρέχει την καινούργια του διεύθυνση. Οι διευθύνσεις των χρηστών αποθηκεύονται σε κάποια βάση δεδομένων για χρονικό διάστημα που προκαθορίζεται από τον χρήστη. Σε περίπτωση που ο χρήστης

αλλάξει θέση εντοπισμού ή μετά την λήξη του συγκεκριμένου χρονικού διαστήματος, ο εξυπηρετητής εγγραφής πρέπει να ενημερωθεί με την αποστολή νέου μηνύματος εγγραφής.



Εικόνα 6 Εγγραφή

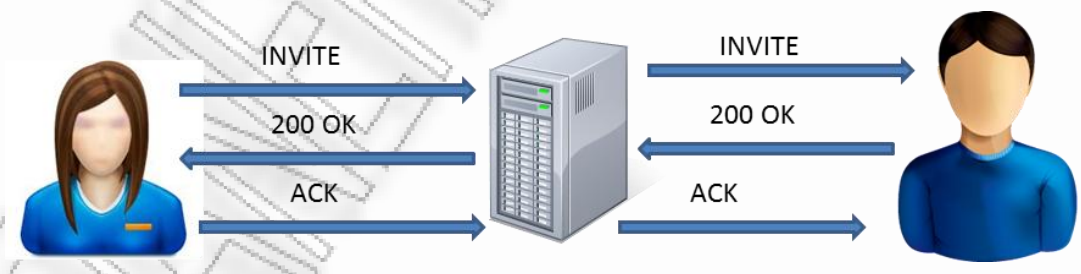
Παρακάτω απεικονίζεται μια αίτηση εγγραφής από τον χρήστη με διεύθυνση annampak@unipi.gr . Ο συγκεκριμένος χρήστης προσδιορίζει την διεύθυνση εντοπισμού του στην κεφαλίδα Contact, με χρονική ισχύ 300 δευτερολέπτων. Με το πέρας του χρονικού αυτού ορίου πρέπει να ενημερώσει τον εξυπηρετητή εγγραφής για την νέα θέση εντοπισμού του. Οι τιμές των πεδίων “From” και “To” περιέχουν διαφορετικές τιμές όταν ένας εξουσιοδοτημένος χρήστης λειτουργεί για λογαριασμό κάποιου άλλου.

REGISTER sip:unipi.gr SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: <sip:annampak@unipi.gr; >;tag=31889090987
To: <sip:annampak@unipi.com;user=phone>
Call-ID: 301829976366@81.0.7.124
Cseq:2 REGISTER
Contact: <annampak@81.0.7.124:5070;user=phone;transport=udp>;expires=300
User-Agent: Cisco ATA 186 v3.1.0 atasip (040211A)
Authorization: Digest username= “annampak”,realm:”unipi.gr”,nonce=’5472368hudey82q878337683727837”,uri”:sip: ”unipi.com”,response:=”87434656abc89ba0108768236544fd99”
Contect-Length:0

Στην κεφαλίδα “Contact” προσδιορίζεται η νέα θέση εντοπισμού του χρήστη και η χρονική ισχύς δηλώνεται στην κεφαλίδα “expires”. Μετά το πέρας του συγκεκριμένου χρονικού διαστήματος θα πρέπει να σταλθεί εκ νέου μια αίτηση εγγραφής. Αυτή η αίτηση θα ληφθεί από τον κατάλληλο Registrar εξυπηρετητή και εφόσον την αποδεχτεί θα αποκριθεί με ένα μήνυμα “200 OK”.

Πληρεξούσιος Εξυπηρετητής (Proxy Server)

Ο Πληρεξούσιος Εξυπηρετητής είναι υπεύθυνος για την δρομολόγηση των αιτήσεων και των αντίστοιχων αποκρίσεων από τους UASs και UACs. Για παράδειγμα όταν κάποιος χρήστης επιθυμεί να επικοινωνήσει με κάποιον άλλο χρήστη, το μήνυμα της αίτησης κλήσης (SIP INVITE) στέλνεται στον κατάλληλο πληρεξούσιο εξυπηρετητή ο οποίος επικοινωνεί με τον Εξυπηρετητή εγγραφής για να ενημερωθεί για την τοποθεσία του χρήστη που καλείται. Στην συνέχεια στέλνει την αίτηση στο UAS του χρήστη ή προωθεί το μήνυμα στον επόμενο πληρεξούσιο. Στην περίπτωση που ο χρήστης που καλείται δεν ανταποκριθεί ή δεν βρεθεί μετά από έναν αριθμό προσπαθειών ο πληρεξούσιος εξυπηρετητής ενημερώνει τον καλούνται για την εξέλιξη της κλήσης. Σε αυτό το σημείο εντοπίζεται και η βασική διαφορά του πληρεξούσιου από έναν απλό δρομολογητή (router) του διαδικτύου. Ο δρομολογητής απλά προωθεί τα πακέτα στον επόμενο κόμβο του μονοπατιού, οι πληρεξούσιοι πρέπει να έχουν την δυνατότητα να στέλνουν απαντήσεις όταν οι αιτήσεις λαμβάνονται και έπειτα για την εξέλιξη/κατάσταση της κλήσης.



Εικόνα 7 Πληρεξούσιος Διακομιστής

Stateful Proxies

Οι Stateful πληρεξούσιοι διαχειρίζονται την κατάσταση μια κλήσης στην οποία αποτελούν μέρος και όχι μόνο ένα μήνυμα. Άρα πρέπει να και να συσχετίσουν τις

αιτήσεις με τις αποκρίσεις σε κάθε διάλογο, για αυτό το λόγο αποθηκεύουν δεδομένα για την κάθε σύνοδο. Όταν γίνεται χρήση Stateful πληρεξούσιου πρέπει όλα τα μηνύματα της ίδιας συνόδου να δρομολογούνται μέσω της ίδιας διαδρομής, ώστε να επιβεβαιώνεται πως όλες οι SIP αποκρίσεις χρησιμοποιούν το ίδιο μονοπάτι με την αίτηση, έτσι ώστε ο πληρεξούσιος εξυπηρετητής να λάβει όλες τις απαντήσεις και οποιαδήποτε επιπρόσθετη αίτηση. Για να επιτευχθεί αυτό κάθε proxy προσθέτει μια VIA κεφαλίδα με την δική του διεύθυνση με σκοπό να χρησιμοποιηθεί για την δρομολόγηση της απόκρισης. Με αυτή την μέθοδο αποφεύγονται οι άσκοπες επανεκπομπές μηνυμάτων αλλά απαιτεί επιπρόσθετη κατανάλωση πόρων.

Stateless Proxies

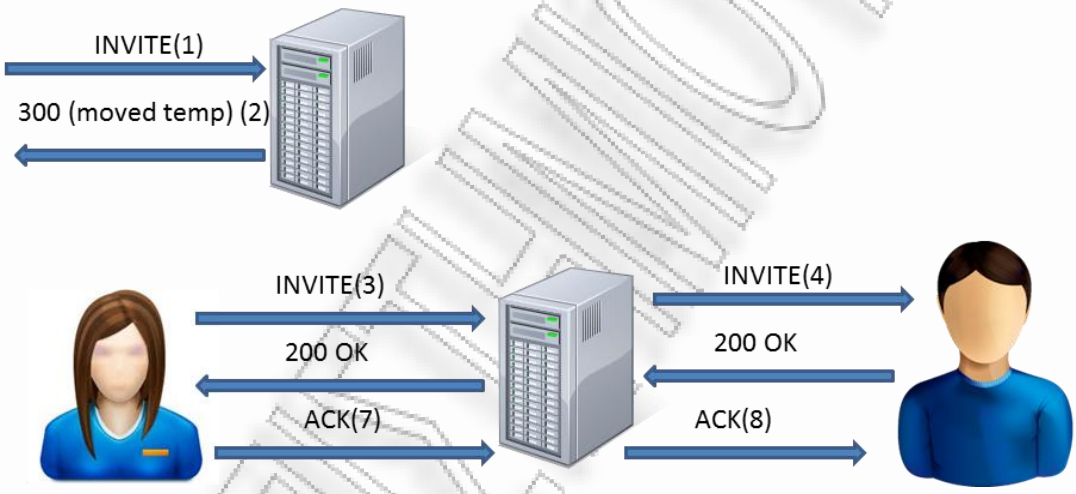
Οι stateless πληρεξούσιοι δεν γνωρίζουν την κατάσταση καμίας κλήσης παρά μόνο επεξεργάζονται και προωθούν στους κατάλληλους αποδέκτες τις αιτήσεις και τις αποκρίσεις χωρίς να διατηρεί τα δεδομένα της κλήσης μετά το πέρας της.

Forking Proxies

Οι Forkinig πληρεξούσιοι εξυπηρετητές δρομολογούν μηνύματα σε περισσότερους από έναν προορισμούς. Ένα παράδειγμα χρήσης τέτοιου εξυπηρετητή είναι στην περίπτωση που κάποιος χρήστης έχει κάνει εγγραφή με πολλές διευθύνσεις, ο Forking εξυπηρετητής θα χωρίσει την μια αρχική αίτηση σε πολλές αιτήσεις, οι οποίες θα σταλθούν σε όλους τους προορισμούς που έχουν εγγραφεί για αυτόν τον συνδρομητή. Αυτό συνεπάγεται πως μόνο η οντότητα γνωρίζει τους προορισμούς και συνεπώς πρέπει να διαχειριστεί τις αποκρίσεις από αυτούς τους προορισμούς, κάτι το οποίο απαιτεί ο Forking εξυπηρετητής να είναι stateful.

Εξυπηρετητής ανακατεύθυνσης (Redirect Server)

Ο εξυπηρετητής ανακατεύθυνσης χρησιμοποιείται για να παρέχει εναλλακτικές διευθύνσεις για αιτήσεις όταν αυτό είναι απαραίτητο. Για παράδειγμα όταν μία αίτηση για εγκατάσταση κλήσης δεν μπορεί να πραγματοποιηθεί μέσω του πληρεξούσιου εξυπηρετητή (λόγω αναβάθμισης του ή λόγω υπερφόρτωσης του από κίνηση κ.α.), τότε αναλαμβάνει ο εξυπηρετητής ανακατεύθυνσης και στέλνει μια 3xx απάντηση η οποία παρέχει τις εναλλακτικές διευθύνσεις που μπορούν να χρησιμοποιηθούν ώστε να φτάσει η αίτηση στον προορισμό της. Όταν ο καλών λάβει αυτό το μήνυμα θα δημιουργήσει εκ νέου μια αίτηση βάζοντας τις εναλλακτικές διευθύνσεις προορισμού.



Εικόνα 8 Διακομιστής Ανακατεύθυνσης

Εξυπηρετητής πύλη (Gateway)

Ένας εξυπηρετητής πύλη είναι ένα είδος πράκτορα χρήστη με την αρμοδιότητα να διασυνδέει συστήματα τηλεφωνίας που χρησιμοποιούν διαφορετικά πρωτόκολλα σηματοδοσίας. Λειτουργεί με δύο τρόπους είτε με ενθυλάκωση της σηματοδοσίας σε μηνύματα SIP αξιοποιώντας τον μηχανισμό MIME στο κύριο μέρος του μηνύματος είτε μετατρέποντας την σηματοδοσία από το ένα πρωτόκολλο στο άλλο.

2.5 SIP Μηνύματα

Τα SIP μηνύματα είναι δύο ειδών, αιτήσεις (requests) ή απαντήσεις (responses) στις αιτήσεις. Η σύνταξη τους αποτελείται από μια αρχική γραμμή (start-line) η οποία είτε είναι γραμμή αίτησης (request-line) είτε γραμμή κατάστασης (status-line) ανάλογα με το είδος του μηνύματος, έπειτα από τα πεδία των κεφαλίδων που περιγράφουν το μήνυμα, μια κενή γραμμή που σηματοδοτεί το τέλος των επικεφαλίδων και είναι απαραίτητη και προαιρετικά από το σώμα του μηνύματος (message body). Το σώμα του μηνύματος χρησιμοποιείται για να περιγράψει τις απαιτήσεις της συνόδου ή ενσωματώνει διάφορους τύπους σηματοδοσίας.

Μια έγκυρη SIP αίτηση πρέπει υποχρεωτικά να περιέχει την γραμμή αίτησης και στην συνέχεια το λιγότερο τις ακόλουθες επικεφαλίδες : To, From, Cseq, Call-ID, Max-Forwards και Via. Σε κάθε αίτηση αυτές οι επικεφαλίδες είναι υποχρεωτικές καθώς παρέχουν τις βασικές πληροφορίες για τις υπηρεσίες δρομολόγησης συμπεριλαμβανομένων την αποστολή των μηνυμάτων, την δρομολόγηση των απαντήσεων, την ακολουθία των μηνυμάτων και το μοναδικό αναγνωριστικό της συναλλαγής. Για μια έγκυρη SIP απάντηση ισχύουν τα ίδια με τα παραπάνω με μόνη διαφορά την γραμμή κατάστασης.

To: Στο πεδίο αυτό περιέχεται η λογική διεύθυνση του επιθυμητού παραλήπτη ο οποίος μπορεί να μην είναι ο τελικός παραλήπτης αλλά κάποιος ενδιάμεσος κόμβος του SIP δικτύου. Η διεύθυνση είναι SIP URI ή κάποια άλλη μορφή URI και επιτρέπεται η απεικόνιση ονόματος.

To: “Alice” <sip:alice@open-ims.test>

From: Η κεφαλίδα From δείχνει την διεύθυνση του χρήστη που δημιούργησε την αίτηση, πρόκειται για λογική ταυτότητα και όχι φυσική άρα δεν μπορεί να είναι μια διεύθυνση IP. Όμοια με την κεφαλίδα To περιέχει ένα URI και ένα όνομα προαιρετικά. Επίσης περιέχεται και μια παράμετρος “tag” η οποία προστίθεται από τον UAC έτσι ώστε να συσχετιστεί αυτό το μήνυμα με τις απαντήσεις.

From: “Alice” <sip:alice@open-ims.test>;tag=1000

Call-ID: Το πεδίο αυτής της κεφαλίδας αποτελεί ένα αναγνωριστικό ώστε να ομαδοποιείται μια σειρά μηνυμάτων που αφορούν στην ίδια σύνοδο. Όταν εγκατασταθεί καινούργια σύνοδος ακόμα και στην περίπτωση που αναμειγνύονται ίδιοι (User Agent) πράκτορες χρήστη θα δημιουργηθεί διαφορετικό Call-Id. Περιέχει ένα αριθμό και την IP του αιτούντα διαχωρισμένα από το σύμβολο @.

Call-ID:409d5cd56788534c724e981ee9f3b9571c@192.168.2.3

Cseq: Σύμφωνα με αυτή την κεφαλίδα ορίζεται η σειρά του μηνύματος μέσα σε ένα διάλογο. Αποτελείται από μια μέθοδο και έναν αριθμό, η μέθοδος πρέπει να ταυτίζεται με αυτή της αίτησης. Κάθε client θα πρέπει να έχει κάποιον μηχανισμό προκειμένου να επιλέγει μία τιμή για την Cseq κεφαλίδα, σύμφωνα με τις παραπάνω κατευθυντήριες οδηγίες.

Cseq: 1 REGISTER

Max-Forwards: Το Max-Forwards χρησιμοποιείται με σκοπό να θέτει ένα όριο στον αριθμό των κόμβων μέσω των οποίων μια αίτηση θα μεταφερθεί μέχρι να φτάσει στον προορισμό της. Αυτό το πεδίο περιέχει έναν ακέραιο αριθμό ο οποίος μειώνεται κατά ένα σε κάθε hop. Εάν αυτή η τιμή γίνει 0 πριν το μήνυμα φτάσει στον προορισμό, θα απορριφθεί και θα στείλει στον αποστολέα ένα μήνυμα λάθους 483(Too Many Hops). Στο RFC 3261 προτείνεται αυτή η τιμή να είναι 70, δηλαδή επαρκώς μεγάλη έτσι ώστε να εγγυάται πως το μήνυμα θα φτάσει όταν δεν υπάρχουν routing loops αλλά και στην περίπτωση που λαμβάνουν χώρα άσκοποι βρόχοι να μην καταναλώνονται οι πόροι των πληρεξούσιων εξυπηρετητών. Χαμηλότερες τιμές είναι προτιμότερο να χρησιμοποιούνται όταν η τοπολογία του δικτύου είναι γνωστή.

Max-Forwards: 20

Via: Το πεδίο της κεφαλίδας Via υποδεικνύει το πρωτόκολλο μεταφοράς που χρησιμοποιείται για την συναλλαγή, την έκδοση του πρωτοκόλλου SIP και την τοποθεσία στην οποία θα σταλθεί η απάντηση. Επίσης στην κεφαλίδα αυτή πρέπει

να περιέχεται και μια παράμετρος branch, η οποία χρησιμοποιείται για να προσδιοριστεί η συναλλαγή που δημιουργήθηκε από μία αίτηση. Η τιμή της παραμέτρου πρέπει να είναι μοναδική για όλες τις αιτήσεις που στέλνονται από έναν UA με εξαίρεση τα μηνύματα CANCEL και ACK και ξεκινάει πάντα με τους χαρακτήρες “z9hG4bK”.

Via:SIP/2.0/UDP
192.168.2.3:5060;branch=z9hG4bKc8ff825bfc09eac462c0a256dc5fe59a363939

Contact: Σε αυτό το πεδίο κεφαλίδας δηλώνεται η διεύθυνση στην οποία επιθυμεί ο αποστολέας να λαμβάνει τις επόμενες αιτήσεις. Όταν υπάρχουν πολλαπλά URIs σε αυτό το πεδίο χρησιμοποιείται η παράμετρος q η οποία δείχνει με ποια σειρά να χρησιμοποιηθούν τα URIs. Ένας redirect server χρησιμοποιεί αυτό το πεδίο για να βρει εναλλακτικές διευθύνσεις.

Contact: “Alice” <sip:alice@192.168.2.3:5060>;+sip.instance=acde2e7b-0a1b-4a02-9855-d0060fe11402

Εκτός όμως από αυτές τις βασικές επικεφαλίδες υπάρχουν αρκετές ακόμα που δίνουν επιπλέον πληροφορίες για το μήνυμα. Ενδεικτικά αναφέρονται οι παρακάτω:

Contect Length: Το πεδίο αυτό δείχνει το μέγεθος του σώματος του μηνύματος, είναι μια δεκαδική τιμή η οποία είναι ίση με το μηδέν σε περίπτωση μη ύπαρξης σώματος του μηνύματος.

Contect Length: 256

Expires: Επιτρέπει στον αποστολέα να δηλώσει πότε ένα γεγονός θα λήξει. Για παράδειγμα όταν αυτή η επικεφαλίδα στέλνεται μαζί με ένα REGISTER μήνυμα, η Expires τιμή δηλώνει μετά από πόσα δευτερόλεπτα η εγγραφή θα λήξει. Συνεπώς μετά από αυτό το χρονικό διάστημα ο χρήστης θα πρέπει να εγγραφεί ξανά.

Expires: 10

MIME Version: Στην περίπτωση που υπάρχει στο σώμα κειμένου περιεχόμενο σε MIME μορφή, αυτή η επικεφαλίδα δείχνει την έκδοση του MIME, ώστε ο παραλήπτης του μηνύματος να καταφέρει να το αποκωδικοποιήσει σωστά.

MIME-VERSION: 1.0

Priority: Αυτή η επικεφαλίδα προστίθεται σε περίπτωση κλήσεων έκτακτης ανάγκης ώστε να έχουν προτεραιότητα σε σχέση με τις φυσιολογική κίνηση του δικτύου. Το RFC ορίζει μερικές προτεινόμενες τιμές για την επικεφαλίδα Priority "normal", non-urgent", "urgent" και "emergency".

Priority: Urgent

2.5.1 SIP Αιτήσεις

Οι SIP αιτήσεις αποτελούνται από την αρχική γραμμή request-line, ακολουθούμενη από τις κεφαλίδες και προαιρετικά από το σώμα του μηνύματος. Η γραμμή αίτησης του μηνύματος περιέχει το όνομα της μεθόδου, την διεύθυνση URI και την έκδοση του πρωτοκόλλου. Όπως βλέπουμε στην παρακάτω εικόνα στην γραμμή αίτησης υπάρχει η μέθοδος REGISTER, η οποία καθορίζει την ενέργεια που επιθυμεί να κάνει ο αποστολέας αυτού του μηνύματος. Οι βασικές μέθοδοι που υποστηρίζονται από το SIP είναι οι εξής:

INVITE: Εγκατάσταση συνόδου μεταξύ χρηστών

ACK: Επιβεβαίωση σε μήνυμα αίτησης (INVITE REQUEST)

CANCEL: Τερματισμός μιας εν αναμονής αίτησης

BYE: Τερματισμός μιας συνόδου

OPTION: Αναζήτηση πληροφοριών για τις ικανότητες των εξυπηρετητών

Η παρακάτω εικόνα απεικονίζει μια SIP αίτηση για εγγραφή από τον χρήστη με URI bob@open-ims.test η οποία λήγει μετά από 300 δευτερόλεπτα, στο πεδίο Contact δηλώνεται η διεύθυνση επικοινωνία του χρήστη, το Max-Forward είναι 70 όπως

προτείνει το RFC και δηλώνει 70 ως μέγιστους κόμβους μέσα από τους μπορεί να δρομολογηθεί το συγκεκριμένο μήνυμα μέχρι να φτάσει στον προορισμό του. Call-ID και CSeq αφορούν το αναγνωριστικό του μηνύματος και την σειρά με την οποία στάλθηκε αντίστοιχα.

Request-Line: REGISTER sip:open-ims.test SIP/2.0
Via: SIP/2.0/UDP 10.1.14.144:5060;rport;branch=z9hjoajishsuudapppianxpspeVEM
Max-Forwards: 70
From: <sip:bob@open-ims.test>;tag=iywhxooxkyaswaoJgDf
To: <sip:bob@ open-ims.test>
Call-ID: FgaoaHertUpid
CSeq:40206 REGISTER
Contact: sip:bob@10.1.14.144:5060;ob
Expires: 300

2.5.2 SIP Αποκρίσεις

Οι SIP αποκρίσεις οι οποίες καθορίζονται όπως και οι SIP αιτήσεις από το RFC 3261 είναι τα μηνύματα που στέλνονται ως απαντήσεις στις SIP αιτήσεις. Διακρίνονται από τα μηνύματα αιτήσεων από την αρχική γραμμή, η γραμμή αίτησης αντικαθίσταται από την γραμμή κατάστασης. Στην γραμμή κατάστασης περιέχονται η έκδοση του πρωτοκόλλου, ένας τριψήφιος αριθμός ο οποίος λέγεται κωδικός κατάστασης και μια φράση που αντιστοιχεί στην περιγραφή του κωδικού αυτού. Το πρώτο ψηφίο του κωδικού κατάστασης καθορίζει την κατηγορία της απάντησης, τα δύο τελευταία ψηφία δεν έχουν κάποιο ρόλο κατηγοριοποίησης και ως εκ τούτου κάθε απόκριση με κωδικό κατάστασης ανάμεσα στο 100 και στο 199 αναφέρεται ως 1xx απόκριση. Ουσιαστικά τα μηνύματα αυτά πληροφορούν τον αιτών για την επιτυχία ή αποτυχία της αίτησης. Περιέχουν επίσης αν είναι απαραίτητο πληροφορίες για την επιτυχή ολοκλήρωση της επιτυχίας ή τους λόγους αποτυχίας. Οι κατηγορίες των μηνύματα των αποκρίσεων με βάση το πρώτο ψηφίο του κωδικού κατάστασης είναι οι εξής :

1xx Provisional:	Λήψη της αίτησης, συνεχιζόμενη διαδικασία αίτησης
2xx Success:	Επιτυχής διεκπεραίωση αίτησης
3xx Redirection:	Περισσότερες ενέργειες πρέπει να γίνουν για να ολοκληρωθεί η αίτηση
4xx Client Error:	Η αίτηση περιέχει λάθος σύνταξη ή δεν μπορεί να πραγματοποιηθεί σε αυτόν τον εξυπηρετητή
5xx Server Error:	Ο εξυπηρετητής απέτυχε να πραγματοποιήσει μια έγκυρη αίτηση
6xx Global Failure:	Η αίτηση δεν μπορεί να πραγματοποιηθεί σε κανέναν εξυπηρετητή

2.5.3 Διευθυνσιοδότηση

Όπως έγινε σαφές από τα παραπάνω βασικό στοιχείο σε όλα τα μηνύματα αιτήσεων και αποκρίσεων είναι ο προσδιορισμός των διευθύνσεων των μερών που επικοινωνούν, διότι χωρίς αυτές η επικοινωνία είναι ανέφικτη. Οι πόροι ενός SIP δικτύου αναγνωρίζονται μέσω του SIP URI ή του SIPS URI. Δεν υπάρχει διαφορά στην μορφή ανάμεσα στα δύο URIs, απλώς το SIPS URI δηλώνει πως η σύνοδος ανάμεσα στο UA και στον πόρο που διευθυνσιοδοτείται γίνεται με χρήση κρυπτογράφησης. Ένας πόρος του δικτύου μπορεί να είναι ένα πρόσωπο ή ένας εξυπηρετητής.

Η επίσημη σύνταξη του SIP URI όπως ορίζεται από το RFC 3261 είναι:

sip : user : password@host : port ; Uri-parameters ?headers

User είναι το αναγνωριστικό του χρήστη, το πεδίο του password είναι ένας κωδικός συσχετισμένος με τον χρήστη αλλά είναι προτιμότερο σύμφωνα με το RFC να παραλείπεται αφού το μήνυμα μεταδίδεται σε plain-text. Το host παρέχει τον SIP πόρο και μπορεί να προσδιοριστεί με την χρήση είτε του domain name ή της IP διεύθυνσης. Στην περίπτωση χρήσης IP διεύθυνσης, η διεύθυνση πρέπει να είναι στατική και μπορεί να υποστηριχθεί IPv4 και IPv6 έκδοση και στην περίπτωση του domain name ο UA που θα λάβει το μήνυμα μπορεί να καθορίσει την IP μέσω του

DNS. Η θύρα μπορεί επίσης να δηλωθεί αλλά αποτελεί ένα προαιρετικό πεδίο. Τέλος οι URI παράμετροι είναι επίσης μη υποχρεωτικοί. Παράδειγμα URI παραμέτρου αποτελεί η maddr παράμετρος η οποία φανερώνει την διεύθυνση του διακομιστή για να έρχεται σε επαφή με αυτό τον χρήστη, όταν αυτή η παράμετρος είναι παρούσα η θύρα και τα στοιχεία της μεταφοράς του URI αντικαθιστούνται από αυτά της παραμέτρου.

Το URI είναι εφικτό να έχει και μορφή τηλεφωνικού αριθμού, όταν χρησιμοποιείται τηλεφωνικός αριθμός οι πληροφορίες του χρήστη αντικαθιστούνται από τα ψηφία του αριθμού.

anna@unipi.gr
Anna@192.68.2.1:5060
Sip:12123123@unipi.gr

(Russel)

2.6 Δομή Πρωτοκόλλου

Το SIP είναι δομημένο σε τέσσερα επίπεδα, καθένα από τα οποία έχει το δικό του σύνολο κανόνων. Όταν λέμε πως ένα στοιχείο (οντότητα) του SIP πρωτοκόλλου περιέχει ένα επίπεδο στην ουσία εννοούμε πως συμμορφώνεται σε ένα σύνολο κανόνων που καθορίζονται από το συγκεκριμένο επίπεδο. Επιπλέον δεν πρέπει να ξεχνάμε πως μια SIP οντότητα δεν είναι ένα φυσικό στοιχείο αλλά ένα λογικό, συμπερασματικά μια φυσική οντότητα μπορεί να υποστηρίζει διαφορετικές λογικές οντότητες. Κάθε SIP οντότητα δεν περιέχει όλα τα επίπεδα, εξαρτάται από τις λειτουργίες της. Εν τούτης όλες οι οντότητες πρέπει να μπορούν να υποστηρίξουν τα πρώτα δύο επίπεδα. Τα επίπεδα του πρωτοκόλλου SIP είναι τα εξής:

- Transaction user (Συνδιαλλαγή χρήστη)
- Transaction layer (Επίπεδο δοσοληψίας)
- Transport layer (Επίπεδο μεταφοράς)
- Syntax and encoding (Σύνταξης και κωδικοποίησης)

Το **επίπεδο σύνταξης και κωδικοποίηση**ς είναι το χαμηλότερο επίπεδο που ορίζεται στο SIP πρωτόκολλο και είναι υποχρεωτικό να υλοποιείται σε κάθε οντότητα δικτύου αφού σε αυτό γίνεται η συντακτική ανάλυση του μηνύματος. Για παράδειγμα όταν ληφθεί ένα μήνυμα από μια δικτυακή οντότητα πρέπει να κατανοήσει τι είδους μήνυμα είναι και για κάθε επικεφαλίδα που αρχίζουν και που τελειώνουν οι παράμετροι, κάτι το οποίο αποτελεί μέρος των ευθυνών αυτού του επιπέδου αφού ουσιαστικά μπορεί να οριστεί ως το σύνολο των κανόνων που ορίζουν και αποτελούν την μορφή και την δομή κάθε SIP μηνύματος.

Το αμέσως υψηλότερο επίπεδο είναι υπεύθυνο για την μεταφορά των αιτήσεων και αποκρίσεων. Κάθε SIP οντότητα δημιουργεί και στέλνει μηνύματα μέσω του δικτύου σε κάποια άλλη οντότητα, συνεπώς είναι απαραίτητο κάθε οντότητα να υλοποιεί το **επίπεδο μεταφοράς**. Σε αυτό το επίπεδο διαχειρίζονται οι συνδέσεις για τα πρωτόκολλα μεταφοράς όπως το TCP ή το SCTP. Για κάθε σύνδεση που εγκαθίσταται μεταξύ δύο οντοτήτων, συντάσσεται ένας πίνακας ο οποίος αποτελείται από την IP διεύθυνση, τον αριθμό της θύρας και το πρωτόκολλο μεταφοράς. Όταν μια σύνδεση δημιουργείται από το επίπεδο μεταφοράς αυτός ο πίνακας έχει οριστεί με την διεύθυνση IP του προορισμού, την θύρα και το πρωτόκολλο μεταφοράς. Όταν η σύνδεση γίνεται αποδεκτή από το επίπεδο μεταφοράς , αυτός ο πίνακας ορίζεται από τα στοιχεία της πηγής και όχι του αποδέκτη όπως στην προηγούμενη περίπτωση.

Μια δοσοληψία ορίζεται ως μια αίτηση σταλμένη από τον SIP πελάτη στον SIP εξυπηρετητή χρησιμοποιώντας το επίπεδο μεταφοράς, συμπεριλαμβάνοντας όλες τις απαντήσεις που σχετίζονται με αυτήν την αίτηση. Το **επίπεδο δοσοληψίας** είναι υπεύθυνο για την διαχείριση επανεκπομπών επιπέδου εφαρμογής, συσχετισμών των απαντήσεων με τις σχετικές αιτήσεις και τις λήξεις χρόνου. Μόνο οι πράκτορες χρήστη και οι stateful proxies έχουν επίπεδο συνδιαλλαγής. Το επίπεδο δοσοληψίας προσδιορίζει δύο ειδών δοσοληψίες τις δοσοληψίες πελάτη (client transaction) και τις δοσοληψίες εξυπηρετητή (server transaction). Κάθε μια από τις παραπάνω κατηγορίες αναπαρίσταται από μια μηχανή πεπερασμένης κατάστασης (finite state machine FSM) ανάλογη με το τύπο του μηνύματος που διαχειρίζεται.

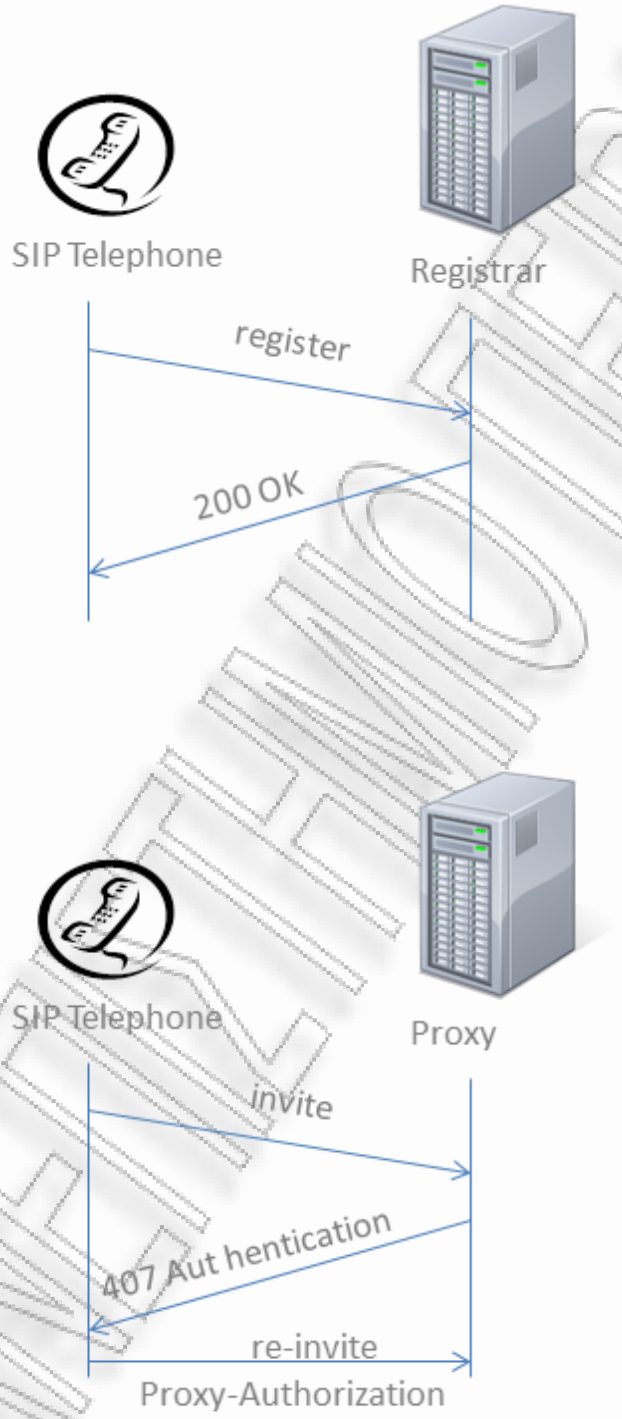
Όλες οι SIP οντότητες εκτός από τους stateless proxy δημιουργούν SIP δοσοληψίες συνεπώς είναι **χρήστες δοσοληψίας**. Ο χρήστης δοσοληψίας είναι μια οντότητα που δημιουργεί μια δοσοληψία πελάτη όπως για παράδειγμα ένα μήνυμα INVITE και επίσης έχει την ικανότητα να ακυρώνει την δοσοληψία. Άρα όταν ο χρήστης δοσοληψίας στείλει ένα αίτημα δημιουργεί μια δοσοληψία πελάτη μαζί με τα απαιτούμενα δεδομένα διεύθυνση IP , θύρα και πρωτόκολλο μεταφοράς του παραλήπτη και όταν στείλει αίτημα CANCEL δημιουργείται εκ νέου μια δοσοληψία και ακυρώνεται η προηγούμενη.

Παραπάνω έγινε η αναφορά στις SIP οντότητες user agent client και server, statelless και statefull proxies και registrars. Για να διαχωρίζονται αυτές οι οντότητες περιέχουν έναν πυρήνα, οι πυρήνες αυτοί πέραν του stateless proxy είναι οι χρήστες δοσοληψίας. Ενώ η συμπεριφορά των UAC και UAS διαφέρει ανάλογα με την μέθοδο υπάρχουν κάποιοι κανόνες που είναι για όλες τις μεθόδους ίδιοι. Για το UAC αυτοί οι κανόνες διέπουν την κατασκευή μιας αίτησης και για το UAS την επεξεργασία μιας αίτησης και την δημιουργία μια απάντησης.

2.7 Εγκατάσταση Συνόδου

Με την έννοια σύνοδος στο πρωτόκολλο SIP εννοούμε βίντεο κλήση, μήνυμα κειμένου, e-mail ή αναπαραγωγή βίντεο. Για να εγκατασταθεί μια σύνοδος πρέπει να υπάρξει διάλογος μεταξύ των οντοτήτων που προσπαθούν να συνδεθούν, κάτι το οποίο τους επιτρέπει να ανταλλάξουν τις απαραίτητες πληροφορίες σχετικά με την σύνδεση. Όταν ένας χρήστης επιθυμεί να καλέσει ένα άλλον χρήστη στέλνει ένα μήνυμα SIP INVITE (το μήνυμα αυτό όπως έχουμε δει παραπάνω στο στέλνει ο UAC) στον αντίστοιχο SIP proxy, ο οποίος ελέγχει στην βάση δεδομένων του Registrar (ή στο DNS), την διεύθυνση του καλούντος και προωθεί την αίτηση εκεί. Ο καλούμενος μπορεί να αποδεχτεί ή να απορρίψει την αίτηση. Κατά την διάρκεια αποστολής αυτών των μηνυμάτων έχει ουσιαστικά δημιουργηθεί ένας διάλογος και οι χρήστες ανταλλάσσουν την διεύθυνση, την θύρα που θέλουν να λαμβάνουν τα δεδομένα της συνόδου που θα δημιουργηθεί και τον τύπο των δεδομένων (βίντεο, φωνή κτλ)

που μπορούν να δεχτούν. Μετά το τέλος των μηνυμάτων έχει πλέον εγκατασταθεί η σύνοδος και οι χρήστες θα ανταλλάσσουν δεδομένα χωρίς την ανάμειξη του proxy.



Εικόνα 9 Ροή μηνυμάτων SIP

Κεφάλαιο 3 Προβλήματα και Μηχανισμοί Ασφάλειας

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο γίνεται περιγραφή των επιθέσεων ξεκινώντας από αυτές στην PSTN και διαδικτυακή τηλεφωνία, καταλήγοντας σε αυτές που αφορούν συγκεκριμένα στο SIP πρωτόκολλο. Μετά την περιγραφή των πιθανών απειλών προκύπτουν οι απαιτήσεις από πλευρά ασφάλειας, στην συνέχεια περιγράφονται οι μηχανισμοί ασφάλειας και τέλος καταγράφεται μια σύντομη σύγκριση των μηχανισμών ασφάλειας.

3.2 Επιθέσεις σε PSTN και διαδικτυακή τηλεφωνία

Για να πραγματοποιηθεί μια επίθεση σε ένα σύστημα απαραίτητη προϋπόθεση αποτελεί η ύπαρξη μια ευπάθειας την οποία και εκμεταλλεύεται μια απειλή με στόχο να δημιουργήσει συγκεκριμένες επιπτώσεις. Εν τούτοις επίθεση θεωρείται κάθε προσπάθεια παραβίασης των υπηρεσιών ασφάλειας ενός πληροφοριακού συστήματος.

Οι περισσότεροι χρήστες υπηρεσιών τηλεφωνίας είναι εξοικειωμένοι με το PSTN δίκτυο καθώς αυτό χρησιμοποιείται για περισσότερο από 100 χρόνια . Παρά όμως τα πολλά χρόνια λειτουργίας του έχουν ληφθεί λίγα μέτρα για την προστασία των δεδομένων που μεταδίδονται μέσω αυτού. Το γεγονός αυτό οφείλεται στο ότι το PSTN βασίζεται σε ένα κλειστό δίκτυο, στο οποίο υπάρχει περιορισμένη πρόσβαση. Όμως ακόμα και στο PSTN υπάρχουν προβλήματα ασφάλειας, τα πιο διαδεδομένα από τα οποία είναι η μη εξουσιοδοτημένη πρόσβαση (unauthorized access) η οποία απαιτεί φυσική πρόσβαση στο δίκτυο, η διεκπεραίωση κλήσεων χωρίς χρέωση (toll frauds calls) που οφείλεται στην μη ορθή διαχείριση των μηνυμάτων εκτός της προκαθορισμένης διαδικασίας και η άρνηση παροχής υπηρεσιών (denial of service). Τα προβλήματα ασφαλείας που εμφανίζονται στο PSTN οφείλονται στην έλλειψη μηχανισμών ασφαλείας για την παροχή υπηρεσιών εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας, στην μη ορθή διαχείριση των δεδομένων που

υφίστανται επεξεργασία και στην συνεργασία του επιτιθέμενου με κάποιον από τους εσωτερικούς χρήστες.

Οι απειλές που εμφανίζονται στα τηλεπικοινωνιακά δίκτυα έχουν ομοιότητες, αυτό που στην ουσία διαφοροποιείται δεν είναι η υπηρεσία αλλά η υποδομή την οποία αξιοποιεί η υπηρεσία. Στην περίπτωση του PSTN για την παροχή της τηλεφωνίας αξιοποιείται ένα κλειστό δίκτυο, ενώ για την διαδικτυακή τηλεφωνία αξιοποιείται το διαδίκτυο. Αυτή και μόνο βέβαια η διαφορά διευκολύνει την πραγματοποίηση αρκετών επιθέσεων. Για παράδειγμα για την επίτευξη μη εξουσιοδοτημένης πρόσβασης στο PSTN αποτελεί προϋπόθεση η φυσική πρόσβαση σε ένα κλειστό δίκτυο, σε αντίθεση με την περίπτωση της διαδικτυακής τηλεφωνίας όπου η πρόσβαση στο δίκτυο είναι άμεση και η μη εξουσιοδοτημένη πρόσβαση αποτελεί μια διαδικασία χωρίς ιδιαίτερη δυσκολία. Γίνεται σαφές πως λόγω της φύσης της διαδικτυακής τηλεφωνίας υπόκεινται στις ίδιες απειλές με κάθε υπηρεσία μέσω διαδικτύου αλλά και σε αυτές λόγω του είδους της υπηρεσίας. Άρα στην διαδικτυακή τηλεφωνία χρήζουν αντιμετώπισης τόσο οι απειλές που συναντάμε στο PSTN όσο και απειλές που εμφανίζονται μόνο στην διαδικτυακή τηλεφωνία. Για παράδειγμα μια απειλή που αφορά αποκλειστικά στην διαδικτυακή τηλεφωνία είναι η πλαστοπροσωπία αφού ο χρήστης προσδιορίζεται από ένα αναγνωριστικό και όχι από μία φυσική διεύθυνση. Ένας κακόβουλος χρήστης είναι πιθανό να στείλει αίτημα στον πάροχο διαδικτυακής τηλεφωνίας χρησιμοποιώντας το αναγνωριστικό κάποιου άλλου χρήστη με σκοπό την αποφυγή χρέωσης του. Επίσης ο επιτιθέμενος μπορεί να λειτουργήσει εκ μέρους της υπηρεσίας ή κάποιου ενδιάμεσου εξυπηρετητή εκμεταλλευόμενος το γεγονός πως το δίκτυο δεν αυθεντικοποιείται στο χρήστη.

3.3 Προβλήματα Ασφάλειας στο SIP

Οι χρήστες έχοντας συνηθίσει στην χρήση του PSTN έχουν και ανάλογες απαιτήσεις ασφάλειας και ιδιωτικότητας και στις υπηρεσίες VOIP, κάτι το οποίο είναι πιο περίπλοκο από την στιγμή που αναφερόμαστε σε υπηρεσίες διαδικτύου.

Συγκεκριμένα για το πρωτόκολλο σηματοδοσίας SIP, τα μηνύματα τα οποία μεταφέρονται περιέχουν πληροφορίες σχετικές με τους χρήστες που επικοινωνούν τις οποίες πιθανόν ο χρήστης να ήθελε να κρατήσει κρυφές. Οι επικεφαλίδες αλλά και το σώμα των μηνυμάτων SIP περιέχουν διευθύνσεις επαφής, ονόματα χρηστών, κλειδιά ασφάλειας κ.α καθώς και όλες τις παραμέτρους που είναι απαραίτητες για την αποκατάσταση συνδέσεων. Οι προαναφερθείσες πληροφορίες θα πρέπει να τηρούνται εμπιστευτικές. Η κρυπτογράφηση θα μπορούσε να αποτελέσει μια λύση σε αυτό το πρόβλημα όμως είναι ανέφικτη στην συγκεκριμένη περίπτωση καθώς τα μηνύματα δρομολογούνται μέσω διαφορετικών πληρεξούσιων εξυπηρετητών και απαιτούν πρόσβαση σε συγκεκριμένα τμήματα του μηνύματος ώστε να επιτευχθεί η σωστή δρομολόγηση στο τελικό παραλήπτη. Για αυτό τον λόγο όταν αναφερόμαστε σε μηνύματα σηματοδοσίας εννοούμε μηνύματα plain text.

Το γεγονός πως τα SIP μηνύματα έχουν μορφή απλού κειμένου δίνουν την ευκαιρία σε επιθέσεις όπως spoofing, hijacking και αλλοιώσεις μηνυμάτων. Η χρήση κακόβουλων SIP μηνυμάτων είναι επίσης μια πιθανή απειλή και μπορεί να προκαλέσει μη εξουσιοδοτημένη πρόσβαση ή άρνηση παροχής υπηρεσιών (DoS). Το πρωτόκολλο SIP σύμφωνα με το RFC 3261 χρησιμοποιεί πρωτόκολλα μεταφοράς όπως το TCP, UDP, SCTP. Ως εκ τούτου το SIP κληρονομεί όλες τις ευπάθειες αυτών των πρωτοκόλλων. Για παράδειγμα θεωρώντας ότι το TCP είναι ευπαθές σε επιθέσεις όπως SYN flood ή TCP session hijacking, είναι πολύ πιθανόν πως το SIP θα είναι επίσης ευπαθές σε όμοιες επιθέσεις. Επιπρόσθετα η διασύνδεση του SIP με το PSTN, εισάγει νέα πιθανά σημεία αποτυχίας, όπως VOIP πύλες οι οποίες είναι ευπαθείς σε επιθέσεις άρνησης υπηρεσιών ή αλλοίωση των μηνυμάτων. Υπάρχουν δύο ειδών πιθανές απειλές σε ένα δίκτυο SIP, οι εξωτερικές και οι εσωτερικές. Οι εξωτερικές απειλές πραγματοποιούνται από κάποιον μη συμμετέχοντα στην ροή των μηνυμάτων κατά την διάρκεια μιας SIP κλήσης. Οι εξωτερικές απειλές συχνά συμβαίνουν σε περιπτώσεις που η φωνή και πακέτα σηματοδοσίας περιλαμβάνουν δίκτυα τρίτων. Οι εσωτερικές απειλές συχνά πραγματοποιούνται από χρήστες κλήσεων μέσω SIP, οι χρήστες αυτοί έχουν ορίσει σχέσεις εμπιστοσύνης και δεν είναι αναμενόμενο ότι θα προάγουν μια επίθεση. (D. Geneiatakis) (Samer EL SAWDA)

Στο υπόλοιπο του κεφαλαίου αναφέρονται κάποιες από τις πιθανές επιθέσεις ενάντια του SIP πρωτοκόλλου.

Eavesdropping

Μια από τις πιο γνωστές επιθέσεις σε συστήματα επικοινωνιών είναι οι υποκλοπές κλήσεων. Ενώ στο PSTN είχαμε μόνο δεδομένα φωνής ως στόχο αυτής της επίθεσης, στις VoIP υπηρεσίες που είναι βασισμένες στο πρωτόκολλο SIP στόχο αποτελούν και τα SIP μηνύματα τα οποία περιέχουν πληροφορία σχετικά με την ταυτότητα του χρήστη, την διεύθυνση επαφής και όλα εκείνα τα δεδομένα που είναι απαραίτητα για την εγκατάσταση μιας συνόδου μεταξύ δύο SIP συμμετεχόντων. Έτσι έχοντας από την μια εργαλεία eavesdropping τα οποία είναι ευρέως διαδεδομένα στο Internet και από την άλλη τα μηνύματα κειμένου του SIP πρωτοκόλλου, η επιτυχία μιας τέτοιου είδους επίθεσης γίνεται σχετικά εύκολη.

Στην περίπτωση κατά την οποία ο επιτιθέμενος υποκλέπτει μηνύματα SIP REGISTER έχουμε ως πιθανά αποτελέσματα αποκάλυψη ιδιωτικών πληροφοριών του χρήστη. Αν η υποκλοπή γίνει σε σύνολο μηνυμάτων SIP REGISTER είναι εφικτή η ανάλυση κίνησης ή ακόμα και η αποκάλυψη του συνθηματικού του χρήστη. Ακόμα και αν τα δεδομένα σηματοδοσίας προστατεύονται με κατάλληλο μηχανισμό κρυπτογράφησης, ο επιτιθέμενος είναι πιθανό να προσπαθήσει να ανακαλύψει τα αντίστοιχα κρυπτογραφικά κλειδιά.

Οι επιθέσεις της συγκεκριμένης κατηγορίας φυσικά επηρεάζουν την ασφάλεια και σε άλλα επίπεδα, όπως την διαθεσιμότητα αφού μπορεί να αποτελέσουν το πρώτο βήμα για κάποια άλλη επίθεση (DoS attack). Ομοίως και την ακεραιότητα.

Signaling Attacks

Επίθεση σηματοδοσίας θεωρείται κάθε προσπάθεια παράνομης τροποποίησης των μηνυμάτων σηματοδοσίας με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης ή/και την τροποποίηση της κατάστασης εγκατεστημένων συνόδων. Οι επιθέσεις σηματοδοσίας στο SIP είναι συνδεδεμένες με απειλές όπως απάτη χρεώσεων, προσποίηση πελάτη και εξυπηρετητή και άρνηση παροχής υπηρεσιών.

Οι κύριες αιτίες εμφάνισης των επιθέσεων σηματοδοσίας είναι πρώτον η μη ορθή χρήση των μηχανισμών αυθεντικόποιησης, είτε γιατί η εφαρμογή μηχανισμού αυθεντικοποίησης δεν είναι υποχρεωτική για όλες τις μεθόδους είτε γιατί σε κάποιες περιπτώσεις δεν είναι εφικτή η η εφαρμογή του λόγω των ίδιων των προδιαγραφών του SIP. Δεύτερη αιτία για την εμφάνιση αυτών των επιθέσεων είναι και η έλλειψη μηχανισμών διασφάλισης της ακεραιότητας των μηνυμάτων σηματοδοσίας. Για να καταφέρει ο επιτιθέμενος να πραγματοποιήσει μια τέτοιου είδους επίθεση πρέπει πρώτα να κρυφακούσει τις παραμέτρους της συνόδου ώστε να αντιστοιχήσει τα SIP μηνύματα με την κατάλληλη σύνοδο.

Υπάρχουν αρκετά σενάρια επιθέσεων σηματοδοσίας, ένα από αυτά αποτελεί η περίπτωση κατά την οποία ο κακόβουλος χρήστης προσποιείται τον εξουσιοδοτημένο χρήστη (MITM) και ως εκ τούτου μπορεί να διακόψει ή να τροποποιήσει τα μηνύματα κατά την διάρκεια της διαδικασίας εγγραφής. Υπάρχει περίπτωση ακόμα και να αλλάξει την διεύθυνση του νόμιμου χρήστη με σκοπό να λαμβάνει κλήσεις εκ μέρους του ή ακόμα και να θέσει την τιμή στη επικεφαλίδα λήξης εγγραφής “0” ώστε να αποσυνδέσει τον νόμιμο χρήστη και να μην καταφέρει να εγγραφεί στην υπηρεσία. Επίσης ο κακόβουλος χρήστης είναι δυνατόν να ωθήσει τον νόμιμο χρήστη να δημιουργήσει το κατάλληλο SIP REGISTER μήνυμα στο οποίο θα περιέχονται και τα διαπιστευτήρια του, προωθώντας του “ unauthorized” μήνυμα που έχει παραχθεί από τον Registar μετά από αίτηση του επιτιθέμενου.

Τέλος, υπάρχει και το ενδεχόμενο υποκλοπής μηνύματος με στόχο την αξιοποίηση του μελλοντικά. Ο επιτιθέμενος έχοντας στην κατοχή του ένα έγκυρο μήνυμα εγγραφής ενός εξουσιοδοτημένου χρήστη με διαπιστευτήρια που έχουν υπολογισθεί σε προηγούμενη σύνδεση μπορεί να πραγματοποιήσει επίθεση επανάληψης. Η προϋπόθεση για να πραγματοποιηθεί με επιτυχία αυτή η επίθεση είναι η υπηρεσία εγγραφής να μην αντιλαμβάνεται τέτοιου είδους επιθέσεις λόγω έλλειψης υλοποίησης κατάλληλου μηχανισμού κατά τον σχεδιασμό της.

Παραπάνω έγινε αναφορά σε επιθέσεις κατά την διαδικασία εγγραφής, όμως επιθέσεις σηματοδοσίας είναι πιθανό να συμβούν και κατά την διαδικασία αποκατάστασης συνόδου . Σε ένα τέτοιου είδους σενάριο ο κακόβουλος χρήστης τροποποιεί το SIP INVITE μήνυμα που στέλνει ο εξουσιοδοτημένος χρήστης και συγκεκριμένα αλλάζει την διεύθυνση επαφής και έπειτα το προωθεί στον SIP Proxy. Ο Proxy στέλνει την αίτηση στον καλούμενο ο οποίος αν δεχτεί την κλήση στέλνει ένα "200 OK" μήνυμα στον Proxy ο οποίος με την σειρά του θα προωθήσει το μήνυμα στον επιτιθέμενο. Ο τελευταίος θα αντικαταστήσει το μήνυμα με ένα "busy" μήνυμα και θα το αποστείλει στον νόμιμο χρήστη ο οποίος τερματίζει την σύνοδο. Ωστόσο η σύνοδος μεταξύ του κακόβουλου χρήστη και του καλούμενου έχει εγκατασταθεί επιτυχώς.

Σε επιθέσεις απάτης χρεώσεων FakeBusy, ByeDealy, ByeDrop, InviteReplay εντοπίζεται η διαφορά στην ύπαρξη ενός ακόμα επιτιθέμενου που λειτουργεί από την πλευρά του καλούμενου. Ο επιτιθέμενος που βρίσκεται στην πλευρά του καλούντα τροποποιεί το αρχικό SIP INVITE μήνυμα όπως και στην προηγούμενη περίπτωση, στέλνοντας στον καλούντα ότι ο καλούμενος είναι απασχολημένος. Ο επιτιθέμενος που βρίσκεται στην πλευρά του καλούμενου παρεμποδίζει την προώθηση των μηνυμάτων στον καλούμενο αλλάζοντας την διεύθυνση επαφής του εξουσιοδοτημένου χρήστη με την δική του με αποτέλεσμα να γίνει αποκατάσταση κλήσης μεταξύ των δύο κακόβουλων χρηστών, χωρίς να γίνει αντιληπτό από καμία οντότητα. Η επίθεση που περιγράφηκε παραπάνω είναι γνωστή και ως FakeBusy, στις ByeDelay και ByeDrop επιθέσεις υπάρχουν αντιστοίχως δύο επιτιθέμενοι που παρεμποδίζουν την προώθηση των SIP BYE μηνυμάτων στον κατάλληλο πληρεξούσιο εξυπηρετητή και συνεπώς και στον εξουσιοδοτημένο χρήστη. Στέλνουν όμως το μήνυμα επιτυχούς τερματισμού της κλήσης , δίνοντας την εντύπωση τερματισμού κλήσης ενώ ο επιτιθέμενος αξιοποιεί τις αρχικές παραμέτρους επικοινωνίας για την μετάδοση δεδομένων με τον επιτιθέμενο που βρίσκεται στην άλλη πλευρά. Με αποτέλεσμα η χρέωση γίνεται στον εξουσιοδοτημένο χρήστη που αρχικοποίησε την συνομιλία.

Όμοια με την επίθεση επανάληψης στην διαδικασία εγγραφής υπάρχει και η InviteReplay σύμφωνα με την οποία ο επιτιθέμενος έχει υποκλέψει ένα μήνυμα SIP INVITE και το χρησιμοποιεί για την αποκατάσταση συνόδου με κάποιον χρήστη, χρεώνοντας τον λογαριασμό του εξουσιοδοτημένου χρήστη που δημιούργησε το μήνυμα SIP INVITE. (SIP HANDBOOK Services, Technologies and Security of Session Initiation Protocol) (Γενειατάκης, 2008) (D. Geneiatakis)

Request Spoofing

Στην περίπτωση κατά την οποία ένας κακόβουλος χρήστης στείλει ένα μήνυμα υποδυόμενος κάποιον αποστολέα με σκοπό να ξεγελάσει τον παραλήπτη, κάνοντας τον να πιστεύει πως επικοινωνεί με κάποια άλλη οντότητα έχουμε request spoofing. Αυτό επιτυγχάνεται στέλνοντας ένα μήνυμα στο οποίο έχει αλλάξει η κεφαλίδα ή το σώμα του. Υπάρχουν τριών ειδών επιθέσεις αυτής της μορφής σε SIP αιτήσεις, spoofing INVITE message, BYE message και spoofing CANCEL message.

- Spoofing INVITE message

Αποτελεί την πιο κοινή επίθεση spoofing, ο επιτιθέμενος αλλάζει τα πεδία των κεφαλίδων From, Via ή Subject. Για παράδειγμα αν θέλει να στείλει ένα μήνυμα υποδυόμενος την Alice θα αλλάξει την κεφαλίδα From βάζοντας το δικό της URI αλλά στην κεφαλίδα Via θα βάλει την δική του IP διεύθυνση προκειμένου η απάντηση να φτάσει σε αυτόν.

- SIP Spoofing BYE Attack (Call Tear Down Attack)

Ο σκοπός αυτής της επίθεσης είναι να τερματιστεί μια σύνοδος νόμιμων χρηστών. Ο επιτιθέμενος δημιουργεί ένα μήνυμα BYE request και το στέλνει στον τελικό χρήστη ώστε να τερματιστεί η κλήση. Ο επιτιθέμενος προκείμενου να πετύχει την επίθεση πρέπει να έχει την δυνατότητα να διακόψει την κλήση, να έχει στη κατοχή του τις σωστές παραμέτρους για τα πεδία Call-ID, To και From και να γνωρίζει το SIP URI του χρήστη.

- Spoofing CANCEL Request

Σκοπός του επιτιθέμενου σε αυτή την επίθεση είναι η ακύρωση μιας αίτησης που βρίσκεται σε εξέλιξη. Ο επιτιθέμενος στέλνει ένα SIP CANCEL μήνυμα στον πληρεξούσιο εξυπηρετητή προσποιούμενος τον καλούντα και στην συνέχεια το μήνυμα προωθείται στον καλούμενο και ακυρώνεται η αίτηση INVITE.

Επιθέσεις άρνησης υπηρεσιών (DoS attack)

Σε αυτή την κατηγορία επιθέσεων συμπεριλαμβάνονται όλες οι επιθέσεις κατά τις οποίες ο επιτιθέμενος δημιουργεί τόσο μεγάλη κίνηση στο δίκτυο ώστε το σύστημα που αποτελεί τον στόχο να καταναλώνει όλους τους διαθέσιμους πόρους και να καθίσταται μη ικανό να εξυπηρετήσει τους νόμιμους χρήστες. Οι επιθέσεις αυτές είναι γνωστές και ως επιθέσεις πλημμύρας (flooding attack) και σε μια δομή δικτύου όπως αυτή του SIP είναι έυκολα πραγματοποιήσιμες αφού δεν υπάρχει διαχωρισμός στο κανάλι της σηματοδοσίας και της μεταφοράς δεδομένων. Γενικά σε μια επίθεση πλημμύρας ο επιτιθέμενος στέλνει μεγάλο αριθμό αιτημάτων τα οποία όμως είναι συμβατά με τις προδιαγραφές του πρωτοκόλλου που χρησιμοποιείται από το σύστημα στόχο. Αυτό μπορεί να επιτευχθεί με δύο τρόπους, είτε με την χρήση ενός συστήματος παραγωγής μηνυμάτων είτε με την χρήση πολλαπλών τέτοιων συστημάτων τα οποία συντονίζονται από ένα κεντρικό σύστημα. Στην δεύτερη περίπτωση πραγματοποιείται μεγαλύτερη κίνηση και συνήθως τα συστήματα συμμετέχουν στην επίθεση εν αγνοία τους. Τέτοιου είδους επιθέσεις λαμβάνουν χώρα και στις υπηρεσίες διαδικτυακής τηλεφωνίας καθότι οι οντότητες που εμπλέκονται είναι ευπαθείς. Αυτή η ευπάθεια οφείλεται στο γεγονός ότι κάθε χρήστης αυθεντικοποιήμενος ή μη, εσωτερικός ή εξωτερικός είναι σε θέση να δημιουργεί και να αποστείλει αιτήματα προς την κατάλληλη οντότητα.

<u>SIP Register Flooding</u>

Οι SIP συσκευές κατά την εκκίνηση της λειτουργίας τους και πριν ακόμα πραγματοποιήσουν κάποια κλήση πρέπει να στέλνουν αίτηση εγγραφής (REGISTER request) ώστε να εγγραφούν στον SIP registar, παρέχοντας μια ή περισσότερες διευθύνσεις στις οποίες θα είναι διαθέσιμος. Κατά την διαδικασία της εγγραφής, όπως έχει αναφερθεί και παραπάνω, γίνεται χρήση του μηχανισμού

αυθεντικοποίησης HTTP Digest για τον υπολογισμό των απαραίτητων διαπιστευτηρίων. Συνεπώς κατά την εκτέλεση μιας επίθεσης πλημμύρας ο σκοπός του επιτιθέμενου είναι η εύρεση του κωδικού κάποιου χρήστη ή πρόκληση άρνησης παροχής υπηρεσιών του αντίστοιχου εξυπηρετητή εγγραφής (SIP registar). Στην επίθεση πλημμύρας SIP REGISTER, ο επιτιθέμενος στέλνει μεγάλο αριθμό από μηνύματα εγγραφής (SIP REGISTER MESSAGES) στον SIP registar ώστε να εξαντλήσει τους διαθέσιμους πόρους του και να μην είναι πλέον σε θέση να εξυπηρετήσει τις νόμιμες αιτήσεις εγγραφής. Ένα σενάριο ώστε ο επιτιθέμενος να επιτύχει τον σκοπό του είναι στέλνοντας αιτήσεις με διαφορετικά ονόματα χρηστών, δηλαδή ουσιαστικά έχοντας τροποποιήσει παραμέτρους του μηνύματος δημιουργεί διαφορετικά μηνύματα ώστε να αντιμετωπίζονται ως διαφορετικές αιτήσεις και η διαδικασία αυθεντικοποίησης να εκτελείται για το κάθε ένα ξεχωριστά. Με αποτέλεσμα τον υψηλό υπολογιστικό φόρτο. Ένα άλλο σενάριο είναι η αποστολή μεγάλου αριθμού αιτήσεων με ονόματα χρηστών που δεν υπάρχουν ώστε ο SIP registar να ψάχνει στην βάση δεδομένων και να στέλνει “Not Found” μηνύματα τα οποία θα αγνοούνται από τον επιτιθέμενο. Φυσικά το τελευταίο σενάριο μπορεί να υλοποιηθεί για οποιαδήποτε απάντηση του εξυπηρετητή.

Επίθεση πλημμύρας σε Πληρεξούσιο εξυπηρέτη

Οι πληρεξούσιοι εξυπηρετητές είναι υπεύθυνοι για την διαχείριση και επεξεργασία όλων των μηνυμάτων, εκτός των μηνυμάτων εγγραφής. Οι πληρεξούσιοι εξυπηρετητές είναι πιθανοί στόχοι επιθέσεων πλημμύρας τόσο όσοι λειτουργούν σε κατάσταση χωρίς μνήμη όσο και αυτοί που λειτουργούν σε κατάσταση μνήμης και είναι πιο ευπαθείς λόγω της επιπρόσθετης επεξεργαστικής ισχύς που απαιτείται για την διαχείριση των μηνυμάτων. Μια απλή περίπτωση επίθεσης τέτοιου είδους προς έναν πληρεξούσιο εξυπηρετητή είναι η δημιουργία και αποστολή πολύ μεγάλου αριθμού SIP INVITE μηνυμάτων τα οποία αντιστοιχούν σε διαφορετικές συνόδους. Η αποστολή διαφορετικών μηνυμάτων με σκοπό την έναρξη διαφορετικών συνόδων επιτυγχάνεται όταν τα SIP INVITE μηνύματα δημιουργούνται με διαφορετικά αναγνωριστικά κλήσεων (call id) ή διαφορετικά αναγνωριστικά καλούμενων. Για κάθε νέο αίτημα που λαμβάνει ο εξυπηρετητής εκχωρεί τους απαραίτητους πόρους

, οι οποίοι αποδεσμεύονται μόλις ληφθεί η τελική απάντηση του αιτήματος ή τερματιστεί η σύνοδος μετά το πέρας του χρόνου επεξεργασίας που ορίζεται από τις προδιαγραφές του SIP.

Τα πρωτόκολλα TCP και SIP παρουσιάζουν ομοιότητες, συγκεκριμένα κατά την διαδικασία αποκατάστασης συνόδων. Άρα είναι πιθανόν στο SIP να εμφανιστούν επιθέσεις πλημμύρας όμοιες με αυτές του TCP. Για την αποκατάσταση μιας σύνδεσης TCP απαιτείται μια τριμερής διαδικασία χειραψίας (three way handshake).

Στο πρωτόκολλο TCP έχει εντοπισθεί από τους επιτιθέμενους μια ευπάθεια η οποία οδηγεί σε εξάντληση της μνήμης ενός TCP εξυπηρετητή και συνεπώς σε άρνηση παροχής υπηρεσιών. Ο επιτιθέμενος αποστέλλει πολλά SYN μηνύματα τα οποία περιλαμβάνουν πλαστή ταυτότητα αποστολέα. Για κάθε ένα τέτοιο μήνυμα ο εξυπηρετητής δεσμεύει την κατάλληλη μνήμη για την διαχείριση της σύνδεσης και στέλνει ένα SYN/ACK μήνυμα πίσω στον αποστολέα. Όμως οι ταυτότητες των αποστολέων είναι πλαστές οπότε ο εξυπηρετητής διατηρεί δεσμευμένους τους πόρους μέχρι να ολοκληρωθεί η διαδικασία όπως ορίζουν οι προδιαγραφές του TCP. Παρόμοια επίθεση θα μπορούσε να πραγματοποιηθεί και στο SIP εάν ο αποστολέας έστελνε SIP INVITE μηνύματα που περιέχουν πλαστή ταυτότητα αποστολέα. Ο SIP εξυπηρετητής δεσμεύει τους πόρους που χρειάζεται για την διαχείριση των συνόδων και στέλνει την αίτηση στον καλούμενο. Στην περίπτωση που ο καλούμενος μπορεί να δεχτεί την κλήση στέλνει ένα μήνυμα “200 OK” στον πληρεξούσιο εξυπηρετητή. Στην συνέχεια ο τελευταίος θα προσπαθήσει να στείλει αυτήν την απάντηση στον αποστολέα στην περίπτωση αυτή στον επιτιθέμενο, όμως το μήνυμα δεν θα αποστέλλεται λόγω των πλαστών διευθύνσεων. Ο εξυπηρετητής θα διατηρεί την κλήση και θα κάνει συνεχείς προσπάθειες επανεκπομπής της απάντησης μέχρι να τερματιστεί η διαδικασία βάσει των προδιαγραφών του SIP. Συνεπώς ο επιτιθέμενος στέλνοντας μεγάλο αριθμό τέτοιου είδους μηνυμάτων μπορεί να προκαλέσει επίθεση πλημμύρας.

Call Flooding Attack

Υπάρχουν επιθέσεις πλημμύρας που έχουν ως στόχο τον τελικό χρήστη. Σε αυτόν το τύπο επίθεσης ο επιτιθέμενος στέλνει μια σειρά από SIP INVITE αιτήσεις σε μια SIP συσκευή και κλείνει όταν λάβει το Ringing ή το 100 OK μήνυμα από την συσκευή. Σαν αποτέλεσμα, η συσκευή του νόμιμου χρήστη δεν θα είναι σε θέση να πραγματοποιήσει ή να λάβει κλήσεις. Σε άλλη περίπτωση ο επιτιθέμενος λειτουργεί όπως στην επίθεση κατά του πληρεξούσιου εξυπηρετητή με την διαφορά πως ο προορισμός των SIP INVITE μηνυμάτων είναι ο ίδιος (URI) και ο πληρεξούσιος εξυπηρετητής δρα ως φορέας της επίθεσης. Στέλνοντας λοιπόν αριθμό αιτήσεων που υπερβαίνει το όριο των εισερχομένων αιτήσεων που μπορεί να διαχειριστεί η τερματική συσκευή, προκαλείται άρνηση παροχής υπηρεσίας στον τελικό χρήστη αφού δεν θα είναι σε θέση να ανταποκριθεί σε άλλες εισερχόμενες αιτήσεις.

Buffer Overflow Attack

Όπως και σε πολλά προγράμματα έτσι και στο SIP μπορεί κάποιος επιτιθέμενος να εκμεταλλευτεί κάποια αδυναμία στην εκτέλεση του SIP και να εισάγει κακόβουλο κώδικα στο μηχάνημα του θύματος και να κερδίσει τον πλήρη έλεγχο του. Είναι σημαντικό να θυμόμαστε πως το λογισμικό VoIP θα αποκτά και κάθε αδυναμία του λειτουργικού συστήματος στο οποίο τρέχει.

De-registration Attack

Αυτός ο τύπος επίθεσης βασίζεται στην αποστολή Register μηνυμάτων με πεδίο expire να ισούται με μηδέν. Αυτός ο τύπος μηνύματος στέλνεται κανονικά από ένα τηλέφωνο (soft phone) ώστε να υποδηλώσει ότι απενεργοποιείται και συνεπώς να μην του σταλούν άλλες κλήσεις. Ο επιτιθέμενος μπορεί να στείλει μηνύματα εγγραφής (REGISTER request) στα οποία πλαστογραφεί την ταυτότητα κάποιου χρήστη με το πεδίο expire να είναι μηδέν. Ο χρήστης αυτός δεν θα είναι πλέον σε θέση να λάβει κλήσεις αλλά ούτε και να πραγματοποιήσει. (Qiu, 2003)

- Registration Hijacking

Όπως έχει εκτενώς αναλυθεί παραπάνω σύμφωνα με το SIP πρωτόκολλο ο πράκτορας χρήστη (UA) πρέπει να εγγραφεί στον SIP registrar. Η επίθεση Registration Hijacking συμβαίνει όταν ο επιτιθέμενος προσποιείται έναν έγκυρο πράκτορα χρήστη στον SIP registrar και αντικαθιστά την διεύθυνση του νόμιμου χρήστη με την δική του. Το αποτέλεσμα αυτής της επίθεσης είναι οι εισερχόμενες κλήσεις που προορίζονται για τον νόμιμο χρήστη να στέλνονται στον επιτιθέμενο.

- Replay attack

Αποτελεί μια κοινή επίθεση στα συστήματα Πελάτη-Εξυπηρετητή τα οποία χρησιμοποιούν μηνύματα ως μέσο επικοινωνίας. Γνωστά παραδείγματα τέτοιων συστημάτων είναι το HTTP, SMTP και το SIP. Στην πιο απλή μορφή τέτοιου είδους επίθεσης ο επιτιθέμενος κρυφακούει το νόμιμο μήνυμα και το επανεκπέμπει αργότερα. Άρα ο επιτιθέμενος συλλαμβάνει όλα τα μηνύματα που στάλθηκαν σε μια σύνοδο και προσπαθεί να τα στείλει εκ νέου στο ίδιο παραλήπτη προσποιούμενος στον νόμιμο αποστολέα. Σε άλλη περίπτωση που είναι και πιο δύσκολα ανιχνεύσιμη ο επιτιθέμενος συλλέγει ένα μήνυμα που δεν έφτασε ποτέ στον προορισμό του, συνεπώς όταν το στείλει στον παραλήπτη θα το εκλάβει ως έγκυρο και δεν θα ανιχνεύσει πως στάλθηκε από μη εξουσιοδοτημένη οντότητα.

- Social Attacks

Οι κοινωνικές επιθέσεις γνωστές και ως social engineering αποτελούν ένα είδος επιθέσεων που απευθύνονται σε αφελείς χρήστες ή χρήστες που δεν έχουν τις απαραίτητες γνώσεις με σκοπό την συλλογή εμπιστευτικών πληροφοριών. Τέτοιου είδους επιθέσεις συναντάμε συχνά στην ηλεκτρονική αλληλογραφία, ο χρήστης λαμβάνει ένα ηλεκτρονικό μήνυμα στο οποίο του ζητείται να υποβάλλει πληροφορίες όπως κωδικούς αριθμούς PIN τραπεζικών καρτών με το πρόσχημα ότι έχει εντοπιστεί κάποιο πρόβλημα στο τραπεζικό λογαριασμό. Στην περίπτωση του SIP πρωτοκόλλου . Παράδειγμα τέτοιας επίθεσης αποτελεί η περίπτωση όπου ζητείται από τον νόμιμο χρήστη να υποβάλλει τα διαπιστευτήρια του σε μια

ψεύτικη ιστοσελίδα που υποδύεται την επίσημη ιστοσελίδα του παρόχου υπηρεσιών.

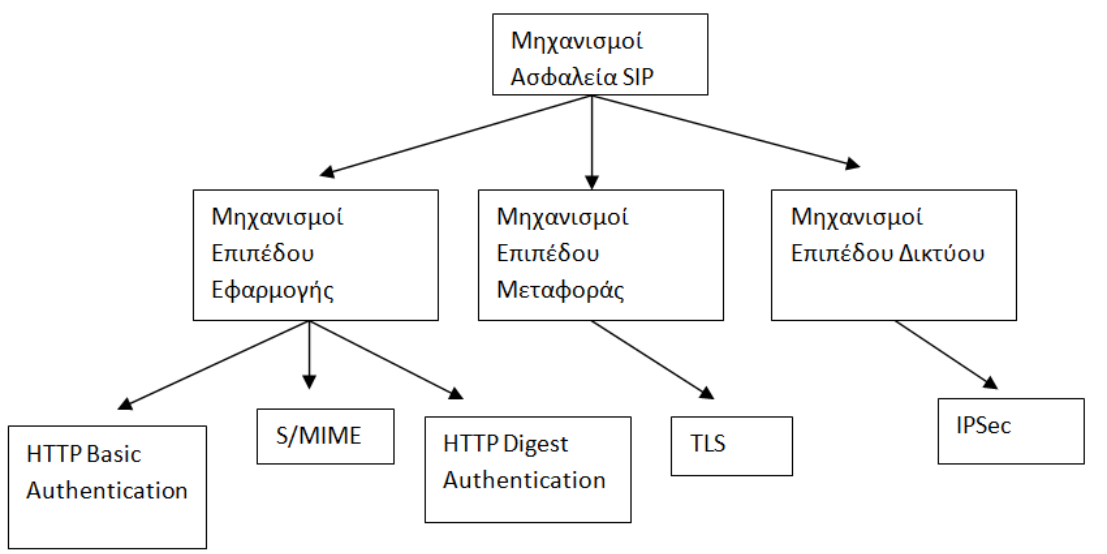
3.4 Απαιτήσεις Ασφάλειας

Από τις απειλές και πιθανές επιθέσεις οι οποίες περιγράφηκαν παραπάνω προκύπτουν οι υπηρεσίες ασφάλειας που απαιτούνται από το SIP πρωτόκολλο. Καταρχήν απαιτείται η διατήρηση της εμπιστευτικότητας και της ακεραιότητας του μηνύματος, η πρόληψη των επιθέσεων επανεκπομπής και την πλαστογράφηση των μηνυμάτων, η παροχή δυνατότητας αυθεντικόποιησης και ιδιωτικότητας των συμμετεχόντων σε μία σύνοδο και πρόληψη επιθέσεων άρνησης παροχής υπηρεσιών. Το SIP πρωτόκολλο προκειμένου να ικανοποιήσει όλες τις παραπάνω απαιτήσει δεν ορίζει καινούργιους μηχανισμούς ασφάλειας αλλά χρησιμοποιεί ήδη υπάρχοντα μοντέλα ασφάλειας που προέρχονται από το HHTP και το SMTP όπου είναι δυνατόν .

Η πλήρης κρυπτογράφηση των μηνυμάτων παρέχει τον πιο αποτελεσματικό τρόπο για την διαφύλαξη της εμπιστευτικότητας της σηματοδοσίας και για την πιστοποίηση ότι τα μηνύματα δεν τροποποιούνται από κακόβουλους ενδιάμεσους. Ωστόσο, οι αιτήσεις και οι αποκρίσεις του SIP δεν μπορούν να είναι κρυπτογραφημένες ολοκληρωτικά από άκρο σε άκρο διότι κάποια πεδία του μηνύματος όπως Request-URI, Route και Via χρειάζεται να είναι ορατά στους πληρεξούσιους εξυπηρετητές ώστε τα SIP να δρομολογηθούν σωστά. Επίσης οι πληρεξούσιοι εξυπηρετητές χρειάζεται να τροποποιούν κάποια χαρακτηριστικά του μηνύματος όπως πεδίο Via ώστε να λειτουργεί σωστά το πρωτόκολλο. Επομένως οι πληρεξούσιοι πρέπει όσο είναι δυνατόν να έχουν σχέση εμπιστοσύνης με τους πράκτορες χρήστη. Για αυτό το σκοπό μηχανισμοί ασφάλειας χαμηλού επιπέδου προτείνονται για το SIP. Οι οντότητες του SIP έχουν επίσης την ανάγκη να ταχτοποιήσουν η μια την άλλη. Όταν ένα τελικό σημείο (endpoint) του SIP υποστηρίζει την ταυτότητα του χρήστη του σε ένα πληρεξούσιο εξυπηρετητή ή σε πράκτορα χρήστη, αυτή η ταυτότητα πρέπει με κάποιο τρόπο να είναι επαληθεύσιμη. Ένας κρυπτογραφικός μηχανισμός αυθεντικοποίησης παρέχεται στο SIP ώστε να ικανοποιείται αυτή η απαίτηση.

3.5 SIP security mechanisms

Το πρωτόκολλο SIP δεν περιέχει συγκεκριμένους μηχανισμούς ασφάλειας, για αυτό προτείνεται η χρήση των γνωστών και αποτελεσματικών μηχανισμών ασφάλειας διαδικτύου. Συγκεκριμένα οι μηχανισμοί ασφάλειας που μπορούν να χρησιμοποιηθούν είναι οι HTTP digest, SIPS, TLS, IP security (IPSec) και Secure MIME (S/MIME) κάθε πρωτόκολλο έχει διαφορετικές δυνατότητες και υλοποίηση σε διαφορετικό επίπεδο . Σε επίπεδο δικτύου υλοποιείται το IPSec, σε επίπεδο μεταφοράς το πρωτόκολλο TLS και σε επίπεδο εφαρμογής το πρωτόκολλο HTTP Digest, το HTTP Basic Authentication και το πρωτόκολλο S/MIME. Ο λόγος που γίνεται χρήση διαφορετικών πρωτοκόλλων σε διαφορετικά επίπεδα είναι επειδή είναι αδύνατο να υπάρξει ένας μηχανισμός που να καλύπτει όλες τις απαιτήσεις ασφάλειας. Αν δεν υπάρξουν άλλες υπηρεσίες κρυπτογράφησης και ασφάλειας από το επίπεδο δικτύου και μεταφοράς το SIP ως πρωτόκολλο επιπέδου εφαρμογής



Εικόνα 10: Επίπεδα μηχανισμών ασφάλειας

παρέχει μόνο την μέθοδο HTTP Digest αυθεντικοποίηση όπως ορίζεται στο RFC 3261. Χρησιμοποιώντας αυτόν τον μηχανισμό ο πράκτορας χρήστη πελάτη μπορεί να αυθεντικοποιηθεί στον πράκτορα χρήστη εξυπηρετητή, στον εξυπηρετητή εγγραφής ή στον πληρεξούσιο εξυπηρετητή. Όμως HTTP Digest παρέχει και mutual αυθεντικοποίηση κατά την οποία ο εξυπηρετητής αυθεντικοποιείται στον πράκτορα χρήστη πελάτη.

3.5.1 HTTP Digest

Η εφαρμοσμένη μέθοδος αυθεντικοποίησης στο SIP είναι βασισμένη στο **HTTP Digest authentication** το οποίο είναι πρωτόκολλο αυθεντικοποίησης βασισμένο στην τεχνική πρόκληση-απάντηση "challenge-response". Για την εφαρμογή του πρωτοκόλλου απαιτείται η προκαθορισμένη εμπιστοσύνη μεταξύ πελάτη και υπηρεσίας για τον διαμοιρασμό των απαραίτητων συνθηματικών και την αποθήκευση τους στον πάροχο της υπηρεσίας. Σε κάθε αίτημα που απαιτείται αυθεντικοποίηση εξελίσσεται η παρακάτω διαδικασία:

- Αρχικά ο χρήστης στέλνει ένα SIP αίτημα για παράδειγμα SIP REGISTER προς τον κατάλληλο πληρεξούσιο.
- Ο πληρεξούσιος απαντά με ένα μήνυμα "401 Unauthorized" όταν απαιτεί αυθεντικοποίηση του μηνύματος. Στο μήνυμα αυτό περιλαμβάνονται και τα δεδομένα τα οποία θα χρησιμοποιήσει ο χρήστης προκειμένου να δημιουργήσει τα διαπιστευτήρια.
- Ο χρήστης λαμβάνοντας αυτό το μήνυμα, δημιουργεί και αποστέλλει νέο αίτημα το οποίο περιλαμβάνει κεφαλίδα "authorization" με τα διαπιστευτήρια τα οποία δημιούργησε βασισμένος στα δεδομένα που συμπεριλαμβάνονταν στην απόκριση του πληρεξούσιου.
- Ο πληρεξούσιος εξυπηρετητής υπολογίζει τα διαπιστευτήρια και εφόσον συμπίπτουν με αυτά που έστειλε ο χρήστης στην κεφαλίδα "authorization" αποστέλλει μήνυμα επιτυχίας "200 OK".

Η αξιοποίηση της προαναφερθείσας μεθόδου μπορεί να εφαρμοστεί για οποιοδήποτε SIP αίτημα, εκτός του SIP CANCEL και SIP ACK όπου όπως ορίζεται από τις προδιαγραφές του SIP, απαιτείται εξειδικευμένος τρόπος διαχείρισης.

Στην απόκριση "401" περιλαμβάνεται ένα πεδίο επικεφαλίδας "WWW-Authenticate" η οποία περιέχει παραμέτρους απαραίτητες για τον υπολογισμό των διαπιστευτηρίων του χρήστη.

WWW-Authenticate: Digest

realm=”unipi.com”

qop=”auth,auth-int”

nonce=”abcd1234567oooppp”

opaque=”67xxxxbbboikoooll”

algorithm=MD5

Η παράμετρος realm περιέχει ένα string το οποίο πρέπει να περιέχει το όνομα του host το οποίο θα εκτελέσει την αυθεντικοποίηση, στην παράμετρο qop (Quality of Protection) καθορίζεται ποιες υπηρεσίες υποστηρίζει ο εξυπηρετητής, οι τιμές μπορεί να είναι “auth” για αυθεντικοποίηση ή “auth-int” για αυθεντικοποίηση με προστασία ακεραιότητας. Nonce είναι μια μοναδική τιμή καθορισμένη από τον εξυπηρετητή και προτείνεται από το RFC 2617 να είναι base64 ή δεκαεξαδικά δεδομένα. Το περιεχόμενο του nonce εξαρτάται από την εφαρμογή, για παράδειγμα είναι πιθανό να φτιαχτεί με κωδικοποιώντας με βάση 64 τις τιμές του time-stamp, το Etag* και ένα ιδιωτικό κλειδί. Όπου το time-stamp είναι η ώρα που παράγεται από τον διακομιστή, Etag είναι μια τιμή της κεφαλίδας HTTP Etag η οποία συσχετίχεται με την οντότητα που έκανε την αίτηση και το ιδιωτικό κλειδί είναι ένα δεδομένο που το γνωρίζει μόνο ο διακομιστής. Η εισαγωγή του Etag προλαμβάνει επαναληπτικές αιτήσεις για μια ανανεωμένη έκδοση του πόρου. Στο πεδίο opaque περιέχεται ένα string δεδομένων, καθορισμένο από τον διακομιστή και το οποίο πρέπει να επιστραφεί από τον πελάτη αμετάβλητο στην κεφαλίδα Authorization σε επακόλουθη αίτηση. Στην παράμετρο Algorithm δηλώνεται ο αλγόριθμος που χρησιμοποιείται για τον υπολογισμό του checksum, η default τιμή δηλαδή ο προκαθορισμένος αλγόριθμος είναι MD5.

*Etag ή entity tag είναι ένα αναγνωριστικό το οποίο χρησιμοποιείται προαιρετικά από το HTTP πρωτόκολλο. Ανατίθεται από τον web server σε μια συγκεκριμένη έκδοση ενός πόρου που βρίσκεται σε ένα URL. Όταν ένα URL ανακτηθεί ο web

server θα επιστρέψει τον πόρο μαζί με την αντίστοιχη ETag τιμή στο πεδίο HTTP ETag. Ο πελάτης (client) έχει την δυνατότητα να αποφασίσει εάν θα αποθηκεύσει το πόρο μαζί με το Etag, έτσι ώστε αν αργότερα ο πελάτης θελήσει να ανακτήσει το ίδιο URL, να στείλει το προηγούμενο αποθηκευμένο Etag. Σε τέτοια πιθανή αίτηση ο διακομιστής συγκρίνει το Etag του πελάτη με το Etag της έκδοσης που έχει εκείνη την χρονική στιγμή ο πόρος.

ETag: “687595893a092271e”.

Μετά την λήψη της πρόκλησης “401” μήνυμα από τον εξυπηρετητή, ο πελάτης ξαναστέλνει αίτηση με τα διαπιστευτήρια συμπεριλαμβάνοντας το πεδίο κεφαλίδας Authorization.

Authorization: Digest username=”anna”

realm=”unipi.com”

nonce= “abcd1234567oooppp”

qop=auth

nc=00000001

cnonce=”0a4f113b”

response=”klka787689001881733annhfieu”

opaque=”67xxxxbbboikoooll”

Οι παράμετροι realm, nonce, qop, algorithm και opaque δίνουν τις ίδιες πληροφορίες ακριβώς με τι παραμέτρους στην κεφαλίδα Authentication του εξυπηρετητή. Το username δηλώνει το όνομα του χρήστη στο συγκεκριμένο realm, η παράμετρος nc φανερώνει το αριθμό των αιτήσεων τις οποίες ο πελάτης έστειλε με την ίδια nonce τιμή και καθορίζεται μόνο στην περίπτωση που έχει σταλθεί από τον διακομιστή το qop στο πεδίο της κεφαλίδας WWW-Authenticate . Το Cnonce πρέπει να ορίζεται εάν στο πεδίο qop υπάρχει κάποια κατεύθυνση, διαφορετικά

δεν συμπληρώνεται από τον πελάτη. Η τιμή είναι ένα string που παρέχεται από τον πελάτη και χρησιμοποιείται από τον ίδιο και από τον διακομιστή ώστε να αποφύγουν κάποιες επιθέσεις εξαιτίας μη κρυπτογράφησης, επίσης για την υλοποίηση αμφίδρομης αυθεντικοποίησης και για να παρέχουν διασφάλιση ακεραιότητας στα μηνύματα.

Τέλος το response αποτελείται από ένα αλφαριθμητικό 32 δεκαεξαδικών ψηφίων του υπολογισμένου checksum.

Response = MD5(HA1:nonce:HA2) εάν η τιμή qop είναι “auth” ή “auth-int” τότε Response = MD5(HA1:nonce:nonce: cnonce:qop:HA2)

HA1 = MD5(username:realm:password)

HA2 = MD5(method:digestURI)

(RFC 2617)

Με την αυθεντικοποιήση του πελάτη επιτυγχάνεται η επιβεβαίωση πως ο χρήστης είναι ο νόμιμος χρήστης όταν εγκαθιστά μια σύνδεση με έναν απομακρυσμένο εξυπηρετητή. Με τη μέθοδο αυθεντικοποίησης υπάρχει η δυνατότητα προστασίας από επιθέσεις όπως, επίθεση επανεκπομπής, ψευδείς αιτήσεις και registration hijacking. Το πρωτόκολλο SIP ορίζει μια τιμή value ώστε να αυθεντικοποιηθεί ο πελάτης στον εξυπηρετητή. Η “nonce” τιμή εξαρτάται από την υλοποίηση. Μια προτεινόμενη υλοποίηση πέραν αυτής που αναφέρθηκε παραπάνω είναι η δημιουργία “nonce” τιμής από την σύνοψη τουλάχιστον δύο τιμών της IP διεύθυνσης και του χρόνου. Αυτή η υλοποίηση κάνει δύσκολη την επίθεση επανεκπομπής αφού ο επιτιθέμενος για να επιτύχει πρέπει να γνωρίζει την IP διεύθυνση την οποία περιμένει ο εξυπηρετητής και μέσα στα χρονικά περιθώρια μέχρι την λήξη του χρόνου μέσα στο οποίο έχει υπολογιστεί η τιμή “nonce”. Συνεπώς υπάρχει ένα χρονικό περιθώριο μέσα στο οποίο μπορεί να επιτευχθεί επίθεση επανεκπομπής άρα για να ένα σύστημα το οποίο δεν είναι ευπαθές σε τέτοιες επιθέσεις πρέπει να δημιουργείται μια τιμή “nonce” η οποία απαγορεύεται

να έχει δεύτερη χρήση. Στην πράξη μια τιμή “nonce” επιτρέπεται να ξαναχρησιμοποιηθεί σε μια περιορισμένη χρονική περίοδο.

3.5.2 IPSec

Όπως είναι γνωστό και έχει αναφερθεί και σε προηγούμενο κεφάλαιο το πρωτόκολλο IP το οποίο χρησιμοποιείται για την μεταφορά των SIP μηνυμάτων είναι ευπαθές σε επιθέσεις όπως Spoofing, Session Hijacking, ανάλυση κίνησης κτλ. Το **IPsec** δημιουργήθηκε για την αντιμετώπιση των προβλημάτων αυτών αλλά και για να παρέχει επιπλέον υπηρεσίες ασφάλειας. Το IPsec περιλαμβάνει τρεις τομείς λειτουργίας πιστοποίηση αυθεντικότητας, διαχείριση κλειδιών και εμπιστευτικότητα στα δεδομένα που μεταφέρονται. Η πιστοποίηση αυθεντικότητας χρησιμοποιεί τον κωδικό μηνυμάτων HMAC. Η πιστοποίηση μπορεί να εφαρμοστεί είτε σε ολόκληρο το αρχικό πακέτο (tunnel mode) είτε σε ολόκληρο το πακέτο εκτός της κεφαλίδας IP (transport mode). Η εξασφάλιση του απορρήτου παρέχεται μέσω μιας μορφής κρυπτογράφησης που ονομάζεται ενθυλάκωση φορτίου ασφάλειας (Encapsulation Security Payload, ESP) παρέχει υπηρεσίας εξασφάλισης της εμπιστευτικότητας, όπως εξασφάλιση απορρήτου για τα περιεχόμενα του μηνύματος καθώς και εξασφάλιση περιορισμένης ροής κυκλοφορίας. Εναλλακτικά μπορεί να χρησιμοποιηθεί και ένα άλλο πρωτόκολλο για την παροχή ασφάλειας η κεφαλίδα πιστοποίησης AH, το οποίο παρέχει έλεγχο πρόσβασης, ασυνδεσμική ακεραιότητα, πιστοποίηση δεδομένων και απόρριψη επαναλαμβανόμενων πακέτων. Ενώ το ESP επιπλέον με όλα τα παραπάνω προσφέρει εμπιστευτικότητα και περιορισμένη εμπιστευτικότητα ροής. Το τμήμα διαχείρισης κλειδιών του IPSec περιλαμβάνει τον προσδιορισμό και την διανομή μυστικών κλειδιών. Μια τυπική απαίτηση είναι τα τέσσερα κλειδιά που χρειάζονται για την επικοινωνία μεταξύ δύο εφαρμογών, ένα ζευγάρι κλειδιών για την μετάδοση και λήψη για τους δύο μηχανισμούς AH και ESP. Το προεπιλεγμένο πρωτόκολλο αυτόματης διαχείρισης κλειδιών για το IPSec είναι το ISAKMP/Oakley.

Σε επίπεδο δικτύου ο μηχανισμός ασφάλειας που χρησιμοποιείται από το SIP είναι το IPSec. Χρησιμοποιώντας το IPsec στην VoIP τηλεφωνία διαφυλάσσεται η σηματοδοσία και τα δεδομένα από τις ευπάθειες του διαδικτύου. Η προϋπόθεση

είναι πως πριν την επικοινωνία έχουν δημιουργηθεί δεσμοί αμοιβαίας εμπιστοσύνης για τον διαμοιρασμό των απαιτούμενων κλειδιών, πιστοποιητικών κτλ.

3.5.3 TLS

Για την προστασία της SIP επικοινωνίας σε επίπεδο μεταφοράς μια λύση είναι η χρήση του πρωτοκόλλου **TLS**. Η αυθεντικοποίηση με την χρήση του συγκεκριμένου πρωτοκόλλου είναι δυνατό να είναι αμφίδρομη μεταξύ των οντοτήτων και πραγματοποιείται ανταλλάσοντας τα πιστοποιητικά τους. Το TLS πρωτόκολλο έχει τα περισσότερα από τα πλεονεκτημάτα του IPsec και είναι αποδεδειγμένη η χρησιμότητα και η αποτελεσματικότητα του από την αρχή χρήσης του στο ενσύρματο ιντερνετ. Επιπλέον με την χρήση του TLS δεν προ-απαιτούνται δεσμοί αμοιβαίας εμπιστοσύνης μεταξύ των επικοινωνούντων οντοτήτων. Τρέχει πάνω από TCP/IP και κάτω από πρωτόκολλα υψηλότερου επιπέδου όπως HTTP ή FTP, συνεπώς η κεφαλίδα TCP δεν κρυπτογραφείται. Όμως η χρήση TLS απαιτεί την χρήση αποκλειστικά του TCP ως πρωτοκόλλου μεταφοράς διότι δεν τρέχει πάνω από το UDP. Ένα μειονέκτημα που παρουσιάζει το TLS σχετικά με την χρήση του συνδυαστικά με το SIP, είναι πως είναι δύσκολο για τους proxy να διατηρούν ταυτόχρονα πολλές TCP συνδέσεις. Στα πλαίσια του SIP, το TLS χρησιμοποιείται για την υποστήριξη του SIP Secure-SIPS (ασφαλές SIP) που ουσιαστικά διασφαλίζει την εφαρμογή του από άκρο σε άκρο (end-to-end) του μονοπατιού σηματοδοσίας.

3.5.4 S/MIME

Το S/MIME (Secure/Multipurpose Internet Mail Extension, Ασφαλείς/γενικές επεκτάσεις ταχυδρομείου Διαδικτύου) είναι μια βελτιωμένη έκδοση ως προς την ασφάλεια για το πρότυπο μορφοποίησης των μηνυμάτων ηλεκτρονικού ταχυδρομείου MIME, το οποίο βασίζεται στην τεχνολογία από την RSA Data Security. Θεωρείται ένας από τους πιο ολοκληρωμένους μηχανισμούς ασφάλειας σε

επίπεδο εφαρμογής, υποστηρίζοντας εμπιστευτικότητα μέσω κρυπτογράφησης των περιεχομένων των μηνυμάτων, αυθεντικότητα και ακεραιότητα μέσω ψηφιακής υπογραφής και κρυπτογράφησης του αποτελέσματος με ιδιωτικό κλειδί και μη αποποίηση του αποστολέα.

Στην περίπτωση του SIP η κρυπτογράφηση ολόκληρου του SIP μηνύματος από άκρο σε άκρο για τον σκοπό της εμπιστευτικότητας δεν είναι η κατάλληλη προσέγγιση γιατί στο δίκτυο μεσολαβούν εξυπηρετητές όπως οι proxy οι οποίοι είναι απαραίτητο να βλέπουν συγκεκριμένες κεφαλίδες ώστε να δρομολογηθεί το μήνυμα σωστά, εάν οι ενδιάμεσοι εξυπηρετητές αποκλείονται από τους συσχετισμούς ασφάλειας (security associations), τότε τα SIP μηνύματα δεν θα δρομολογηθούν.

Ωστόσο, το S/MIME επιτρέπει τους πράκτορες χρήστη του SIP να κρυπτογραφούν τα MIME κύρια μέρη του μηνύματος εντός SIP, διασφαλίζοντας αυτά τα κύρια μέρη από άκρο σε άκρο χωρίς να επηρεάζονται οι κεφαλίδες του μηνύματος. Είναι επίσης πιθανή η χρήση του S/MIME ώστε να παρέχει μια φόρμα ακεραιότητας και εμπιστευτικότητας για τις SIP κεφαλίδες μέσω SIP μηνυμάτων σήραγγας. Σε αυτή την περίπτωση το S/MIME ενθυλακώνει ολόκληρο το SIP μήνυμα εντός του κυρίου σώματος του MIME και εφαρμόζει την Ασφάλεια MIME σε αυτό το κύριο σώμα με τον ίδιο τρόπο όπως ένα τυπικό κύριο σώμα SIP. Αυτές οι ενθυλακωμένες SIP αιτήσεις και απαντήσεις δεν αποτελούν ξεχωριστό διάλογο ή δοσοληψία, είναι ένα αντίγραφο του εξωτερικού μηνύματος το οποίο χρησιμοποιείται ώστε να επικυρωθεί η ακεραιότητα ή να υποστηρίξει επιπλέον πληροφορία. Όσο αφορά στην εμπιστευτικότητα όταν τα μηνύματα κρυπτογραφούνται, τα πεδία των κεφαλίδων μπορεί να εμπεριέχονται στο κρυπτογραφημένο κύριο μέρος και να μην υφίστανται στο εξωτερικό μήνυμα. Κάποια πεδία καφαλίδων πρέπει να είναι πάντοτε μη κρυπτογραφημένα (plaintext) επειδή είναι τα απαραίτητα πεδία στις αιτήσεις και αποκρίσεις. Αυτά τα πεδία είναι τα (To, From, Call-ID, Cseq, Contact). Εάν το πεδίο From έχει διαφορετική τιμή στο κρυπτογραφημένο κύριο μέρος του μηνύματος και στο εξωτερικό μήνυμα, η τιμή εντός της κρυπτογράφησης εμφανίζεται στον χρήστη, αλλά δεν χρησιμοποιείται σε εξωτερικά πεδία κεφαλίδας

σε μελλοντικά μηνύματα. Το κύριο μέρος των MIME μηνυμάτων επισυνάπτεται στο εσωτερικό μήνυμα και κρυπτογραφούνται πεδία κεφαλίδων του MIME όπως το MIME-Version, Content-type, Content-Length, Content-Language, Content-Encoding και Content-Disposition. Στο εξωτερικό μήνυμα υπάρχουν τα κατάλληλα πεδία κεφαλίδας του MIME για το σώμα του S/MIME. Δεν είναι πρακτικό να γίνει κρυπτογράφηση των ακόλουθων κεφαλίδων, Min-Expires, Timestamp, Authorization, Priority και WWW-Authenticate. Κάποιες από αυτές τις κεφαλίδες είναι πιθανό να αλλάξουν από τους proxy εξυπηρετητές. (RFC 3261)

3.5 Σύγκριση μηχανισμών Ασφάλειας στο SIP

Το HTTP Digest παρέχει μονόδρομη αυθεντικοποίηση και προστασία από επιθέσεις επανεκπομπής αλλά δεν υποστηρίζει μηχανισμό για την εξασφάλιση της ακεραιότητας και της εμπιστευτικότητας. Είναι ευπαθές σε επιθέσεις τύπου αποκρυπτογράφησης με γνωστό κείμενο, λόγω του ότι τα δεδομένα που χρησιμοποιούνται για τον υπολογισμό των διαπιστευτηρίων και τα διαπιστευτήρια μπορεί να υποκλαπούν από τον επιτιθέμενο, καθώς μεταδίδονται με την υποβολή του νέου αυθεντικοποιημένου μηνύματος. Παρά το γεγονός πως για την λειτουργία του HTTP digest απαιτείται η αμοιβαία εμπιστοσύνη μεταξύ υπηρεσίας και πελάτη για τον διαμοιρασμό και την αποθήκευση των συνθηματικών ακόμα και εάν αυτή γίνει κρυπτογραφημένα δεν προσφέρεται επιπρόσθετο επίπεδο ασφάλειας λόγω του τρόπου υπολογισμού των διαπιστευτηρίων. Το IPSec παρέχει υπηρεσίες αυθεντικοποίησης όπως και το HTTP Digest επιπλέον προσφέρει και υπηρεσίες ακεραιότητας και εμπιστευτικότητας δεδομένων από κόμβο σε κόμβο όμως απαιτεί όπως και το HTTP Digest την ύπαρξη προ-εγκατεστημένων δεσμών αμοιβαίας εμπιστοσύνης μεταξύ των μερών που επικοινωνούν. Το κύριο μειονέκτημα στην εφαρμογή του IPSec έγκειται στο γεγονός πως υλοποιείται σε επίπεδο λειτουργικού συστήματος με αποτέλεσμα οι τερματικές συσκευές των χρηστών να μην το υποστηρίζουν. Το TLS παρέχει αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα των δεδομένων χωρίς να απαιτείται προ-εγκατεστημένη σχέση εμπιστοσύνης μεταξύ των οντοτήτων. Για παράδειγμα είναι κατάλληλο σε περιπτώσεις όπως η

παρακάτω : Ο χρήστης Α εμπιστεύεται τον τοπικό πληρεξούσιο διακομιστή, ο οποίος εμπιστεύεται τον διακομιστή τον οποίο εμπιστεύεται ο χρήστης Β ύστερα από ανταλλαγή πιστοποιητικών. Άρα ο Α και ο Β μπορούν να επικοινωνήσουν με ασφάλεια. Το συγκεκριμένο πρωτόκολλο έχει και το πλεονέκτημα της από άκρο σε άκρο (end-to-end) παροχής υπηρεσιών ασφάλειας υπό συγκεκριμένες προϋποθέσεις (SIP Secure- SIPS). Όσο αφορά στα μειονεκτήματα, όπως αναφέρθηκε το TLS δεν υποστηρίζει ασυνδεσμικά πρωτόκολλα όπως το UDP, στο οποίο βασίζεται κατά κύριο λόγο η μεταφορά δεδομένων στη διαδικτυακή τηλεφωνία. Επιπλέον οι συνδέσεις που δημιουργεί προκαλούν αυξημένο υπολογιστικό φόρτο καθώς και επιπρόσθετη καθυστέρηση στην επεξεργασία των δεδομένων σηματοδοσίας. Όσο αφορά στο πρωτόκολλο S/MIME παρόλο που είναι το μόνο που μπορεί να παρέχει εμπιστευτικότητα και ακεραιότητα που μπορεί να εφαρμοστεί από άκρο σε άκρο, είναι ανέφικτη η αξιοποίηση του σε όλα τα δεδομένα ενός μηνύματος SIP. Ο λόγος είναι πως οι πληρεξούσιοι εξυπηρετητές απαιτείται να έχουν πρόσβαση με δικαιώματα τροποποίησης σε συγκεκριμένες κεφαλίδες ώστε να διαχειριστούν σωστά τα εισερχόμενα μηνύματα. Συνεπώς σε αυτές οι κεφαλίδες δεν είναι εφικτό να εφαρμοστούν υπηρεσίες ακεραιότητας και κεφαλίδες οι οποίες εξυπηρετούν στην δρομολόγηση του μηνύματος δεν μπορούν να καλύπτονται από τις υπηρεσίες εμπιστευτικότητας. Για παράδειγμα για την σωστή δρομολόγηση των SIP μηνυμάτων, οι κεφαλίδες οι οποίες τροποποιούνται είναι οι Request URI, Via, Record Route και Record και οι κεφαλίδες πρέπει να διαβαστούν από τους διακομιστές είναι οι From, To και Call Id. Επιπρόσθετα η ενσωμάτωση των MIME μηνυμάτων στο κύριο μέρος των SIP μηνυμάτων εισάγουν δικτυακή επιβάρυνση.

Κεφάλαιο 4 Υλοποίηση

4.1 Εισαγωγή

Αυτό το κεφάλαιο έχει σκοπό την παρουσίαση της μεθοδολογίας της υλοποίησης της παρούσας διπλωματικής. Η υλοποίηση αφορά την χρήση δύο διαφορετικών κρυπτογραφικών αλγορίθμων, με σκοπό την απόκρυψη του ονόματος χρήστη στα μηνύματα εγγραφής που αποστέλλονται στο δίκτυο στον αρμόδιο εξυπηρετητή. Σε κάθε περίπτωση αρχικά περιγράφεται αναλυτικά ο αλγόριθμος που χρησιμοποιείται και έπειτα περιγράφεται η εφαρμογή του στην συγκεκριμένη περίπτωση. Στην συνέχεια του κεφαλαίου γίνεται αναφορά στα Web Services τα οποία χρησιμοποιήθηκαν με σκοπό την πρόσβαση στην Βάση Δεδομένων από την πλευρά του Server. Η τελευταία ενότητα του κεφαλαίου περιέχει την σύγκριση μεταξύ των δύο προτεινόμενων προσεγγίσεων.

4.2 Περιγραφή του Αλγορίθμου AES

Ο κρυπτογραφικός αλγόριθμος AES δημιουργήθηκε ύστερα από πρόσκληση που εξέδωσε ο NIST το 1997 με σκοπό να αντικατασταθεί ο 3DES. Οι προδιαγραφές που θα πρέπει να πληρούσε ο αλγόριθμος ήταν ίση ή μεγαλύτερη απόδοση από τον 3DES με σημαντικά βελτιωμένη απόδοση. Επιπλέον απαίτηση ήταν ο αλγόριθμος να είναι συμμετρικός με μέγεθος τμήματος 128 bit και υποστήριξη για μεγέθη κλειδιών 128, 192 και 256 bit. Τα κριτήρια αξιολόγησης περιελάμβαναν την ασφάλεια, την υπολογιστική αποδοτικότητα, τις απαιτήσεις μνήμης, την καταλληλότητα του υλικού και λογισμικού και την ευελιξία.

Ο κρυπτογραφικός αλγόριθμος AES είναι βασισμένος στην αρχή γνωστή ως substitution-permutation network σύμφωνα με την οποία για να παραχθεί το κρυπτογράφημα, εφαρμόζονται αρκετοί εναλλακτικοί γύροι από αντικαταστάσεις (substitution boxes S-boxes) και μεταθέσεις (permutation boxes P-boxes) σε ένα τμήμα του αρχικού μηνύματος και του κλειδιού. Ο AES είναι γρήγορος και στο λογισμικό και στο υλισμικό και σε αντίθεση με τον προκάτοχο του τον DES δεν χρησιμοποιεί την δομή Feistel.

Ο AES χρησιμοποιεί μέγεθος τμήματος 128 bit και μήκος κλειδιού που μπορεί να είναι 128, 192 ή 256 bit. Το κλειδί που δίνεται ως είσοδος επεκτείνεται σε έναν πίνακα από σαράντα τέσσερις λέξεις των 32 bit. Τέσσερις διαφορετικές λέξεις (128 bit) χρησιμοποιούνται ως κλειδί γύρου για κάθε γύρο.

Χρησιμοποιούνται τέσσερα διαφορετικά στάδια, ένα στάδιο μετάθεσης και τρία στάδια αντικατάστασης:

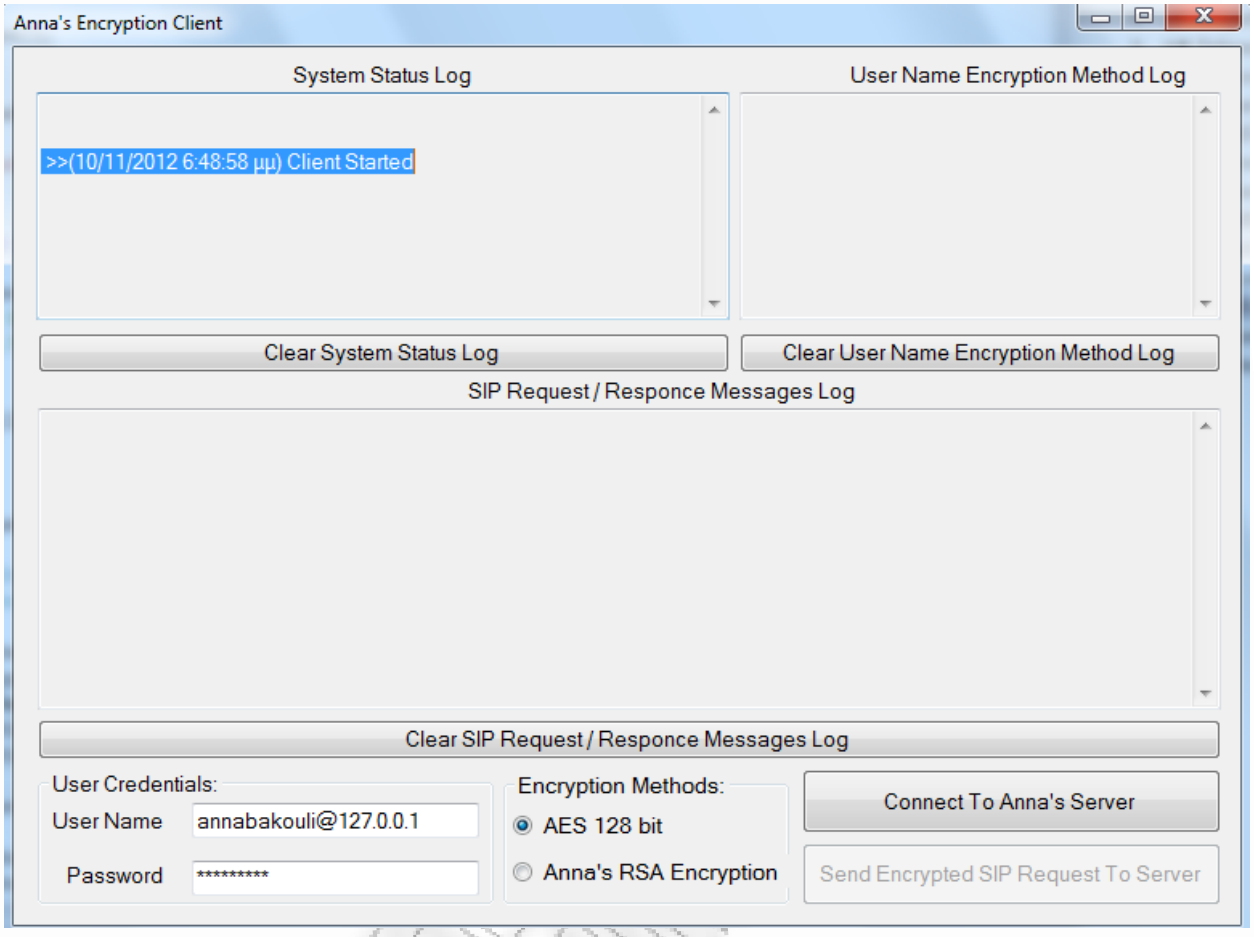
- Αντικατάσταση byte (substitute bytes): Χρησιμοποιείται ένας πίνακας (S-box) ώστε να εκτελείται μια byte προς byte αντικατάσταση του τμήματος.
- Μετατόπιση γραμμών (shift rows): Μια απλή μετάθεση που εκτελείται γραμμή προς γραμμή.
- Ανάμιξη στηλών (mix columns): Μια αντικατάσταση η οποία εναλλάσσει κάθε byte της στήλης ως συνάρτηση όλων των byte της στήλης.
- Προσθήκη κλειδιού γύρου (add round key): Μια απλή πράξη XOR bit προς bit του τρέχοντος τμήματος με ένα κομμάτι του επεκταμένου κλειδιού.

Η δομή είναι αρκετά απλή. Για την κρυπτογράφηση αλλά και για την αποκρυπτογράφηση το κρυπτογραφικό σύστημα ξεκινά από το στάδιο προσθήκης του κλειδιού γύρου, ακολουθούμενο από εννέα άλλους γύρους καθένας από τους οποίους περιέχει και τα τέσσερα στάδια και τέλος ακολουθεί ένας δέκατος γύρος τριών σταδίων. Μόνο το στάδιο προσθήκης κλειδιού χρησιμοποιεί το κλειδί. Για το σκοπό αυτό η κρυπτογράφηση ξεκινά και τελειώνει με ένα τέτοιο στάδιο. Το στάδιο προσθήκης κλειδιού γύρου δεν θα είχε σημασία από μόνο του. Τα υπόλοιπα τρία στάδια τροποποιούν τα bit, αλλά μόνα τους δεν θα παρείχαν καμία ασφάλεια επειδή δεν χρησιμοποιούν το κλειδί. Το σύστημα μπορεί να θεωρηθεί ως εναλλασσόμενες λειτουργίες κρυπτογράφησης ενός τμήματος με το τελεστή XOR (φάση προσθήκης του κλειδιού γύρου, ακολουθούμενες από μια τροποποίηση του τμήματος (οι άλλες τρεις φάσεις), ακολουθούμενες από μια κρυπτογράφηση με τον τελεστή XOR, κ.ο.κ. Αυτή η δομή είναι και αποδοτική και ιδιαίτερα ασφαλής. Κάθε στάδιο είναι εύκολα αντιστρέψιμο. Για τα στάδια αντικατάστασης των byte, μετατόπισης των γραμμών και αναδιάταξης των στηλών χρησιμοποιείται μια αντίστροφη συνάρτηση στον αλγόριθμο αποκρυπτογράφησης. Για την φάση

προσθήκης του κλειδιού γύρου η αντιστροφή επιτυγχάνεται με εφαρμογή του τελεστή XOR μεταξύ του ίδιου κλειδιού γύρου και του τμήματος, με χρήση της σχέσης A XOR A XOR B = B. Όπως συμβαίνει με τα περισσότερα συστήματα κρυπτογράφησης, ο αλγόριθμος αποκρυπτογράφησης χρησιμοποιεί το επεκταμένο κλειδί με αναστραμμένη σειρά. Ωστόσο ο αλγόριθμος αποκρυτπογράφησης δεν είναι ακριβώς ίδιος με αυτόν της αποκρυπτογράφησης. Αυτό αποτελεί συνέπεια της συγκεκριμένης δομής του αλγόριθμου AES. Ο τελικός γύρος της κρυπτογράφησης και της αποκρυπτογράφησης αποτελείται μόνο από τρία στάδια. Και πάλι, αυτό αποτελεί συνέπεια της συγκεκριμένης δομής του αλγορίθμου AES και απαιτείται έτσι ώστε να είναι το σύστημα αντιστρέψιμο.

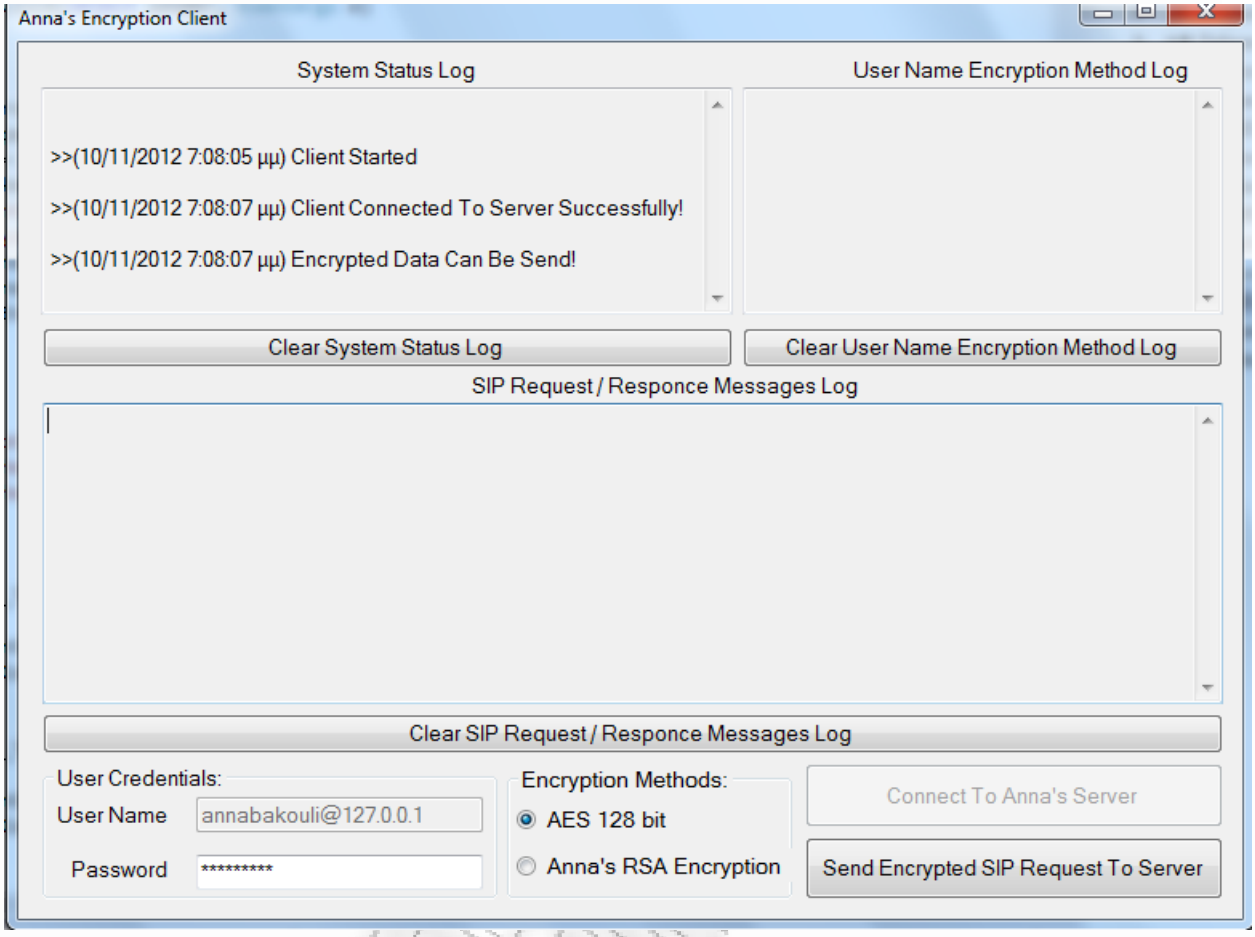
4.2.1 Κρυπτογράφηση username με χρήση AES

Στην παρούσα διπλωματική ο AES χρησιμοποιήθηκε για την κρυπτογράφηση του username του χρήστη (client) που επιθυμεί να κάνει εγγραφή (registration) στο δίκτυο. Πιο αναλυτικά, δημιουργήθηκε μια φόρμα μέσα από την οποία ο χρήστης συνδέεται στον server και αφού επιλέξει με ποιόν κρυπτογραφικό αλγόριθμο επιθυμεί να κρυπτογραφηθεί το username του, στέλνει το μήνυμα στον server. Από την ίδια φόρμα επίσης γίνεται και η απεικόνιση των μηνυμάτων που στέλνονται από και προς τον χρήστη. Παρακάτω περιγράφεται η συνολική λειτουργία του λογισμικού στην περίπτωση επιλογής του κρυπτογραφικού αλγόριθμου AES.



Εικόνα 11 Φόρμα Client

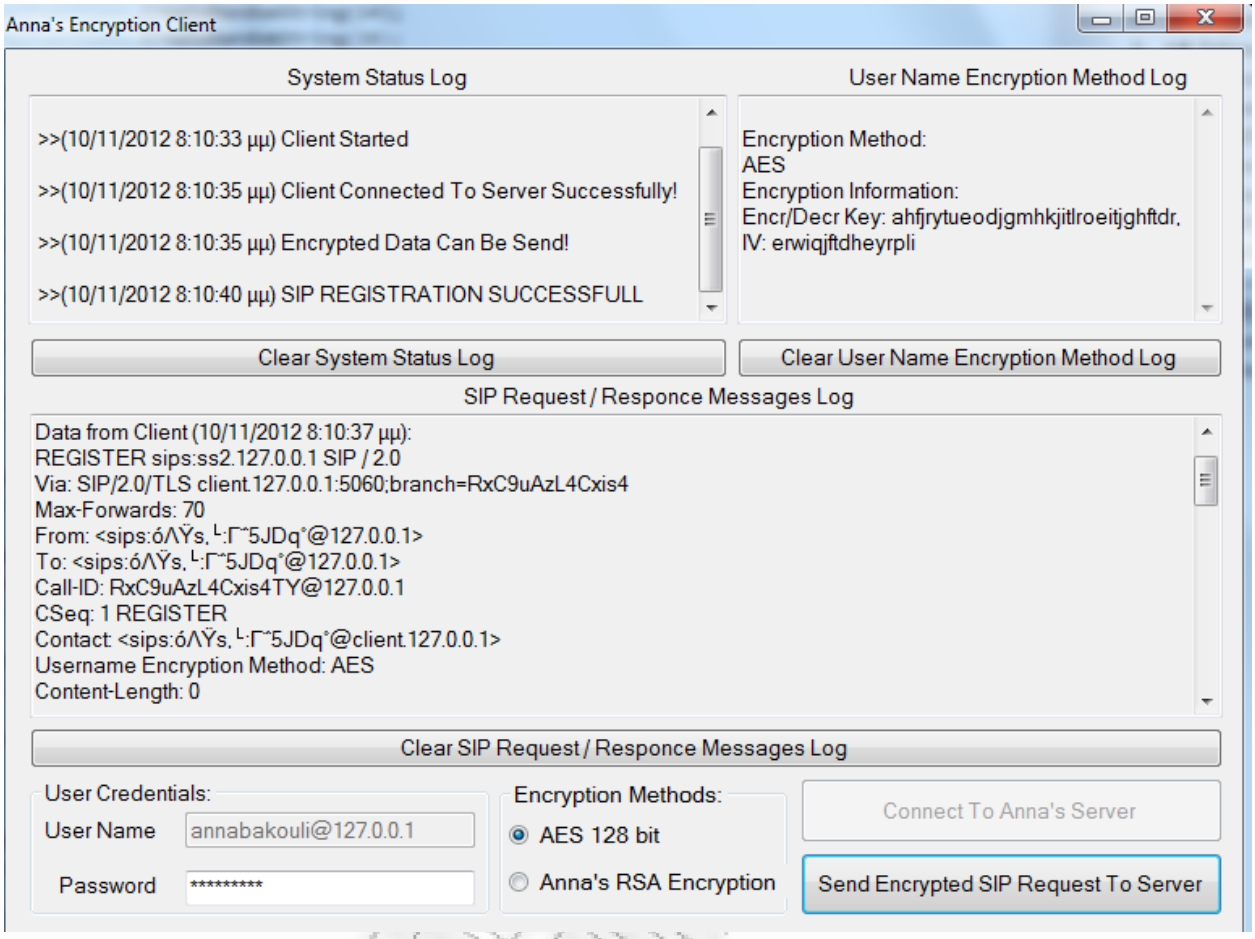
Αφού συμπληρώσει ο χρήστης το username και το password πρέπει να επιλέξει το "Connect to Anna's Server" ώστε να συνδεθεί με τον Server και να μπορέσει να στείλει SIP μηνύματα.



Εικόνα 12 Φόρμα σύνδεση με Server

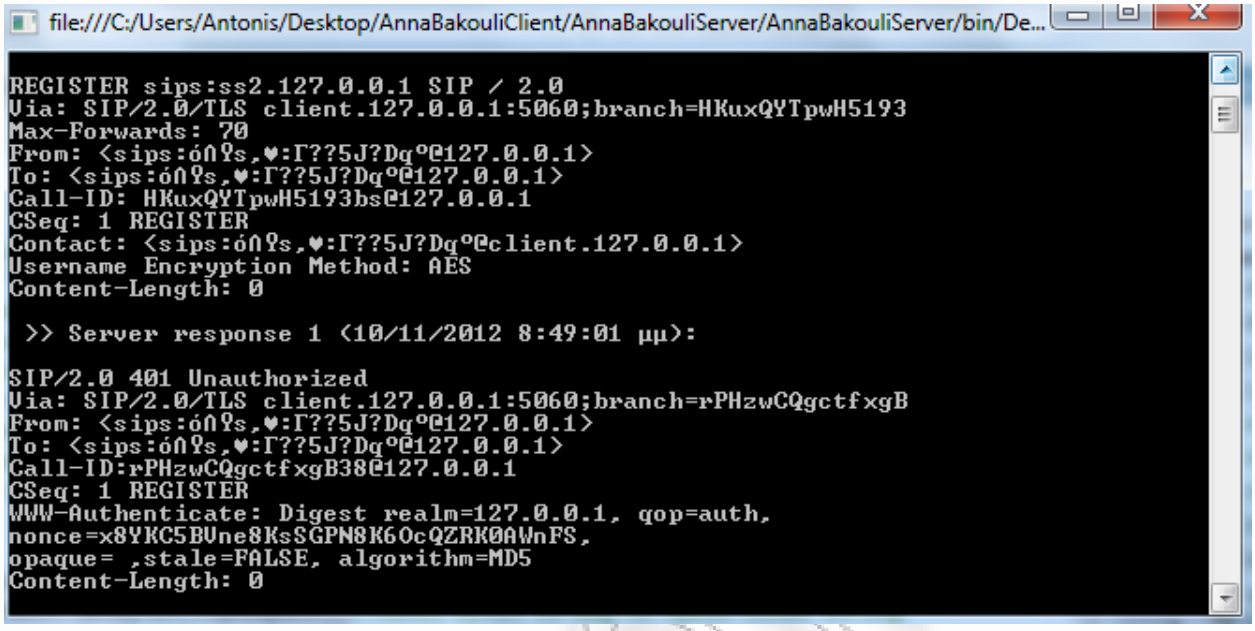
Αμέσως μετά την επιτυχημένη σύνδεση με τον Server ο χρήστης θα επιλέξει να στείλει SIP request μήνυμα για την εγγραφή του στον Server .

Στην περίπτωση που μέθοδος κρυπτογράφησης είναι ο AES τότε θα χρησιμοποιηθεί για την κρυπτογράφηση ένα κλειδί προκαθορισμένο και διαμοιρασμένο μεταξύ client και server και θα πρέπει να δημιουργηθεί τυχαία ένας IV. Αφού δημιουργηθούν τα παραπάνω από την πλευρά του client τότε θα σταλεί το πρώτο SIP μήνυμα για την αίτηση εγγραφής. Στην παρακάτω εικόνα φαίνεται το μήνυμα του client καθώς επίσης και πληροφορίες σχετικές με τον αλγόριθμο που χρησιμοποιείται οι οποίες δεν στέλνονται στον server.

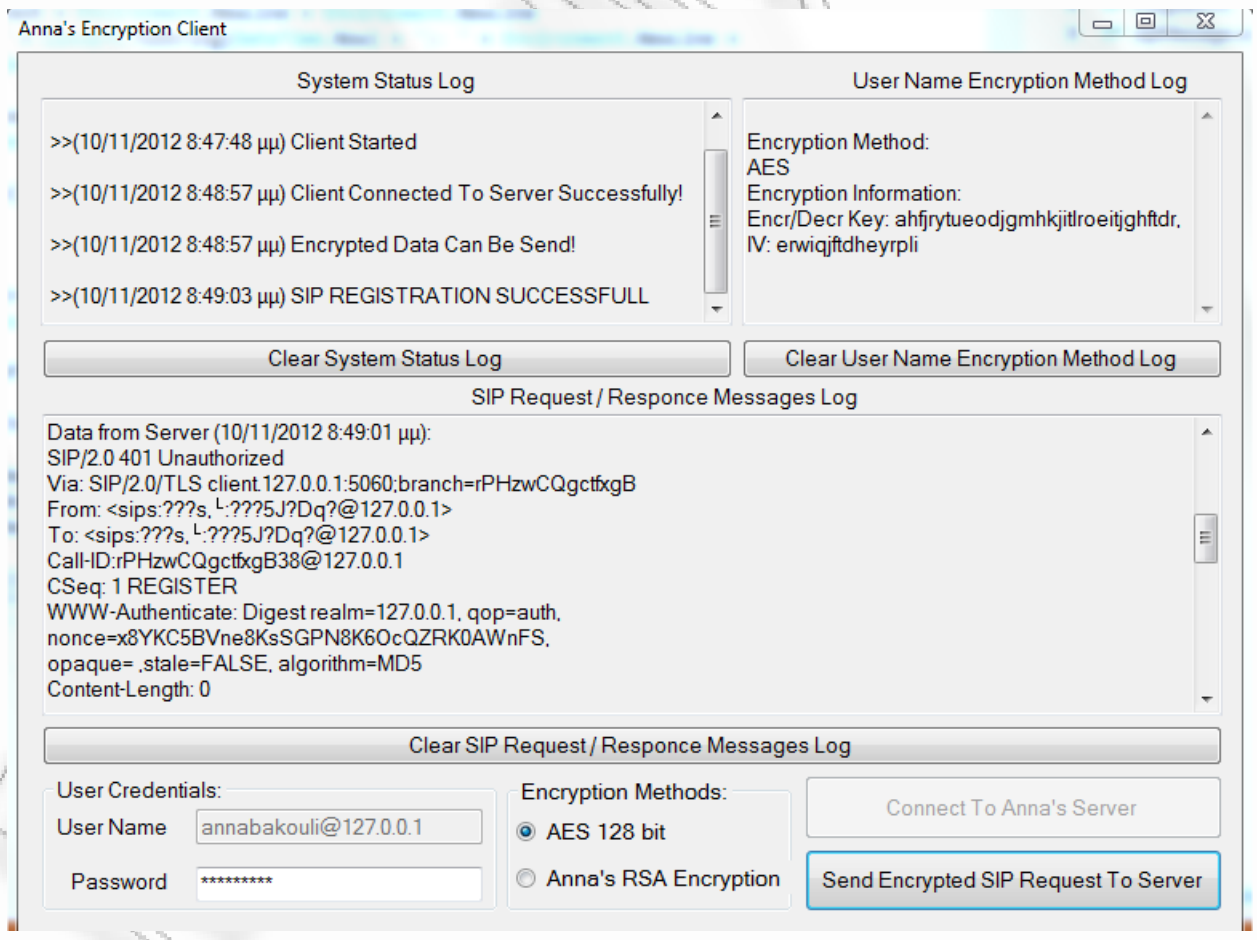


Εικόνα 13 Αποστολή sip register με χρήση AES

Ο Server περιμένει για νέα μηνύματα και όταν λάβει την αίτηση εγγραφής από τον client ελέγχει εάν υπάρχει authorization κεφαλίδα και στην περίπτωση που δεν υπάρχει όπως τώρα θα στείλει μήνυμα που θα περιέχει το challenge με βάση το HTTP Digest. Ο server λοιπόν, δημιουργεί το SIP μήνυμα το οποίο πρέπει να περιέχει την WWW-Authenticate κεφαλίδα η οποία εμπεριέχει μια τυχαία τιμή nonce η οποία θα χρησιμοποιηθεί από τον client για το challenge – response της αυθεντικοποίησης. Στην παρακάτω εικόνα φαίνονται στην κονσόλα του server τα μηνύματα που ανταλλάσσονται.



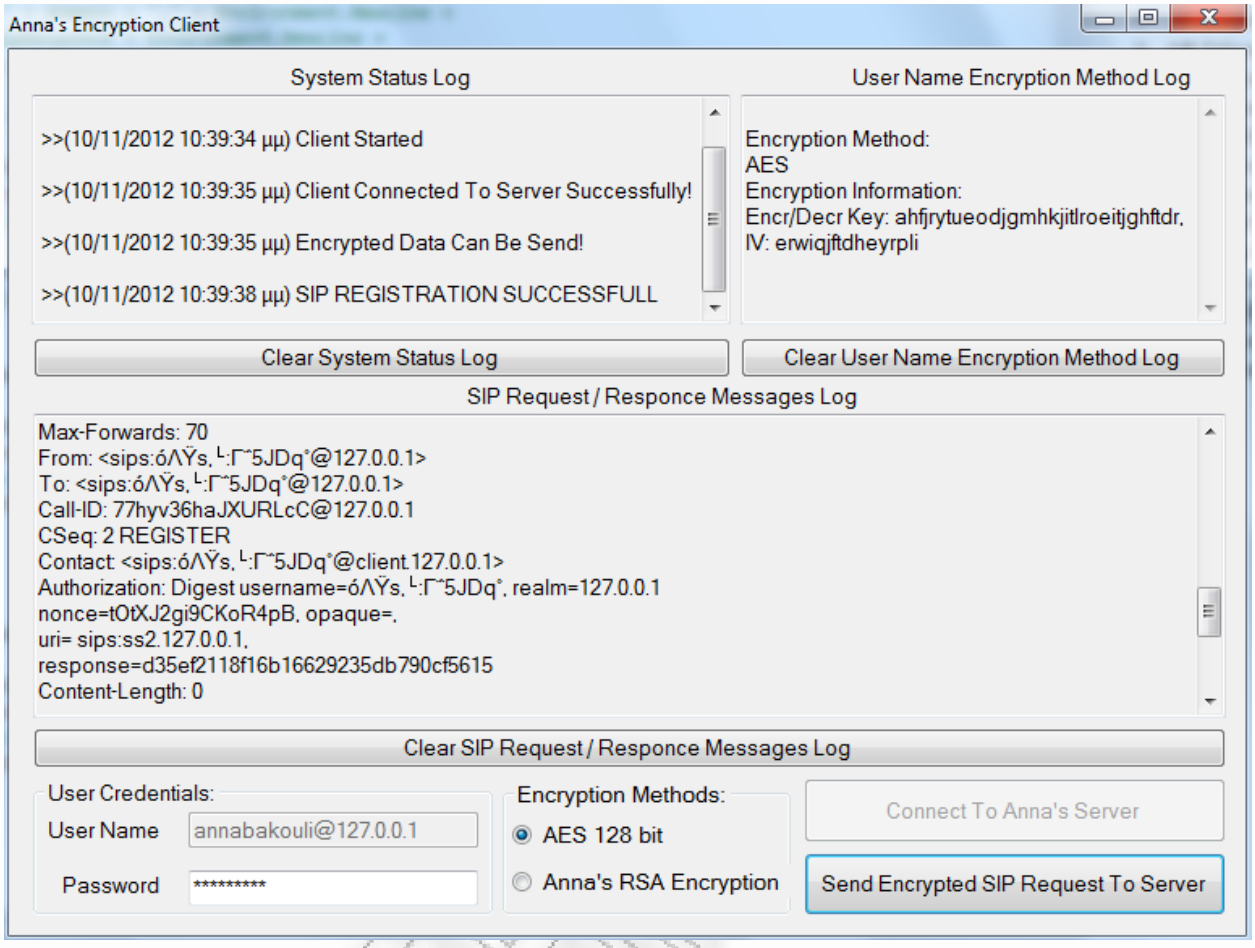
Εικόνα 14 Μηνύματα του Server



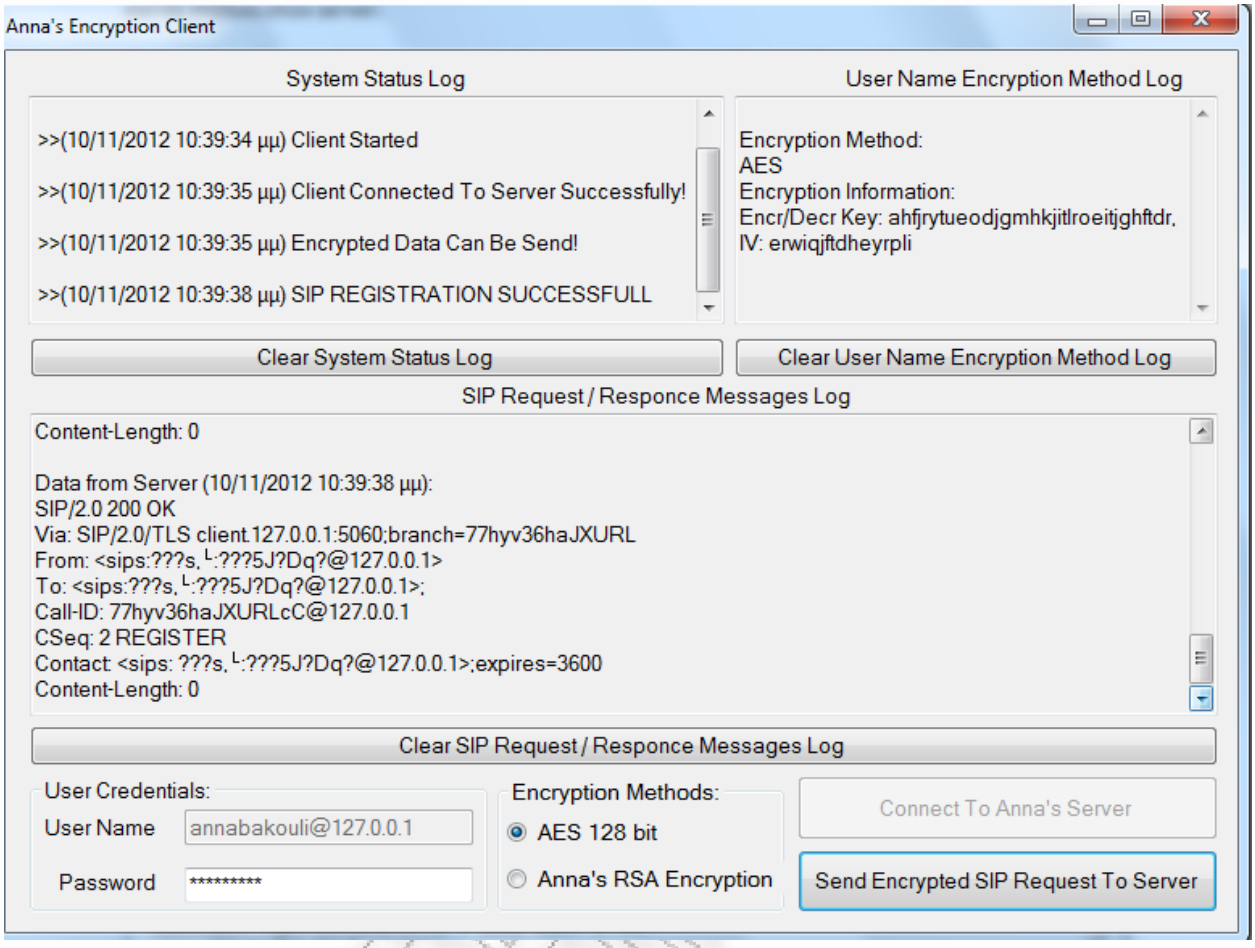
Εικόνα 15 Unauthorized μήνυμα από τον Server

Ομοίως ο client λαμβάνει το μήνυμα και χρησιμοποιώντας το nonce που στάλθηκε από τον servre υπολογίζει τις hash τιμές που απαιτούνται από το πρωτόκολλο HTTP digest κάνοντας χρήση των username, domain, password, URI, της nonce τιμής του server και μιας nonce τιμής που παράγει ο client. Το μήνυμα του server τυπώνεται στην φόρμα και ο client δημιουργεί το μήνυμα που θα στείλει στον server. Το μήνυμα περιέχει επιπλέον σε σχέση με το πρώτο στο authorization header όλες τις τιμές που χρησιμοποιήθηκαν για το response (υπολογισμένο hash) όπως το cnonce. Τυπώνεται και αυτό στην φόρμα και στέλνεται στον Server.

Ο server λαμβάνει το δεύτερο στην σειρά μήνυμα και προκειμένου να διαχωρίσει ποιό μήνυμα είναι ελέγχει το μέγεθος του Authorization header. Εάν είναι μεγαλύτερο του μηδενός, σημαίνει πως είναι το δεύτερο μήνυμα οπότε πρέπει να ελέγξει εάν ο χρήστης υπάρχει στην βάση μέσω των web services. Εάν τα webservices δεν στείλουν τίποτα σημαίνει πως ο χρήστης δεν υπάρχει Βάση δεδομένων και το μήνυμα που θα σταλεί στον client θα είναι 401 Unauthorized. Σε διαφορετική περίπτωση υπολογίζει τα hash για να ελέγξει εάν το response του χρήστη συμπίπτει με αυτό που θα υπολογιστεί στον server με βάση το username και password που είναι αποθηκευμένα στην βάση. Εάν ταυτίζονται οι δύο τιμές τότε θα στείλει μήνυμα 200OK. Το οποίο μόλις το λάβει ο client θα το τυπώσει στην φόρμα όπως και τα προηγούμενα.



Εικόνα 16 Client response



Εικόνα 17 200OK μήνυμα

4.3 Περιγραφή RSA Commutative Key

Ο RSA αποτελεί ένα από τα πρώτα συστήματα δημοσίου κλειδιού, αναπτύχθηκε από τους Ron Rivest, Adi Shamir και Len Adleman στο MIT. Ο αλγόριθμος RSA έχει από τότε κυριαρχήσει ως η πιο ευρέως αποδεκτή και υλοποιημένη προσέγγιση κρυπτογράφησης δημοσίου κλειδιού. Ο συγκεκριμένος αλγόριθμος είναι ένας κωδικοποιητής τμημάτων (μπλοκ), στον οποίο το αρχικό κείμενο και το κρυπτογράφημα είναι ακέραιοι μεταξύ ο και n-1, για κάποια τιμή του n.

Η κρυπτογράφηση και η αποκρυπτογράφηση έχουν την παρακάτω μορφή, για κάποιο δεδομένο τμήμα αρχικού κειμένου M και κρυπτογραφήματος C:

$C=M^e \bmod n$

$M= C^d \bmod n= (M^e)^d \bmod n = M^{ed} \bmod n$

Τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να γνωρίζουν τις τιμές των n και e, ενώ μόνο ο παραλήπτης γνωρίζει την τιμή του d. Ο RSA είναι ένας αλγόριθμος κρυπτογράφησης δημοσίου κλειδιού με δημόσιο κλειδί KU = {e,n} και ιδιωτικό κλειδί KR = {d,n}.

Για να είναι αυτός ο αλγόριθμος ικανοποιητικός για κρυπτογράφηση δημοσίου κλειδιού πρέπει να πληρούνται οι παρακάτω απαιτήσεις:

- Πρέπει να είναι δυνατό να βρεθούν τιμές για τα e, d και n τέτοιες ώστε Medmod n = M mod n για κάθε M < n.
- Πρέπει να είναι σχετικά εύκολο να υπολογιστούν τα Me και Cd για κάθε M < n.
- Πρέπει να είναι να υπολογιστεί το d με δεδομένα τα e και τα n.

Οι δύο πρώτες απαιτήσεις ικανοποιούνται εύκολα, η τρίτη απαίτηση μπορεί να ικανοποιηθεί για μεγάλες τιμές των e και n.

Συνοπτικά ο αλγόριθμος μπορεί να περιγραφεί από τα παρακάτω βήματα.

1. Επιλέγουμε δύο πρώτους αριθμούς, p, και q έστω p= 17 και q= 11
2. Υπολογίζουμε το γινόμενο τους n= pq στην προκειμένη περίπτωση n= 187
3. Υπολογίζουμε την ϕ(n)= (p-1)(q-1)= 16x10= 160
4. Επιλέγουμε το e έτσι ώστε να είναι πρώτος ως προς τον ϕ(n)= 160 και μικρότερος από το ϕ(n), επιλέγουμε e= 7 (ΜΚΔ (e, ϕ(n)= 1)
5. Ορίζουμε το d τέτοιο ώστε demod160= 1 και d< 160. Η σωστή τιμή είναι d= 23, επειδή 23x7 = 161 = 10x16+1

Δημόσιο κλειδί είναι KU = {e,n} και αν το αρχικό μήνυμα είναι M < n το κρυπτογράφημα είναι C= Memod n και για το αρχικό κείμενο υπολογίζεται σύμφωνα με το M= Cdmod n.

Η ποσότητα ϕ(n) αναφέρεται ως συνάρτηση Euler για το n, το οποίο είναι ο αριθμός των θετικών ακεραίων που είναι μικρότεροι από n και πρώτοι ως προς αυτόν.

Υπάρχουν δύο πιθανές προσεγγίσεις για την κατάρριψη του αλγορίθμου RSA. Η πρώτη είναι η προσέγγιση της εξαντλητικής αναζήτησης κλειδιών, επομένως όσο

μεγαλύτερα είναι τα e, d τόσο πιο ασφαλής είναι ο αλγόριθμος. Ωστόσο, επειδή οι υπολογισμοί που εμπλέκονται στη δημιουργία των κλειδιών και την κρυπτογράφηση/αποκρυπτογράφηση είναι πολύπλοκοι, όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο πιο αργό θα είναι το σύστημα κατά την εκτέλεση. Στο ζήτημα το οποίο έχουν εστιάσει περισσότερο σχετικά με την κρυπτανάλυση του RSA είναι ο χωρισμός του n στους δύο πρώτους παράγοντες του. Για μεγάλο n με μεγάλους πρώτους αριθμούς για παράγοντες η διαδικασία του χωρισμού σε παράγοντες είναι ένα δύσκολο πρόβλημα, αλλά όχι τόσο όσο ήταν κάποτε.

Για να έχει ο αλγόριθμος RSA την commutative ιδιότητα πρέπει τα κλειδιά να δημιουργηθούν με χρήση κοινού n. Δηλαδή ο αποστολέας στέλνει στον παραλήπτη τα p, q και n κρατά ιδιωτικό το e. Ο παραλήπτης γνωρίζοντας τα p, q, n δημιουργεί τα δικά του e και d. Σε αυτή την εκδοχή ο αλγόριθμος έχει τελείως διαφορετικό σκοπό, ο σκοπός είναι να μπορεί οποιοδήποτε αρχικό κείμενο να κρυπτογραφηθεί και αποκρυπτογραφηθεί με οποιαδήποτε σειρά.

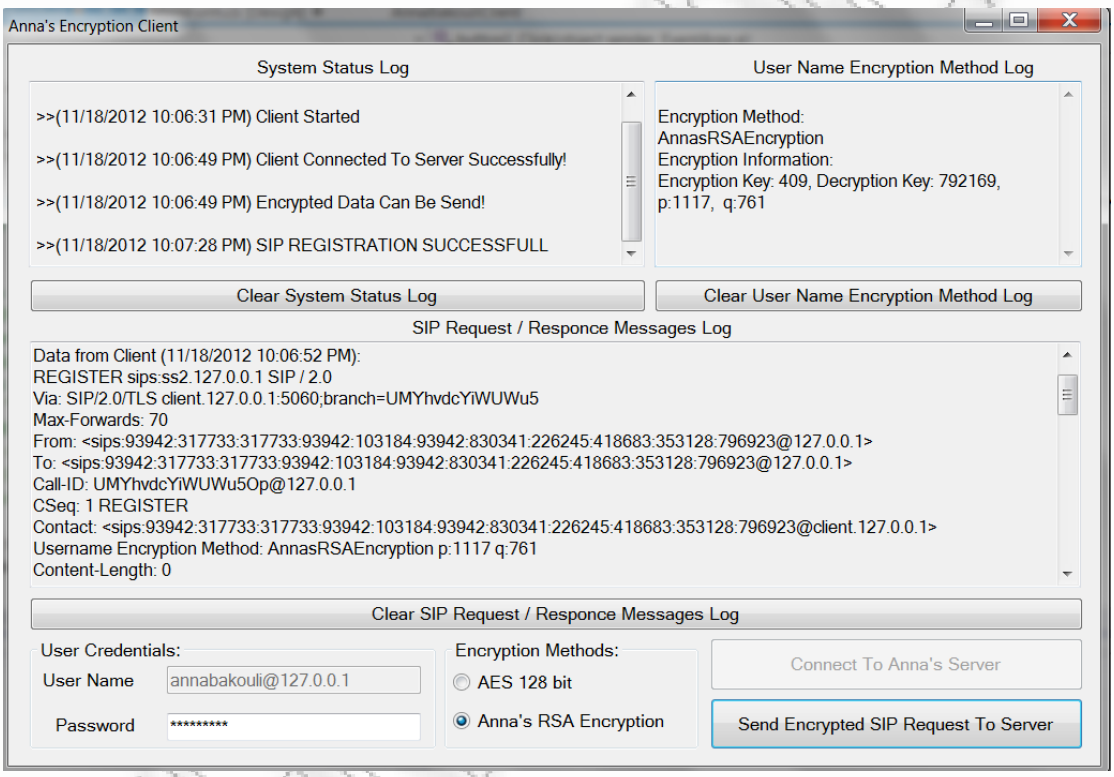
Αρχικά ο αποστολέας επιλέγει δύο πρώτους αριθμούς έστω p=13 και q=5 τότε το n=65 και το φ(n)=48 και επιλέγει e= 7. Τότε το d=7 και στον παραλήπτη θα σταλεί το p,q και σε αυτή την περίπτωση και το n. Έστω ότι ο παραλήπτης επιλέξει για e= 11 τότε και το d=35.

Εάν το μήνυμα που θέλουμε να κρυπτογραφήσουμε είναι το M=2 τότε

- C1= 27mod65=63 αυτό το μήνυμα στέλνει ο αποστολέας Α.
- C2= 6311mod65=32 ο παραλήπτης Β κρυπτογραφεί το μήνυμα ξανά με το δικό του κλειδί.
- M1=327mod65=33 ο Α αποκρυπτογραφεί το μήνυμα με το δικό του κλειδί και το στέλνει ξανά.
- Τέλος ο Β αποκρυπτογραφεί το μήνυμα με το δικό του κλειδί M=3335mod65=2

4.3.1 Κρυπτογράφηση username με χρήση RSA

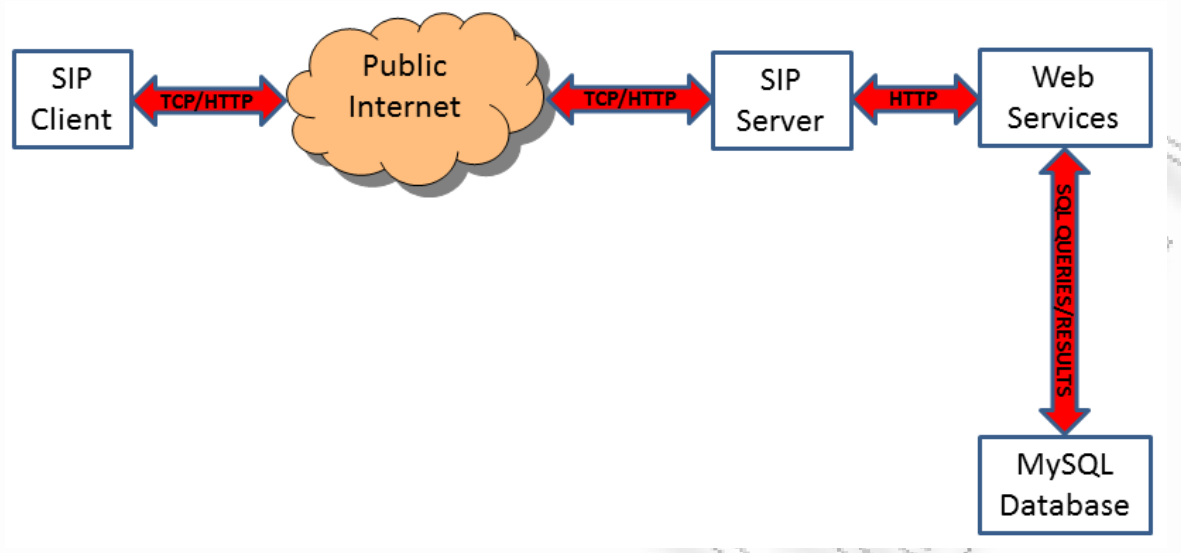
Στην περίπτωση που επιλεχθεί η χρήση του RSA, σε επίπεδο χρήστη ισχύουν τα ίδια ακριβώς με την περίπτωση επιλογής του AES, με την διαφορά πως στην φόρμα τα μηνύματα που στέλνονται περιέχουν και κάποιες επιπλέον τιμές. Το πρώτο μήνυμα του client περιέχει τα p και q που απαιτούνται για την δημιουργία των κλειδιών κρυπτογράφησης. Η διαδικασία για την αποστολή των μηνυμάτων παραμένει ίδια, όσον αφορά στην διεπαφή με τον χρήστη.



Εικόνα 18: Αίτηση εγγραφής με RSA κρυπτογράφηση

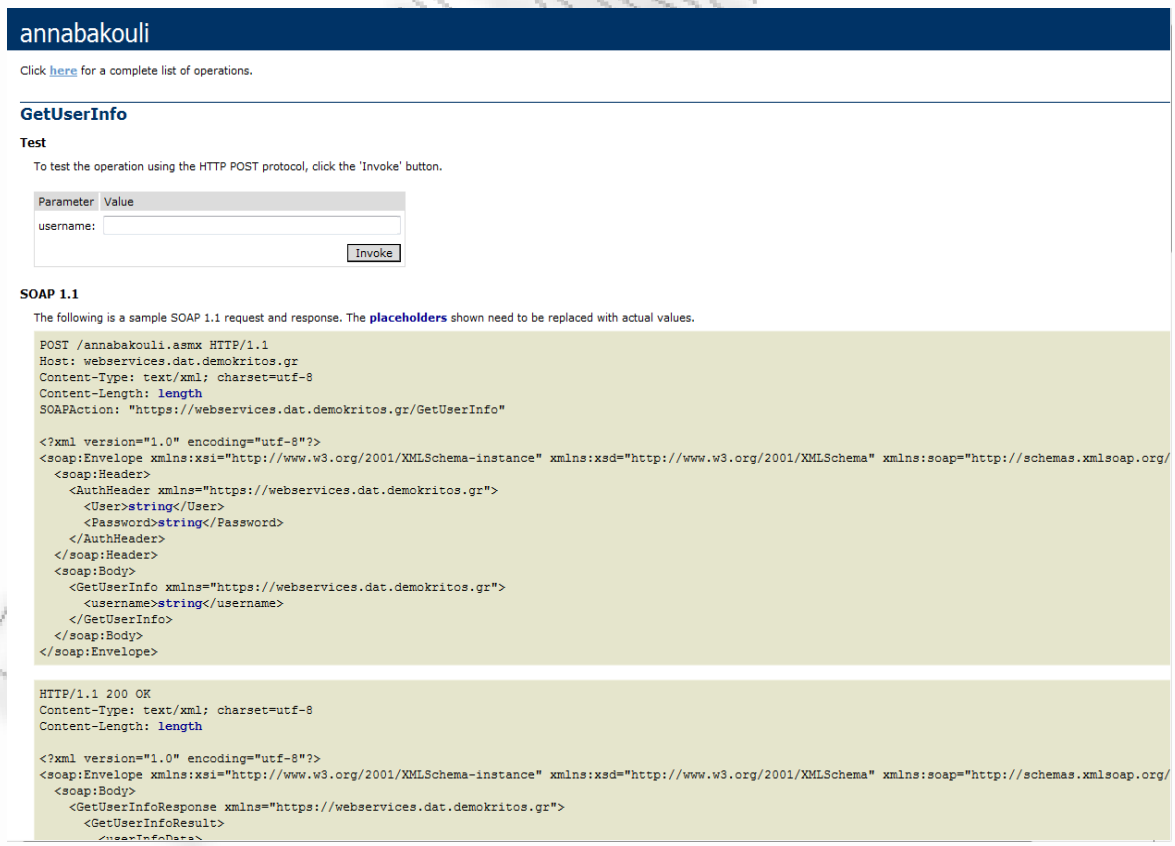
Κεφάλαιο 4.4 Ανάλυση λογισμικού

Ο SIP client μέσω HTTP και TCP πρωτοκόλλων επικοινωνεί με τον SIP Server. Ο Server προκειμένου να επικοινωνήσει με την Βάση Δεδομένων επικοινωνεί με Web Services τα οποία δίνουν την δυνατότητα σύνδεσης με την Βάση, παρέχοντας ένα παραπάνω επίπεδο ασφάλειας. Παρακάτω απεικονίζεται η γενική αρχιτεκτονική του περιβάλλοντος στο οποίο πραγματοποιήθηκε η υλοποίηση του λογισμικού με βάση τα όσα αναφέρθηκαν παραπάνω.



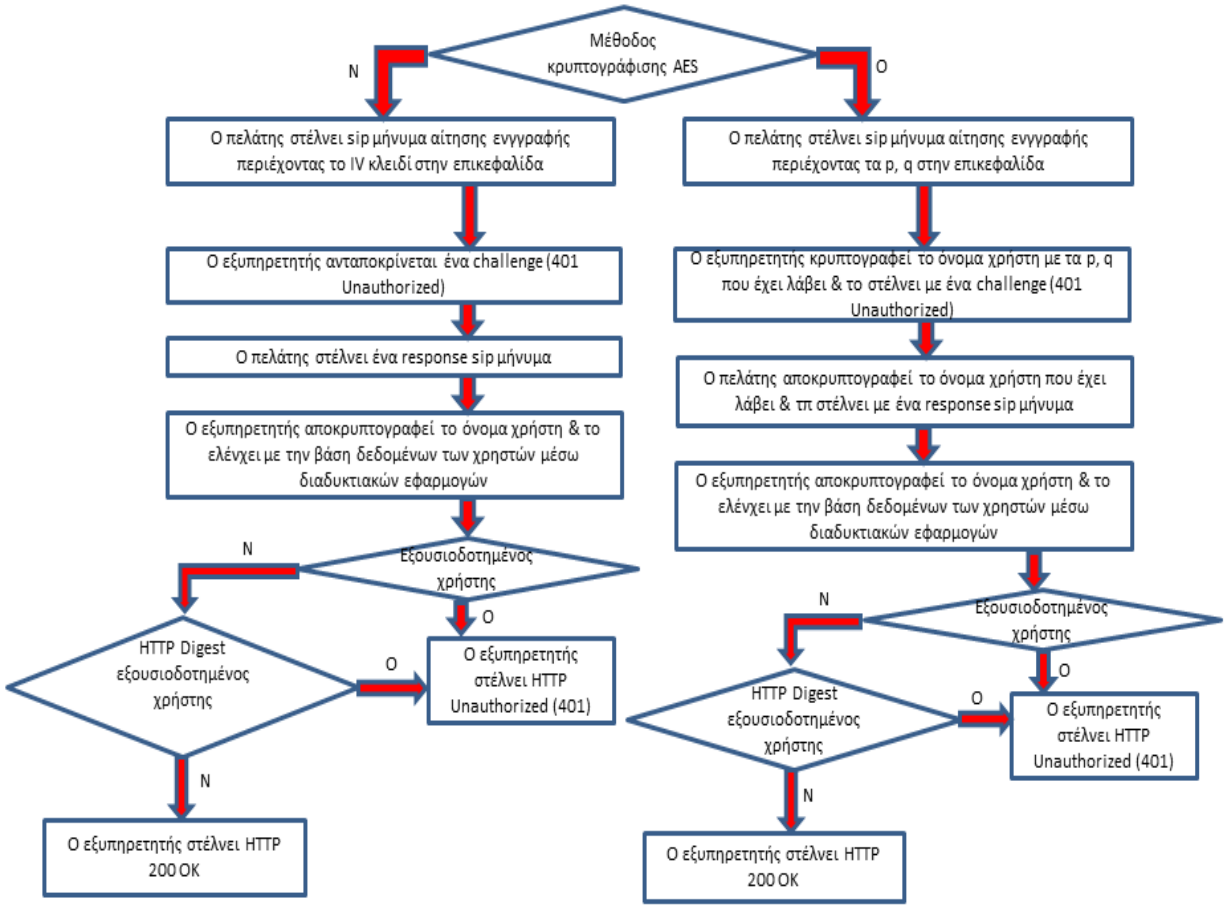
Εικόνα 19: Σχηματικό διάγραμμα αρχιτεκτονικής

Τα Web Services προκειμένου να χρησιμοποιηθούν περιμένουν username και password με σκοπό την αυθεντικοποίηση του χρήστη που τα καλούν. Επιπλέον δέχονται το όνομα του χρήστη το οποίο συγκρίνεται με τα αποθηκευμένα ονόματα χρηστών στην Βάση Δεδομένων και επιστρέφουν σε περίπτωση που υπάρχει καταχωρημένος χρήστης το κωδικό του και το κλειδί κρυπτογράφησης/αποκρυπτογράφησης στην περίπτωση του AES.



Εικόνα 20: Web Services

Στην επόμενη εικόνα απεικονίζεται η ροή των μηνυμάτων λαμβάνοντας υπ' όψιν κάθε δυνατή περίπτωση, δίνοντας μια γενική εικόνα για την λειτουργία του συνολικού λογισμικού.



Εικόνα 21: Διάγραμμα ροής λογισμικού

Για την καλύτερη δυνατή προσομοίωση της επικοινωνίας μεταξύ του client και του server, έγινε χρήση C# .NET για την δημιουργία client-server με TCP sockets. Ο client στέλνει μήνυμα για την εγγραφή του στον Registar server και μετά την ανταλλαγή τεσσάρων συνολικά μηνυμάτων όπως ορίζει το πρωτόκολλο HTTP πρέπει ο server να έχει αποδεχτεί ή να έχει απορρίψει την αίτηση για την εγγραφή του client.

Ο Client δημιουργεί την φόρμα και στο Load της φόρμας εμφανίζεται το μήνυμα Client Started:

```
msg("Client Started");
```

Η msg είναι συνάρτηση η οποία γράφει στο textBox1 ότι υπήρχε ήδη γραμμένο, ημερομηνία και οποιοδήποτε μήνυμα string πάρει ως παράμετρο.

Όταν ο χρήστης επιλέξει να συνδεθεί με τον server εκτελείται από πίσω ο κώδικας που είναι συνδεδεμένος με αυτό το button. Κατά την εκτέλεση του κώδικα αυτού του button αποθηκεύεται το URI από το TextBox2 σε μια μεταβλητή parseUserName. Από αυτή την μεταβλητή εξάγεται το domain και το username.

```
string parseUserName = textBox2.Text;
domain = parseUserName.Substring(parseUserName.IndexOf("@") + 1);
userName = parseUserName.Substring(0, parseUserName.IndexOf("@"));
```

Το domain εξάγεται δίνοντας του την αρχή parseUserName.IndexOf("@") + 1. Αφού γίνει το ίδιο ακριβώς και για το username πραγματοποιείται η σύνδεση με τον server χρησιμοποιώντας το domain που βρήκε με την μέθοδο που αναφέρθηκε παραπάνω και τυπώνει τα δύο μηνύματα το textbox1 σχετικά με την επιτυχή σύνδεση στον server χρησιμοποιώντας την msg.

Μετά την επιλογή του δεύτερου κουμπιού “Send encrypted request to Server” και στην περίπτωση που είναι επιλεγμένος ο AES, δημιουργείται ένα τυχαίο IV και καλείται η μέθοδος encryptStringToBytes_AES της κλάσης AES με ορίσματα το username, το κλειδί και το IV, η κλάση AES περιέχει τον κρυπτογραφικό αλγόριθμο.

Το κρυπτογραφημένο όνομα χρήστη προκύπτει από την μέθοδο encryptStringToBytes_AES της κλάσης AES και επιστρέφεται σε έναν πίνακα από Bytes. Στην συνέχεια τυπώνονται στο TextBox5 “User Name Encryption Method Log” οι γενικές πληροφορίες της κρυπτογράφησης και δημιουργείται το SIP request μήνυμα που θα σταλεί στον Server. Αφού δημιουργήσει το μήνυμα το οποίο είναι ένα string, το τυπώνει στο TextBox 4, το μετατρέπει σε Bytes και το στέλνει στον Server.

```
NetworkStream serverStream = clientSocket.GetStream();
```

```
byte[] outStream1 = Encoding.Default.GetBytes(sipRequest);

serverStream.Write(outStream1, 0, outStream1.Length);
serverStream.Flush();
```

Ο Server με την σειρά του ακούει στην πόρτα 5060 και περιμένει να σταλεί κάποιο μήνυμα. Όταν λάβει το μήνυμα , το διαβάζει και το μετατρέπει σε ένα string

```
dataFromClient = Encoding.Default.GetString(bytesFrom)
```

ώστε να εξάγει το κρυπτογραφημένο username, το domain και την μέθοδο κρυπτογράφησης.

Αφού η κρυπτογράφηση είναι AES θα χρησιμοποιήσει το προκαθορισμένο κλειδί και το IV και αφού μετατρέψει το κρυπτογραφημένο username σε bytes θα καλέσει την μέθοδο αποκρυπτογράφησης από την κλάση AES.

```
DecryptedUserName = AES.decryptStringFromBytes_AES(encryptedUserName,
key, IV);
nonce = GeneralFunctions.CreateRandomString(32);
```

Στην συνέχεια έχοντας το κρυπτογραφημένο username, δημιουργεί το μήνυμα που θα στείλει ως απάντηση στον client. Για αυτό το μήνυμα δημιουργείται επιπλέον μια τυχαία τιμή nonce η οποία θα εμπεριέχεται στο μήνυμα και αποτελεί το challenge προς τον χρήστη.

```
nonce = GeneralFunctions.CreateRandomString(32);
```

Έπειτα μετατρέπει το μήνυμα από string σε Bytes ώστε να το στείλει στον client και τα στέλνει στον client.

```
Byte[] sendBytes = Encoding.ASCII.GetBytes(sipResponse;
networkStream.Write(sendBytes, 0, sendBytes.Length);
```

Ομοίως ο client λαμβάνει το μήνυμα το μετατρέπει σε string και εξάγει με παρόμοιο τρόπο την nonce τιμή που έχει στείλει ο server. Έχοντας την τιμή nonce ο client υπολογίζει το response που θα περιέχεται στο μήνυμα που θα στείλει στον server ώστε να αυθεντικοποιηθεί. Επιπλέον στο response εκτός από τα username, password, domain και nonce, περιλαμβάνεται και μια ακόμα τιμή η cnonce, η οποία είναι μια τυχαία τιμή που υπολογίζεται από τον client.

```
string HA1 = MD5Hash.getMd5Hash(userName + ":" + domain + ":" +
MD5Hash.getMd5Hash(textBox3.Text));

string HA2 = MD5Hash.getMd5Hash("REGISTER:" + textBox2.Text);

string cnonce = GeneralFunctions.CreateRandomString(16);

string sipResponce = MD5Hash.getMd5Hash(HA1 + ":" + serverNonce + ":00000001:"
+ cnonce + ":auth:" + HA2);
```

Μετά την δημιουργία του response, ο client δημιουργεί το μήνυμα που θα στείλει στο οποίο έχει προστεθεί η επικεφαλίδα “Authorization” η οποία περιέχει το response και το cnonce. Τέλος μετατρέπει το μήνυμα σε Bytes το τυπώνει στο TextBox4 και το στέλνει στον server.

Λαμβάνοντας το μήνυμα ο server, καλεί την μέθοδο GetUserInfo του web service, με ορίσματα όνομα χρήστη και κωδικό για αυθεντικοποίηση στο web service και το όνομα χρήστη ώστε να γίνει ο έλεγχος για την ύπαρξη του χρήστη στην Βάση Δεδομένων και την εξαγωγή του κωδικού του ώστε να υπολογιστεί το response από την πλευρά του χρήστη για τον έλεγχο της αυθεντικοποίησης του χρήστη.

```
annasWebService.annabakouliSoapClient webservice = new
annasWebService.annabakouliSoapClient("annabakouliSoap");

                        annasWebService.AuthHeader header = new
annasWebService.AuthHeader();

                        header.User = "annabakouli";
                        header.Password = "universityOfPireus";

annasWebService.userInfoData[]   userInfo   =   webservice.GetUserInfo(header,
DecryptedUserName);
```

Έχοντας αυτά τα δεδομένα, το cnonce από το μήνυμα του client και το nonce που είχε παράγει προηγουμένως ο server υπολογίζει την σύνοψη και αν ταυτίζεται με αυτή που έχει στείλει ο client θα απαντήσει με 200 OK διαφορετικά με 401 Unauthorized.

Εάν ο χρήστης επιλέξει την μέθοδο κρυπτογράφησης RSA “Anna’s RSA Encryption” τότε η διαδικασία που ακολουθείται από την κρυπτογράφηση του ονόματος χρήστη και έπειτα είναι διαφορετική από την περίπτωση του AES. Ότι ίσχυε και για την πρώτη περίπτωση την στιγμή που ο χρήστης επιλέξει το Button2 “Connect to Anna’s Server” ισχύει και σε αυτή την περίπτωση.

Στην περίπτωση του RSA αλγόριθμου, προκείμενου να κρυπτογραφηθεί το username το οποίο πιθανό να αποτελείται από χαρακτήρες, σύμβολα και νούμερα, είναι απαραίτητη η μετατροπή του σε με μια μορφή που να αποτελείται αποκλειστικά από αριθμούς ώστε να γίνει η κρυπτογράφηση. Αυτό επιτυγχάνεται με συνάρτηση μετατροπής που παρέχεται από την C#. Με αυτό τον τρόπο και δημιουργώντας στην συνέχεια ένα πίνακα, το όνομα χρήστη θα μετατρέπεται σε ένα πίνακα από ASCII χαρακτήρες.

```
byte[] word = Encoding.ASCII.GetBytes(username);
```

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Εικόνα 22 ASCII χαρακτήρες

Καλείται από τον client η μέθοδος RSAEncryption της κλάσης AnnasRSA με όρισμα το όνομα χρήστη με σκοπό να κρυπτογραφηθεί. Σε αυτή την κλάση AnnasRSA αρχικά δημιουργούνται δύο τυχαίοι ακέραιοι p, q επειδή η κλήση της συνάρτησης για την δημιουργία τυχαίων αριθμών γίνεται πολύ γρήγορα είναι πιθανό οι δύο αυτοί αριθμοί να είναι ίσοι και για να αποφευχθεί αυτό έχει εισαχθεί ένας έλεγχος ώστε σε περίπτωση ισότητας να ξανά υπολογίζεται το q. Στην συνέχεια υπολογίζεται το n το οποίο είναι το γινόμενο του p με το q και το f το οποίο είναι το γινόμενο του (p-1)*(q-1). Έπειτα πρέπει να υπολογισθεί το e για το οποίο πρέπει να ισχύει GCD(e,f)=1 και το d για το οποίο πρέπει να ισχύει e*dmodf ισοδύναμο με το 1modf. Για να κρυπτογραφηθεί το username πρέπει από string να αποθηκευτεί σε έναν πίνακα από bytes όπου ο κάθε χαρακτήρας αποθηκεύεται με τον ASCII κωδικό του. Για την κρυπτογράφηση σε κάθε έναν από τους χαρακτήρες του πίνακα εφαρμόζεται η παρακάτω πράξη:

```
c = BigInteger.ModPow(word[i], e, n);
```

που στην ουσία είναι η κρυπτογράφηση του γράμματος βασισμένη στην πράξη xemodn. Κάθε γράμμα που κρυπτογραφείται αποθηκεύεται εκ νέου στην πρώτη θέση ενός πίνακα διαχωρισμένο το ένα από το άλλο με το σύμβολο ‘:’. Στον ίδιο πίνακα στην δεύτερη θέση αποθηκεύεται η τιμή του p, στην τρίτη η τιμή του q και στην τέταρτη και πέμπτη οι τιμές d και e αντίστοιχα.

```
encryptedUser[0] = encryptedUser[0].Substring(1);
encryptedUser[1] = " p:" + p.ToString();
encryptedUser[2] = " q:" + q.ToString();
encryptedUser[3] = d.ToString();
encryptedUser[4] = e.ToString();
```

Επιστρέφοντας λοιπόν στον client και αφού έχει λάβει τον πίνακα που έχει επιστρέψει η RSAEncryption συνάρτηση , δημιουργεί το μήνυμα που θα στείλει στον server με την διαφορά ότι στέλνει από τον παραπάνω πίνακα την δεύτερη και τρίτη τιμή ώστε να μπορέσει ο server να υπολογίσει τα αντίστοιχα n, e, d. Επίσης εμφανίζει στην φόρμα όπως και στην προηγούμενη περίπτωση τις πληροφορίες σχετικά με την κρυπτογράφηση.

```
encryptionInfo =  "Encryption Method: "+ Environment.NewLine + encryptionMethod
+ Environment.NewLine +"Encryption Information:" + Environment.NewLine +
"Encryption Key: " + EncryptedUserNameS[4] + ", Decryption Key: " +
EncryptedUserNameS[3] + "," + EncryptedUserNameS[1] + ", " +
EncryptedUserNameS[2] + Environment.NewLine;
textBox5.Text = textBox5.Text + Environment.NewLine + encryptionInfo;
```

Ο Server ακριβώς όπως και στην προηγούμενη περίπτωση, λαμβάνει το μήνυμα και αφού βρει το username, το domain και την μέθοδο κρυπτογράφησης , εξάγει τα p και q από το μήνυμα του client και καλεί την δική του RSAEncryption μέθοδο.

```
DecryptedUserName      =      AnnasRSA.AnnasRSADecryption(EncryptedUserNameS[0],
Convert.ToInt32(EncryptedUserNameS[1]), p, q);
```

Σε αυτή την μέθοδο αφού υπολογίζονται πρώτα τα n, e και d και αφαιρεθούν από το encrypted username οι ειδικοί χαρακτήρες ":",

```
string[] parsedUserName = username.Split(':');
```

ξανακρυπτογραφείται το username και στέλνεται στον client.

Ο client λαμβάνοντας μήνυμα από τον server το αποθηκεύει σε πίνακα από string και ελέγχει εάν το authorization header είναι μεγαλύτερο του μηδενός εάν είναι τότε πρόκειται για το πρώτο μήνυμα του server που θα περιέχει την nonce τιμή και επίσης ελέγχει εάν πρόκειται για RSA κρυπτογράφηση. Σε περίπτωση που όλα τα παραπάνω ισχύουν τότε ο client καλεί την μέθοδο RSAdecryption από την κλάση AnnaRSA ώστε να αποκρυπτογραφήσει το username. Ύστερα από τις κατάλληλες μετατροπές ώστε το username από string να μετατραπεί σε int για να μπορέσει να κρυπτογραφηθεί η ακόλουθη πράξη εφαρμόζεται σε κάθε ένα από τους χαρακτήρες του username.

```
c = BigInteger.ModPow(usernameToDecrypt[i], decKey, n1);
```

Η παραπάνω τιμή επιστρέφεται στον Client που κάλεσε την συνάρτηση, στην συνέχεια ακολουθείται ακριβώς η ίδια διαδικασία για τον υπολογισμό του response (nonce, hash) και το μήνυμα στέλνεται στον Server. Ο Server κάνει την ίδια διαδικασία για την αποκρυπτογράφηση του username και στην συνέχεια την σύγκριση με αυτό που υπάρχει στην βάση δεδομένων. Τέλος, ελέγχει το response

και εάν όλα συμπίπτουν με όσα υπάρχουν στην βάση δεδομένων τότε στέλνει το 200OK μήνυμα, διαφορετικά θα στείλει 401Unauthorized.

Κεφάλαιο 4.5 Σύγκριση των δύο προσεγγίσεων

Στην πρώτη προσέγγιση, η υλοποίηση του αλγόριθμου AES προϋποθέτει τον διαμοιρασμό κλειδιών. Κάθε χρήστης έχει ένα κοινό κλειδί με τον Server, το οποίο ο Server αποθηκεύει μαζί με το username και το password σε μια Βάση Δεδομένων. Συνεπώς σε αυτή προσέγγιση θεωρούμε ως δεδομένη την ύπαρξη ενός έμπιστου περιβάλλοντος από την πλευρά του χρήστη. Στην Βάση Δεδομένων αποθηκεύονται το όνομα χρήστη, ο κωδικός του σε hash μορφή (MD5), το κλειδί του AES σε μορφή κειμένου και σε hash. Το hash του κλειδιού αποθηκεύεται στην Βάση προκειμένου να γίνει η ταυτοποίηση με τον χρήστη. Πιο συγκεκριμένα στο register μήνυμα του χρήστη, θα στέλνεται το κλειδί του σε hash μορφή ούτως ώστε ο Server από την πλευρά του να λαμβάνοντας το μήνυμα με το κρυπτογραφημένο όνομα χρήστη να χρησιμοποιεί το κλειδί για να κάνει αναζήτηση στην Βάση και να μπορεί να συνδέσει το χρήστη με το αντίστοιχο κλειδί.

Στην δεύτερη προσέγγιση τα p και q αποστέλλονται στον Server με το πρώτο μήνυμα σε μορφή απλού κειμένου κάτι το οποίο από πλευρά ασφάλειας μπορεί να θεωρηθεί ευπάθεια για μια πιθανή man in the middle attack όμως τα p,q υπολογίζονται κάθε φορά εκ νέου τυχαία. Η εφαρμογή κρυπτογράφησης σε αυτά θα ήταν ένα επιπλέον βήμα με το οποίο θα έχανε το νόημα του ο συγκεκριμένος τρόπος κρυπτογράφησης. Διότι ο λόγος που αυτή η μέθοδος θεωρείται κατάλληλη επιλογή είναι το γεγονός πως δεν απαιτεί την αποθήκευση καμίας παραπάνω πληροφορίας αφού τα κλειδιά που χρησιμοποιούνται υπολογίζονται κάθε φορά.

Με την χρήση του AES επιτυγχάνεται πλήρης κρυπτογράφηση και απόκρυψη του username αλλά απαιτείται η αποθήκευση δύο επιπλέον πεδίων στην Βάση, του κλειδιού σε μορφή απλού κειμένου και του κλειδιού σε σύνοψη. Με την χρήση του RSA δεν χρειάζεται καμία επιπλέον πληροφορία να αποθηκευτεί αλλά τα p,q στέλνονται σε μορφή απλού κειμένου. Επιπλέον με τον RSA γίνεται εκμετάλλευση και των τεσσάρων μηνυμάτων που ούτως ή άλλως αποστέλλονται λόγω του HTTP Digest.

Κεφάλαιο 5 Εναλλακτική Προσέγγιση

5.1 Εισαγωγή

Με σκοπό όλα τα παραπάνω να εφαρμοστούν σε πραγματικές συνθήκες, έγινε μια προσπάθεια εφαρμογής του με χρήση του Open IMS core, το οποίο είναι μια υλοποίηση των IMS Call Session Control Functions (CSCFs). Για αυτή την προσέγγιση είναι απαραίτητη και η χρήση ενός client ο οποίος να παρέχει την δυνατότητα εισαγωγής δεδομένων στις κεφαλίδες που στέλνονται. Μετά την εγκατάσταση του προαπαιτούμενου λογισμικού, η οποία παρατίθεται αναλυτικά παρακάτω διαπιστώθηκε πως είναι εξαιρετικά πολύπλοκα αξιοποιήσιμο για το συγκεκριμένο σκοπό. Παρ' όλα αυτά η διαδικασία που ακολουθήθηκε κρίθηκε σκόπιμο να αναφερθεί στο παρών κεφάλαιο, καθότι όλα τα βήματα που απαιτούνται έχουν διατυπωθεί αναλυτικά κάτι που θεωρείται χρήσιμο για όποιον επιθυμεί να ασχοληθεί με παρόμοιο θέμα.

5.2 Open IMS Core Installation

Οι προϋποθέσεις για την εγκατάσταση αλλά και οι βασικές οδηγίες βρίσκονται στο επίσημο site OpenIMSCore [http://www.openimscore.org/]. Βασική προϋπόθεση για την εγκατάσταση του OpenIMSCore αποτελεί το λειτουργικό σύστημα το οποίο πρέπει να είναι κάποια έκδοση των Linux. Η συγκεκριμένη υλοποίηση έγινε σε Ubuntu 11.10. Για μεγαλύτερη απόδοση μπορείς χωρίς να αποτελεί βέβαια προϋπόθεση να προσθέσεις περισσότερα Gigabytes RAM και αν έχεις όσους πιο πολλούς διαθέσιμους πυρήνες CPU. Από πλευράς λογισμικού χρειάζονται 100 Mbytes χώρος στο σκληρό δίσκο, ο compiler GCC και make, η java JDK έκδοση μεγαλύτερα από 1,5 και το build tool ant. Επιπρόσθετα MySQL πρέπει να είναι εγκατεστημένη και να τρέχει ή κάποιο άλλο DBMS. Απαιτείται η εγκατάσταση των Bison,Flex και των βιβλιοθηκών libxml2(>2,6) και libmysql και οι δύο μαζί με το

development, curl και libcurl4-gnutls-dev . Επίσης το bind εγκατεστημένο και να τρέχει ή οποιονδήποτε άλλον name server.

Συγκεκριμένα τα βήματα που ακολουθήθηκαν είναι τα παρακάτω:

1) Sudo apt-get install subversion, ant, bison, flex, mysql-server, libmysqlclient-dev, libxml2, libxml2-dev, bind9, libcurl3, libcurl3-dev libcurl4-gnutls-dev.
2) Επόμενο βήμα είναι η εγκατάσταση της Java, από την επίσημη ιστοσελίδα της Sun [ ] κατεβάσαμε το .tar.gz αρχείο για τα Linux και στην συνεχεία με tar xvf jdk-7u3-linux-i586.tar.gz το αρχείο αποσυμπιέζεται. Με τις παρακάτω εντολές γίνεται η εγκατάσταση της Java όμως προηγουμένως πρέπει να γίνει απεγκατάσταση αν υπάρχει άλλη Java η προηγούμενη έκδοση από την 1,5.

   Sudo mv jdk 1.7.0_03 /opt μεταφέρεις την java από τον φάκελο που έχει αποθηκευτεί στο opt.
   Sudo gedit ~/.bashrc πρέπει να γίνει edit το αρχείο bashrc ώστε να προστεθούν οι παρακάτω γραμμές:
   export JAVA-HOME = /opt/ jdk 1.7.0_03
   export PATH = $JAVA-HOME/bin
   export CLASSPATH = $JAVA-HOME/lib

   Έπειτα από τα παραπάνω βήματα η JAVA πρέπει να έχει εγκατασταθεί σωστά και με την εντολή java-version το διαπιστώνουμε.
   java version "1.7.0_03"
   Java(TM) SE Runtime Environment (build 1.7.0_03-b04)
   Java HotSpot(TM) Client VM (build 22.1-b02, mixed mode)
3) Δημιουργούμε τους φακέλους opt, OpenIMSCore, ser_ims και FHoSS
   mkdir opt

cd opt

mkdir OpenIMSCore

cd OpenIMSCore

mkdir ser_ims

mkdir FHoSS

4) Κάνουμε make μέσα στο ser_ims

Cd ser_ims

Make install-libs all

Cd ..

5) cd FHoSS

ant compile

ant deploy

cd ..

6) Στην συνέχεια πρέπει να γίνει η διαμόρφωση του DNS :

Ένα υπόδειγμα αρχείου DNS zone υπάρχει στον φάκελο ser_ims/cfg/open-ims.dnszone, πρέπει να αντιγραφεί στο bind configuration φάκελο. Στην συνέχεια πρέπει να εισάγεις το μονοπάτι του φακέλου στο named.conf αρχείο.

sudo cp ser_ims/cfg/open-ims.dnszone etc/bind/

cd /etc/bind/named.conf

zone "open-ims.test" {

type master;

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

};

Μετά από αυτό το βήμα πρέπει να γίνει επανεκίνηση του DNS με sudo /etc/init.d/bind9 restart

http://www.oracle.com/technetwork/java/javase/downloads/jdk-7u3-download-1501626.html

7) Σε αυτό το βήμα τρέχει η mysql (mysql –u root –p localhost) και εκτελούνται οι παρακάτω εντολές:

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

8) Η διαμόρφωση του IMS Core γίνεται σε αυτό το βήμα ως εξής : Αντιγράφονται τα παρακάτω αρχεία στο opt/OpenIMSCore

cp ser_ims/cfg/*.cfg

cp ser_ims/cfg/*.xml

cp ser_ims/cfg/*.sh

9) Σε αυτό το σημείο μπορούν να ξεκινήσουν να τρέχουν τα μέρη του συστήματος τα οποία πρέπει να τρέχουν παράλληλα.

./pcscf.sh

./icscf.sh

./scscf.sh

FHoSS/deploy/startup.sh

Αν όλα τα βήματα έχουν ολοκληρωθεί επιτυχώς στο URL http://localhost:8080/ είναι το web interface του FHoSS.

Τα επόμενα βήματα αφορούν τροποποίηση αρχείων

10) etc/hosts

10.1.14.139 localhost

10.1.14.139 anna-M7

10.1.14.139 open-ims.test mobicents.open-ims.test ue.open-ims.test presence.open-ims.test icscf.open-ims.test scscf.open-ims.test pcscf.open-ims.test hss.open-ims.test

11) /etc/resolv.conf

#Generated by NetworkManager

search open-ims.test

domain open-ims.test

nameserver10.1.14.139

12) Επανεκκίνηση του bind server

sudo /etc/init.d/bind9 restart

13) Επιβεβαίωση των αλλαγών

Στην κονσόλα, εκτέλεση της dig open-ims.test και στην απάντηση πρέπει να υπάρχει η IP 10.1.14.139 την οποία έχουμε ορίσει στα παραπάνω αρχεία.

14) Αφού έχει οριστέι ως IP η 10.1.14.139 και όχι η localhost (127.0.0.1) όπως είναι προκαθορισμένο να τρέχει το OpenIMSCore θα πρέπει να γίνουν και οι αντίστοιχες αλλαγές στα .cfg και .xml αρχεία των pscsf, icscf και scscf. Επίσης στις ρυθμίσεις του FhoSS από τα αρχεία DiameterPeerHSS.xml και hss.properties.

4.2 Εγκατάσταση Client

Αφού η εγκατάσταση του OpenIMSCore έχει ολοκληρωθεί επιτυχώς το επόμενο βήμα είναι η εγκατάσταση κάποιου IMS client με σκοπό την εγκατάσταση μια κλήσης ώστε να επιβεβαιωθεί πως το OpenIMS λειτουργεί σωστά κάνει εγγαφές χρηστών και εξυπηρετεί κλήσεις. Αρχική επιλογή ήταν ο UCT IMS Client όμως λόγω αντιμετώπισης αρκετών προβλημάτων εξ' αιτίας της μη συμβατότητας του με

Ubuntu έκδοσης νεότερης από 10.04, επιλέχθηκε το Mymonster μια τηλεπικοινωνιακή σουίτα της εταιρίας Fraunhofer. Πρόκειται για εφαρμογή που εγκαθίσταται εύκολα, με διεπαφή πολύ φιλική προς τον χρήστη και με σαφείς οδηγίες εγκατάστασης και χρήσης στην επίσημη ιστοσελίδα []. Τα βήματα που ακολουθήθηκαν για την εγκατάσταση και τις απαιτούμενες ρυθμίσεις περιγράφονται παρακάτω.

Αφού κατέβει το αρχείο για λειτουργικό Linux από το τερματικό, πρέπει να αποσυμπιεστεί, από το τερματικό αυτό γίνεται όπως και παραπάνω με την εντολή :

tar xvf mymonster-0.9.25

και στην συνέχεια το τρέχουμε με:

./monster

έτσι ανοίγει το γραφικό περιβάλλον όπου πρέπει να γίνουν οι απαραίτητες ρυθμίσεις για το IMS δίκτυο:

domain: open-ims.test
public identity: sip:bob@open-ims.test
private identity: bob@open-ims.test
secret key: bob
PCSCF: pcscf.open-ims.test
port:4060

Τα public και private identity καθώς και το secret key πρέπει να συμπίπτουν με τις αντίστοιχες καταχωρήσεις που υπάρχουν για τον συγκεκριμένο χρήστη στην βάση δεδομένων HSS του IMS δικτύου. Το FhoSS του OpenIMSCore έχει ήδη καταχωρημένους δύο χρήστες τον Bob και την Alice.

1. Alice

- Private Identity: alice@open-ims.test
- Secret Key: alice

- OP: 0x00...0
- AMF: 0x00...0
- Use of Anonimity Key: enable
- Public Identity: sip:alice@open-ims.test
- Realm: open-ims.test
- Strict Outbound Proxy: sip:pcscf.open-ims.test:4060

2.Alice

- Private Identity: bob@open-ims.test
- Secret Key: bob
- OP: 0x00...0
- AMF: 0x00...0
- Use of Anonimity Key: enable
- Public Identity: sip:bob@open-ims.test
- Realm: open-ims.test
- Strict Outbound Proxy: sip:pcscf.open-ims.test:4060

Πριν γίνει το REGISTER και ένα test call πρέπει να γίνουν κάποιες ακόμα ρυθμίσεις. Πρέπει να γίνει χρήση του αλγορίθμου MD-5 και για αυτό το λόγο στο HSS μέσα από το γραφικό περιβάλλον πρέπει να επιλεγεί η χρήση του συγκεκριμένου αλγορίθμου και στην συνεχεία να τροποποιήσουμε και τον κώδικα του SCSCF στο αρχείο scscf.cfg ορίζοντας τον MD5 ως προκαθορισμένη μέθοδο αυθεντικοποίησης αντί του AKAv1-MD5. Το τελευταίο βήμα μπορεί να γίνει και από τις ρυθμίσεις του client, έπειτα από αυτό μπορεί να γίνει η δοκιμή για εγγραφή και με την χρήση του Wireshark παρακολουθείται η κίνηση SIP με αποτέλεσμα να γνωρίζεις ακριβώς ποια πακέτα ανταλλάσσονται.

4.3 PJSIP – Open Source SIP Stack

Προαπαιτούμενα για απλή χρήστη χωρίς βίντεο:

- GNU make
- GNU gcc

Αφού κατεβάσουμε το πακέτο από την επίσημη ιστοσελίδα πρέπει να το αποσυμπιέσουμε, από την κονσόλα αυτό γίνεται με την εντολή :

tar xvjf pjproject-2.0-rc.tar.bz2

Στην συνέχεια τρέχουμε ./configure μέσα στο φάκελο του πακέτου χωρίς ορίσματα ώστε το script να εντοπίσει τις κατάλληλες ρυθμίσεις για το host. Στην συνέχεια εκτελούμε με την ακόλουθη σειρά :

make dep

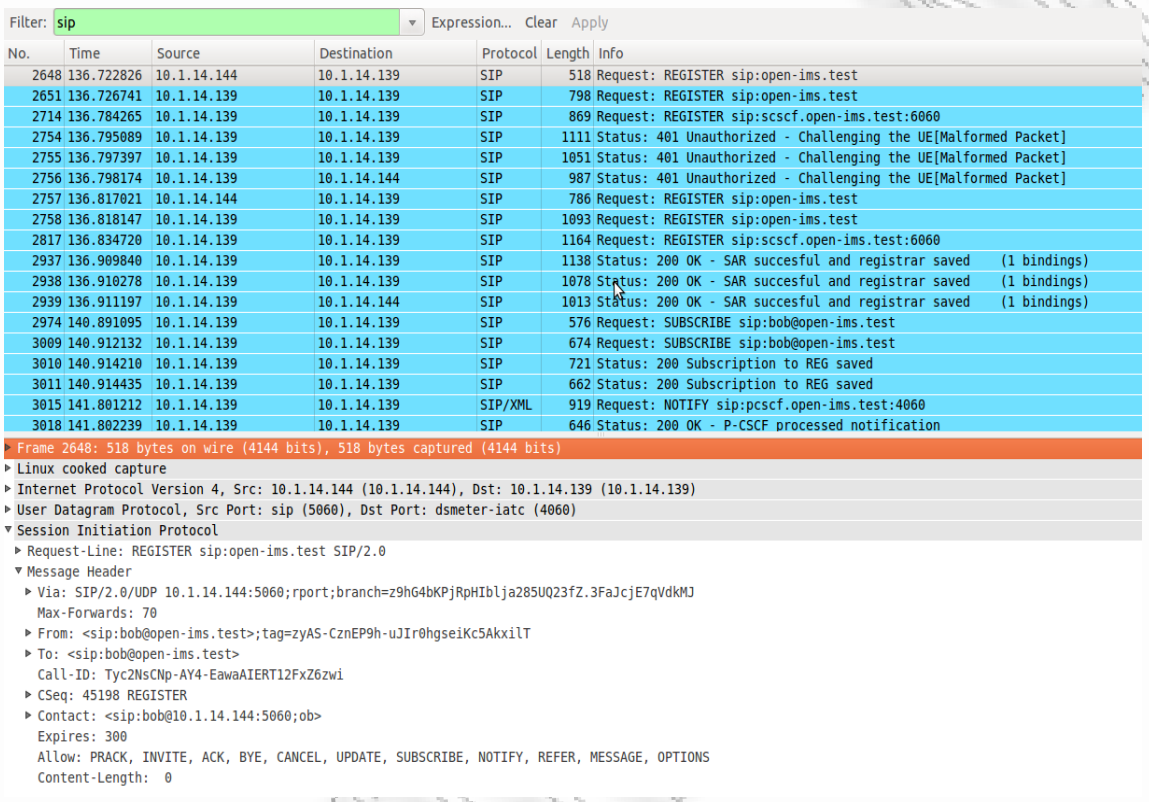
make

make install

Για εξοικειωθεί ο χρήστης με το PJSIP δίνεται η δυνατότητα να τρέξει την εφαρμογή pjsua η οποία ενώ δεν έχει όλα τα χαρακτηριστικά του PJSIP, περιέχει τα περισσότερα.

Στην συγκεκριμένη περίπτωση το pjsua εγκαταστήθηκε σε διαφορετικό μηχάνημα από αυτό του OpenIMSCore και συγκεκριμένα σε Ubuntu 11.10 Server. Πριν σταλθεί το μήνυμα Register και σε αυτή την περίπτωση είναι απαραίτητες κάποιες τροποποιήσεις. Στο αρχείο simple_pjsua.c που βρίσκεται στο /pjsip-apps/src/samples/simple_pjsua.c πρέπει να καταχωρηθούν τα στοιχεία του χρήστη username και password τα οποία και πάλι πρέπει να συμπίπτουν με αυτά της βάσης ώστε να μπορεί να γίνει η ταυτοποίηση του χρήστη και η εγγραφή επιτυχώς. Επιπλεόν πρέπει να εισαχθεί και το SIP_DOMAIN δηλαδή στην περίπτωση μας το open-ims.test. Επειδή ο proxy PCSCF ακούει στην πόρτα 4060 πρέπει να αλλαχθεί η πόρτα στο αρχείο sip_transport.c που βρίσκεται στον κατάλογο /pjsip/src/pjsip/. Μετά τις αλλαγές πρέπει να γίνει make στον κεντρικό φάκελο και τέλος να τρέξουμε

το εκτελέσιμο ./simple_pjsua το οποίο βρίσκεται στο κατάλαγο pjsip-apps\bin\samples\i686-pc-linux-gnu. Στην οθόνη μας βλέπουμε πλέον τα μηνυματα που ανταλλάσσονται μεταξύ του client και του IMS δικτύου.



Εικόνα 23 Wireshark SIP πακέτα

Κεφάλαιο 6 Συμπεράσματα και μελλοντικές κατευθύνσεις

6.1 Συμπεράσματα

Στις υπηρεσίες διαδικτυακής τηλεφωνίας η ασφάλεια αποτελεί πολύ σημαντικό κομμάτι, αφ' ενός για την αποδοχή από το ευρύ κοινό καθώς τα θέματα ασφάλειας επηρεάζουν άμεσα την αξιοπιστία και την διαθεσιμότητα και αφ' έτερου γιατί η αξιοποίηση δικτύων ανοιχτής αρχιτεκτονικής δημιουργεί νέες ευκαιρίες επιθέσεων και απειλών στην ασφάλεια. Οι προτεινόμενες λύσεις διαφοροποιούνται πολύ συγκριτικά με αυτές του συμβατικού τηλεφώνου αφού το τελευταίο βασίζεται σε κλειστή αρχιτεκτονική.

Στην παρούσα διπλωματική εργασία αφού έγινε η απαραίτητη περιγραφή του πρωτοκόλλου SIP, που αποτελεί ένα ευρέως χρησιμοποιούμενο πρωτόκολλο σηματοδοσίας, αναφέρθηκαν οι πιθανές απειλές σε αυτό και τον τρόπο με τον οποίο μπορούν να εκμεταλλευτούν οι ευπάθειες αυτού. Στην συνέχεια περιγράφηκαν μηχανισμοί ασφάλειας ώστε να αντιμετωπιστούν και να αποφθεχθούν περιστατικά ασφάλειας.

Η συμβολή της συγκεκριμένης διπλωματικής αφορά θέματα ιδιωτικότητας που προκύπτουν κατά την αποστολή μηνυμάτων εγγραφής του χρήστη. Προτάθηκαν δύο προσεγγίσεις βασισμένες σε διαφορετικούς αλγορίθμους κρυπτογράφησης. Ο ένας κάνοντας χρήση προ- διαμοιρασμένου κλειδιού και ο δεύτερος με χρήση κλειδιών που δημιουργούνται εκ νέου κάθε φόρα που αποστέλλεται ένα καινούργιο μήνυμα εγγραφής. Η επιλογή του κατάλληλου αλγορίθμου έχει να κάνει με το εάν η δημιουργία νέων πεδίων στην Βάση δεδομένων του δικτύου είναι προτιμότερη από τον υπολογισμό των κλειδιών κατά την αποστολή των μηνυμάτων.

6.2 Μελλοντικές κατευθύνσεις

Με βάση την παρούσα διπλωματική μια προτεινόμενη μελλοντική κατεύθυνση θα μπορούσα να ήταν η εφαρμογή των αλγορίθμων σε εξομοίωση πραγματικών συνθηκών με χρήση του Open IMS Core. Έχοντας ως δεδομένο τον αλγόριθμο που θα χρησιμοποιηθεί και τον τρόπο υλοποίησης του, καθώς επίσης και όλα τα βήματα εγκατάστασης και παραμετροποίησης του Open IMS Core και του client, γίνεται εφικτή η έρευνα για την υλοποίηση σε ένα τέτοιο περιβάλλον και πραγματοποιείται και πλήρης αξιοποίηση της παρούσας διπλωματικής.

Βιβλιογραφία

D. Geneiatakis, G. K. (n.d.). SIP Security Mechanisms: A state-of-the-art review. *SIP Security Mechanisms: A state-of-the-art review Department of Information and Communication Systems Engineering*.

Ericsson. (2012, 02 02). IMS Architecture Overview.

mobilein.com. (n.d.). Ανάκτηση 01 20, 2012, από http://www.mobilein.com/CSCF.htm///ericson

Qiu, Q. (2003, December). Study of Digest Authentication for Session Initiation Protocol (SIP). SITE, University of Ottawa.

RFC 2617. (n.d.). Ανάκτηση από http://www.ietf.org/rfc/rfc2617.txt

RFC 3261. (n.d.).

Russel, T. (n.d.). *SESSION INITIATION PROTOCOL (SIP) controlling convergent networks.* McGRAW-HILL COMMUNICATIONS.

Russell, T. (n.d.). *SIP Controlling Convergent Networks.* McGRAW-HILL COMMUNICATION.

Samer EL SAWDA, P. U. (n.d.). SIP Security Attacks and Solutions: A state-of-the-art review.

SIP HANDBOOK Services, Technologies and Security of Session Initiation Protocol. (n.d.). SYED A. AHSON MOHAMMAD ILYAS.

Wikipedia. (n.d.). Ανάκτηση 01 20, 2012, από http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem

Wireshark. (n.d.). Ανάκτηση από http://www.wireshark.org/

Γ. Καμπουράκης, Σ. Γ. (n.d.). *Ασφάλεια Κινητών και Ασύρματων Δικτύων.*

Γενειατάκης, Δ. (2008, 06). Πλαίσιο Ανίχνευσης και Αντιμετώπισης Περιστατικών Ασφάλειας σε Συστήματα Διαδικτυακής Τηλεφωνίας.

Π.Αντωνίου, Μ. Π. (2005, Ιούνιος). Σχεδίαση και ανάπτυξη λογισμικού για τη χρήση του Πρωτοκόλλου Έναρξης Συνόδου (SIP) ως γενικευμένου πρωτοκόλλου σηματοδοσίας σε. Αθήνα.