Πανεπιστήμιο Πειραιώς

Τμήμα :Ψηφιακών Συστημάτων και Διδακτικής της Τεχνολογίας

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Κατεύθυνση :Ψηφιακών επικοινωνιών και δικτύων

Πτυχιακή Εργασία με Θέμα : Η ασφάλεια στο SIP πρωτόκολλο και η λύση των SBC's

Αντώνογλου Πρόδρομος

Περιεχόμενα

Εισαγωγή

Με την εργασία αυτή αρχικά, θα αναδειχτεί το πρόβλημα των διαφορετικών τύπων δικτύων που υπάρχουν και πρόκειται να υπάρξουν και πως η χρήση ενός πρωτόκολλου σηματοδοσίας όπως το SIP, το οποίο βασίζεται στην τεχνολογία του IP-διαδικτύου, μπορεί να συμβάλλει στην διαλειτουργικότητα των υπάρχοντων και μελλοντικών δικτύων στο τομέα της φωνητικής - πολυμεσικής επικοινωνίας.

Στη συνέχεια θα δούμε την λειτουργία του SIP πρωτοκόλλου την αρχιτεκτονική του , τα μηνύματά του καθώς και παραδείγματα κλήσης σε SIP σύστηματα.

Ένα τόσο σημαντικό πρωτόκολλο στο τομέα των τηλεπικοινωνιών θα πρέπει να είναι ασφαλές ώστε να χρησιμοποιηθεί σε ευρεία κλίμακα. Έτσι στο επόμενο κεφάλαιο θα αναλύσουμε τα θέματα ασφαλείας καθώς και τις διάφορες επιθέσεις που είναι δυνατόν να υπάρξουν σε SIP συστήματα που αποτελεί και από τους βασικούς σκοπούς της συγκεκριμένης εργασίας.

Επιπλέον, θα δούμε τους υπάρχοντες μηχανισμούς ασφαλείας που υπάρχουνε ήδη στο πρωτόκολλο και ποίους περιορισμούς έχουνε στην εφαρμογή τους.

Στο τελευταίο μέρος της εργασίας θα δούμε την λύση των Οριακών Ελεγκτών Συνόδου «SBC» σε θέματα ασφάλειας και λειτουργικότητας των SIP συστημάτων. Θα αναλύσουμε τις διάφορες λειτουργίες που μπορούν να εκτελέσουν οι «SBC» , τον ρόλο τους στην αποστρατικοποιημένη ζώνη (demilitarized zone) «DMZ» και πως τα πακέτα σηματοδοσίας(SIP) και πολυμέσων διασχίζουνε την «DMZ» με την συμβολή των Οριακών Ελεγκτών Συνόδου «SBC».

1.1 Προϋπάρχοντα Δίκτυα Τηλεπικοινωνιών Διαφορετικής Τεχνολογίας

Αρκετά πριν την ανάδειξη του ιντερνέτ οι πάροχοι τηλεπικοινωνιακών υπηρεσιών και οι χρήστες ήταν συνηθισμένοι να σκέφτονται διαφορετικούς τύπους δικτύων.

Οι τύποι αυτοί είναι: δίκτυο για φωνή , δίκτυο για δεδομένα και δίκτυο για τηλεόραση - ραδιόφωνο.

Κάθε τύπος από τα δίκτυα αυτά θα μπορούσε να διαιρεθεί σε πολλά μη συμβατά δίκτυα ανάλογα τις γεωγραφικές περιοχές που συναντούνται, τα οποία αρκετές φορές στηρίζονται και σε διαφορετικά πρωτόκολλα - τεχνολογίες .

Για αυτό βρίσκουμε διαφορετικούς τύπους τηλεφωνικών αριθμητικών σχεδίων (telephony numbering plans), σηματοδοσίας (πινάκας 1), τηλεοπτικών προτύπων (TV standards) και διαφορετικά δίκτυα δεδομένων. Η ασυμβατότητα και η ποικιλία αυτή κάνει δύσκολη την ενσωμάτωση όλων αυτών των δικτύων σε ένα παγκόσμιο δίκτυο. **Αλλά επίσης δύσκολη την ενιαία αντιμετώπιση των θεμάτων ασφαλείας και αξιοπιστίας που προκύπτουν στα δίκτυα αυτά.**

QSIG (Q-Signaling protocol)
H.225.0
SIP (Session Initiation Protocol)
H.323
H.248
MGCP (Media Gateway Control Protocol)
SS7 (Signaling System #7)
C7
C5
DTMF (Dual-Tone Multi-Frequency)

R1
R2
ISDN (Integrated Services Digital Network)
NBAP (Node B Application Part)
SCCP (Skinny Call Control Protocol), or 'Skinny' for short

Πίνακας 1. πρωτόκολλα σηματοδοσίας

Τα δίκτυα δεδομένων που αρχικοποιήθηκαν από την τηλεπικοινωνιακή βιομηχανία (ITU-T και IEEE κυρίως) προέκυψαν σε διαφορετικούς τύπους όπως οι ψηφιακές ιδιωτικές-μισθωμενες γραμμές , X.25 , **ISDN** , SDMS, frame relay και ATM

Αυτά τα δίκτυα έχουν εμπνευστεί από τα circuit-switched τηλεφωνικά θέματα. Το όνομα τους προκύπτει από το γεγονός ότι δεν έχουν σχεδιαστεί για να μεταφέρουν φωνή.

Τα δίκτυα για φωνή μπορούν επίσης να χρησιμοποιηθούν για δεδομένα και φαξ εξαιτίας της γενικότερης διαθεσιμότητας τους. Όμως βρίσκονται στο τέλος της εξέλιξης τους αφού έχουν δημιουργηθεί κυρίως για φωνή. Τέλος , τα τηλεοπτικά δίκτυα (καλωδιακά και μη) έχουν σχεδιαστεί και δημιουργηθεί για την μεταφορά βίντεο.

Η τεραστία διάδοση διαφόρων τύπων ασύρματων κινητών δικτύων (wifi ,wi-max UMTS, GSM, κτλ.) έχει αυξήσει την δικτυακή ποικιλία ακόμη περισσότερο!

Επιπλέον όλα αυτά τα διαφορετικά δίκτυα είχαν και έχουν διαφορετικές συσκευές τελικού – χρήστη οι οποίες δεν μπορούσαν να χρησιμοποιηθούν σε διαφορετικά δίκτυα.

Σύμφωνα με στατιστικά στοιχεία από τον International Telecommunication Union (Οκτ. 2010) έως το τέλος του χρόνου θα υπάρχουν 5,3 δισεκατομμύρια συνδέσεις κινητής τηλεφωνίας που αντιστοιχεί στο 77% του παγκόσμιου

πληθυσμού και είναι τεράστια αύξηση από τα 4,6 δις συνδέσεων στο τέλος του 2009.

Στον παρακάτω πίνακα μπορούμε να δούμε στατιστικά στοιχεία σχετικά με διαφορετικούς τύπους δικτύων όπως κινητής τηλεφωνίας , σταθερής τηλεφωνίας και σταθερού αλλά και κινητού ευζωνικού ιντερνέτ και να συμπεράνουμε το μέγεθος της ανάπτυξης των ασύρματων κινητών δικτύων.

Key Global Telecom Indicators for the World Telecommunication Service Sector in 2010 (all figures are estimates)									
	Global	**Developed nations**	**Developing nations**	**Africa**	**Arab States**	**Asia & Pacific**	**CIS**	**Europe**	**The Americas**
Mobile cellular subscriptions	5,282	1,436	3,846	333	282	2,649	364	741	880
Per 100 people	76.2 %	116.1%	67.6%	41.4 %	79.4 %	67.8 %	131.5 %	120.0 %	94.1%
Fixed telephone lines	1,197	506	691	13	33	549	74	249	262

Per 100 people	17.3 %	40.9%	12.1%	1.6%	9.4%	14.0 %	26.6 %	40.3%	28.1%
Mobile broadband subscriptions	940	631	309	29	34	278	72	286	226
Per 100 people	13.6 %	51.1%	5.4%	3.6%	9.7%	7.1%	25.9 %	46.3%	24.2%
Fixed broadband subscriptions	555	304	251	1	8	223	24	148	145
per 100 people	8.0%	24.6%	4.4%	0.2%	2.3%	5.7%	8.7%	23.9%	15.5%
Source: International Telecommunication Union (October 2010)								**via: mobiThinking**	

Πίνακας 2. Στατιστικά στοιχεία χρήσης διαφορετικών τηλ/κών δικτύων

1.2 Η «επανάσταση» του Ιντερνέτ-Διαδικτύου

Βλέποντας τις τεχνολογικές και κοινωνικές εξελίξεις των τελευταίων δεκαετιών η φράση «επανάσταση» δεν αποτελεί υπερβολή. Πέρα από τις αλλαγές στον τρόπο ζωής των νέων αλλά και παλαιότερων γενιών το διαδίκτυο συμβάλει στο μέλλον των τηλεπικοινωνιών.

Επωφελήθηκε από ένα αριθμό διαφορετικών παραγόντων σε σχέση με τα προϋπάρχοντα δίκτυα , όπως η τεράστια πρόοδος των υπολογιστικών και λειτουργικών συστημάτων και η παγκοσμιοποίηση.

Αυτή η πρόοδος μπορεί να αποδοθεί και στην εξειδίκευση ερευνητικών, ακαδημαϊκών και μηχανικών κοινοτήτων (όπως IETF) των οποίων η αφοσίωση στην διάκριση , καινοτομία και στη ανοιχτή συνεργασία σε παγκόσμια βάση κατάφερε να ξεπεράσει σε ένα βαθμό την εμπορική πίεση, που συνήθως καθυστερεί την αλματώδη εξέλιξη των τεχνολογιών και την ανταγωνιστική εταιρική μυστικότητα που έχει ως αποτέλεσμα την δημιουργία μη συμβατών πρωτοκόλλων και τεχνολογιών.

Αυτό συντέλεσε σε ένα διαδίκτυο (IP network) που χρησιμοποιεί σύμφωνα-σταθερα πρωτόκολλα σε παγκόσμια βάση και είναι ικανά να μεταφέρουν δεδομένα ,φωνή αλλά και βίντεο-πολυμέσα.

Δίνοντας έτσι μια λύση στο πρόβλημα των διαφορετικών δικτύων που προϋπήρχαν με την χρησιμοποίηση ενός IP δικτύου για όλες τις υπηρεσίες (φωνή – δεδομένα - τηλεόραση).

Στο παρακάτω σχήμα μπορούμε να δούμε συνοπτικά τα στρώματα της αρχιτεκτονική του TCP/ IP δικτύου

Στρώμα Εφαρμογής
Στρώμα Μεταφοράς
Στρώμα Διαδικτύου
Στρώμα Σύνδεσης

Πίνακας 3. TCP/ IP

1.2.1 Επίπεδο Ζεύξης (Στρώμα Σύνδεσης)

Το επίπεδο- ζεύξης ή στρώμα σύνδεσης είναι το πεδίο δικτύωσης μιας σύνδεσης τοπικού δικτύου στην οποία ένας συνδρομητής είναι συνδεδεμένος. Αυτό ονομάζεται link [ζεύξη - σύνδεση] στην ορολογία του Ιντερνέτ. Αυτό είναι το χαμηλότερης στάθμης στοιχείο των πρωτοκόλλων του Ιντερνέτ, καθώς το TCP/IP έχει σχεδιασθεί να είναι ανεξάρτητο από το μηχάνημα - hardware . Σαν αποτέλεσμα, το TCP/IP είναι πάνω από σχεδόν οποιαδήποτε τεχνολογία υλικών δικτύωσης που υπάρχει.

Το επίπεδο ζεύξης χρησιμοποιείται για να μεταφέρει πακέτα μεταξύ διασυνδέσεων του διαδικτύου δυο συνδρομητών στην ίδια ζεύξη. Η διαδικασία εκπομπής και λήψης πακέτων σε μια ζεύξη μπορεί να ελεγχθεί και στη συσκευή οδήγησης του λογισμικού - software για την κάρτα δικτύου, καθώς και στο ενδιάμεσο λογισμικό - firmware ή σε ειδικά ολοκληρωμένα κυκλώματα.

Αυτά θα εκτελέσουν λειτουργίες δεδομένων ζεύξης [data link] όπως να προσθέσουν επικεφαλίδα πακέτου [packet header] να το προετοιμάσουν για εκπομπή, και μετά να εκπέμψουν το πλαίσιο μέσω ενός φυσικού μέσου [physical medium].

Το μοντέλο TCP/IP περιλαμβάνει προδιαγραφές για την ερμηνεία των μεθόδων διευθυνσιοδότησης του δικτύου που χρησιμοποιούνται στο πρωτόκολλο του ιντερνέτ για τη διευθυνσιοδότηση της ζεύξης δεδομένων [data link] , όπως είναι το μέσο ελέγχου πρόσβασης media access control [MAC] , πάντως όλες οι άλλες πτυχές κάτω από αυτό το επίπεδο που υποτίθεται ότι υπάρχουν στο επίπεδο ζεύξης, αλλά δεν καθορίζονται ρητά.

Το επίπεδο ζεύξης είναι επίσης το επίπεδο όπου τα πακέτα μπορεί να επιλεγούν να σταλούν σε ένα εικονικό ιδιωτικό δίκτυο (VPN) ή άλλη σήραγγα [κανάλι] δικτύωσης.
Σ'αυτό το σενάριο τα δεδομένα [data] του επιπέδου ζεύξης μπορεί να θεωρηθούν δεδομένα εφαρμογής που περνάνε μια άλλη συγκεκριμενοποίηση στη στοίβα του IP για εκπομπή ή λήψη άλλης σύνδεσης IP. Τέτοια σύνδεση, ή εικονική ζεύξη, μπορεί να εγκατασταθεί με ένα πρωτόκολλο μεταφοράς ή ακόμη με ένα πρωτόκολλο πεδίου εφαρμογής που χρησιμεύει σαν σήραγγα [tunnel]στο επίπεδο ζεύξης [Link Layer] της στοίβας του πρωτοκόλλου. Έτσι, το μοντέλο TCP/IP δεν υπαγορεύει μια αυστηρή ιεραρχικά ενθυλακωμένη ακολουθία.

1.2.2 Επίπεδο Διαδικτύου (IP)

Το Επίπεδο Διαδικτύου (Internet Layer) λύνει το πρόβλημα της αποστολής πακέτων σε ένα ή περισσότερα κυκλώματα .Η διαδικτύωση απαιτεί την αποστολή πληροφοριών από το προερχόμενο κύκλωμα στο κύκλωμα προορισμού. Αυτή η διαδικασία λέγεται routing.[δρομολόγηση].

Το πρωτόκολλο ιντερνέτ εκτελεί δύο βασικές λειτουργίες :

- ταυτοποίηση και διευθυνσιοδότηση : Αυτή επιτυγχάνεται με ένα σύστημα ιεραρχικής διευθυνσιοδότησης [IP address]
- δρομολόγηση πακέτων: Αυτό είναι το βασικό καθήκον της παραλαβής πακέτων δεδομένων[datagrams] από την πηγή προς τον προορισμό με την αποστολή τους στον επόμενο κόμβο του δικτύου [δρομολογητή] που είναι ποιο κοντά στον τελικό προορισμό.

Το IP μπορεί να μεταφέρει πληροφορίες από αριθμό διαφορετικών πρωτοκόλλων ανωτέρου στρώματος[upper layer protocols].Αυτά τα

πρωτόκολλα αναγνωρίζονται το καθένα από ένα μοναδικό αριθμό πρωτοκόλλου για παράδειγμα, Internet Control Message Protocol [ICMP] και Internet Group Management Protocol [IGMP] είναι τα πρωτόκολλα 1 και 2 αντίστοιχα .

Κάποια από τα πρωτόκολλα που μεταφέρονται από το IP ,όπως το ICMP [που χρησιμοποιείται για την εκπομπή διαγνωστικών πληροφοριών για την εκπομπή του IP και το IGMP [που χρησιμοποιείται για τη διαχείριση πληροφοριών IP Multicast] στρωματοποιούνται στην κορυφή του IP αλλά εκτελούν λειτουργίες διασυνεργασίας .

1.2.3 Επίπεδο-Στρώμα Μεταφοράς

Οι αρμοδιότητες του στρώματος μεταφοράς περιλαμβάνουν δυνατότητες μεταφοράς μηνυμάτων από άκρη σε άκρη ανεξάρτητα από το υποκείμενο δίκτυο, μαζί με έλεγχο λαθών, κατάτμηση, έλεγχο ροής, έλεγχο συμφόρησης, και εφαρμογή διευθυνσιοποίησης [αριθμοί θυρών].

Η από-άκρη-σε-άκρη εκπομπή μηνύματος ή οι εφαρμογές σύνδεσης στο στρώμα μεταφοράς μπορούν να κατηγοριοποιηθούν σαν προσανατολισμένες στη σύνδεση ή συνδεσμοστραφείς [connection –oriented], που υλοποιούνται στο πρωτόκολλο ελέγχου εκπομπής Transmission Control Protocol [TCP], ή χωρίς σύνδεση[connectionless], που υλοποιούνται στο User Datagram Protocol [UDP].

Το στρώμα μεταφοράς μπορεί να θεωρηθεί σαν ένας μηχανισμός μεταφοράς, δηλαδή ένα όχημα με την ευθύνη να βεβαιώσει ότι τα περιεχόμενά του [επιβάτες/ αγαθά] θα φθάσουν στον προορισμό τους ασφαλώς και σώα , εκτός αν ένα άλλο στρώμα πρωτοκόλλου είναι υπεύθυνο για την ασφαλή διανομή.

Το Στρώμα [επίπεδο] μεταφοράς παρέχει την υπηρεσία της σύνδεσης εφαρμογών με την χρήση θυρών υπηρέτησης [service ports]. Επειδή το IP

παρέχει την καλύτερη δυνατή διανομή, το στρώμα μεταφοράς είναι το πρώτο στρώμα του TCP/IP που προσφέρει αξιοπιστία. Το IP μπορεί να τρέξει πάνω σε ένα αξιόπιστο πρωτόκολλο ζεύξης πληροφοριών όπως το πρωτόκολλο υψηλής στάθμης έλεγχος πληροφοριών ζεύξης - High-Level Data Link Control [HDLC]. Πρωτόκολλα πάνω από τη μεταφορά όπως το RPC, μπορούν επίσης να προσφέρουν αξιοπιστία.

Για παράδειγμα το Transmission Control Protocol [TCP] πρωτόκολλο ελέγχου εκπομπής είναι προσανατολισμένο στη σύνδεση, και διευθύνει πολυάριθμα ζητήματα αξιοπιστίας για να παρέχει ένα αξιόπιστο byte stream.

- τα δεδομένα φτάνουν στη σειρά
- τα δεδομένα έχουν ελάχιστα λάθη [δηλ. ακρίβεια]
- αντίγραφο δεδομένων απορρίπτεται
- χαμένα/ απορριπτόμενα πακέτα επανεκπέμπονται
- περιλαμβάνει έλεγχο συμφόρησης κυκλοφορίας

Το νεότερο Stream Control Transmission Protocol [SCTP] πρωτόκολλο ελέγχου ροής εκπομπής είναι επίσης ένας αξιόπιστος , connection –oriented μηχανισμός μεταφοράς.

Είναι Message-stream-oriented , όχι byte-stream-oriented όπως το TCP και παρέχει πολλαπλές ροές[streams] πολυπλεγμένες πάνω σε μία σύνδεση. Παρέχει επίσης πολυεπιστρέφουσα υποστήριξη [multi-homing] στην οποία το τέλος μιας σύνδεσης μπορεί να παρουσιασθεί με πολλαπλή διεύθυνση IP [που αντιπροσωπεύει πολλαπλές φυσικές διεπαφές] έτσι ώστε αν μία αποτύχει η σύνδεση δεν διακόπτεται. Αρχικά είχε αναπτυχθεί για εφαρμογές της τηλεφωνίας [για μεταφορά του SS7 πάνω στο IP], αλλά μπορεί να χρησιμοποιηθεί και σε άλλες εφαρμογές.

Το πρωτόκολλο User Datagram [πακέτα δεδομένων χρήστη] είναι ένα χωρίς σύνδεση πρωτόκολλο datagram. Σαν το IP , είναι ένα σχετικά «αναξιόπιστο» πρωτόκολλο. Αξιοπιστία επιτυγχάνεται με ανίχνευση λαθών με τη χρήση ενός του αδύνατου αλγόριθμου checksum. Το UDP τυπικά χρησιμοποιείται

σε εφαρμογές όπως media ροής [audio, video, Voice over IP κλπ] όπου η έγκαιρη άφιξη είναι ποιο σημαντική από την αξιοπιστία, ή σε απλές εφαρμογές ερώτησης / απάντησης όπως οι αναζητήσεις DNS , όπου η επιβάρυνση της δημιουργίας μιας αξιόπιστης σύνδεσης είναι δυσανάλογα μεγάλη. Το πρωτόκολλο real- time Transport [RTP] είναι πρωτόκολλο πακέτων δεδομένων σχεδιασμένο για πληροφορίες πραγματικού χρόνου όπως η ροή audio και video.

TCP καιUDP χρησιμοποιούνται για την εκτέλεση ποικιλίας υψηλοτέρου επιπέδου εφαρμογών . Το κατάλληλο πρωτόκολλο μεταφοράς επιλέγεται με βάση την εφαρμογή πρωτοκόλλου υψηλοτέρου επιπέδου. Για παράδειγμα, το File Transfer Protocol [πρωτόκολλο μεταφοράς φακέλου] αναμένει μια αξιόπιστη σύνδεση, αλλά το Network File System [NFS] σύστημα φακέλου δικτύου υποθέτει ότι το δευτερεύον πρωτόκολλο Remote Procedure Call [διαδικασίας απομακρυσμένης κλήσης], όχι μεταφοράς, θα εγγυηθεί αξιόπιστη μεταφορά. Άλλες εφαρμογές , όπως το VoIP, μπορεί να επιτρέπουν κάποιες απώλειες πακέτων, αλλά όχι την ανακατάταξη ή καθυστέρηση που θα μπορούσε να προκαλέσει επανεκπομπή .

Οι εφαρμογές σε κάθε δεδομένη διεύθυνση δικτύου διαχωρίζονται από την πόρτα TCP ή UDP. Κατά συνθήκη, κάποιες καλά γνωστές πόρτες συνδέονται με ειδικές εφαρμογές. [λίστα των αριθμών θυρών TCP και UDP]

1.2.4 Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής αναφέρεται στα πρωτόκολλα υψηλότερης στάθμης που χρησιμοποιούνται από τις περισσότερες εφαρμογές στην επικοινωνία δικτύου.

Παραδείγματα από πρωτόκολλα επιπέδου εφαρμογής περιλαμβάνουν το File Transfer Protocol [FTP] και το Simple Mail Transfer Protocol [SMTP]

Πληροφορίες κωδικοποιημένες ανάλογα με τα πρωτόκολλα του επιπέδου

εφαρμογής ενθυλακώνονται σε ένα ή ενίοτε περισσότερα πρωτόκολλα επιπέδου μεταφοράς [όπως το Transmission Control {TCP} ή το User Datagram Protocol {UDP}],τα οποία με τη σειρά τους χρησιμοποιούν πρωτόκολλα κατωτέρου επιπέδου με αποτέλεσμα την πραγματική μεταφορά δεδομένων .

Αφού το IP stack δεν καθορίζει στρώματα μεταξύ των επιπέδων εφαρμογής και μεταφοράς, το επίπεδο εφαρμογής πρέπει να περιλαμβάνει οποιαδήποτε πρωτόκολλα που λειτουργούν σαν παρουσίαση του OSI και πρωτοκόλλων στρώματος συνόδου.

Τα πρωτόκολλα του επιπέδου[στρώματος] εφαρμογής χρησιμοποιούν τα πρωτόκολλα του επιπέδου μεταφοράς [και κατώτερης τάξης] σαν «black boxes» που παρέχουν μια σταθερή σύνδεση με την οποία επικοινωνεί σε όλο το δίκτυο, αν και οι εφαρμογές συνήθως είναι ενήμερες για τις βασικές ιδιότητες της σύνδεσης του επιπέδου μεταφοράς όπως οι end point IP addresses [διευθύνσεις IP τελικού σημείου] και τους αριθμούς θυρών [port numbers].όπως σημειώθηκε πιο πάνω, τα επίπεδα [στρώματα] δεν καθορίζονται καθαρά απαραίτητα στην ακολουθία του πρωτοκόλλου του διαδικτύου. Τα πρωτόκολλα επιπέδου εφαρμογής είναι ως επί το πλείστον συνδεδεμένα με εφαρμογές του client- server, και τα κοινά servers έχουν ειδικές πόρτες που τους έχουν ανατεθεί από την IANA : η HTTP έχει την πόρτα 80, η Telnet έχει την πόρτα 23,κλπ. Οι πελάτες [clients] από την άλλη, τείνουν να χρησιμοποιούν εφήμερες πόρτες [ephemeral ports], δηλ. αριθμό θυρών που αποδίδεται τυχαία από μια σειρά που προορίζεται γι'αυτό.

Το επίπεδο μεταφοράς και τα μικρότερης σημασίας στρώματα είναι σε μεγάλο βαθμό αδιάφορα για τις ιδιαιτερότητες των πρωτοκόλλων του στρώματος εφαρμογής.

Οι routers και switches δεν «ψάχνουν» την επικοινωνία για να δουν τι πρωτόκολλο εφαρμογής αντιπροσωπεύει, αλλά μάλλον απλά παρέχουν έναν αγωγό γι'αυτά . πάντως, κάποιες εφαρμογές firewall και bandwidth throttling [τείχος προστασίας και ρύθμιση εύρους ζώνης] πράγματι προσπαθούν να

καθορίσουν τι βρίσκεται μέσα, όπως το Resource Reservation Protocol [RSVP].Είναι επίσης μερικές φορές απαραίτητο για τις διευκολύνσεις Network Address Translation [NAT] [ερμηνεία διεύθυνσης δικτύου] να λαμβάνονται υπ'όψιν οι ανάγκες των πρωτοκόλλων κάποιου ιδιαίτερου στρώματος εφαρμογής.[η NAT επιτρέπει στους συνδρομητές σε ιδιωτικά δίκτυα να επικοινωνούν με τον έξω κόσμο με μία ορατή διεύθυνση IP με τη χρήση προώθησης θυρών [port forwarding], και αυτό είναι ένα ευρέως διαδεδομένο χαρακτηριστικό των σύγχρονων οικιακών broadband routers.

Αν και το διαδίκτυο αναπτύχθηκε γρήγορα ως δίκτυο δεδομένων η χρήση της φωνής πάνω από αυτό καθυστέρησε αρκετά. Αυτό δεν έχει να κάνει τόσο με την ικανότητα μεταφοράς φωνής μέσω διαδικτύου ίσης η ακόμα και καλύτερης ποιότητας φωνής σε σχέση με το προϋπάρχον τηλεφωνικό δίκτυο αλλά κυρίως με **το «πρόβλημα» και την σημασία της σηματοδοσίας στις φωνητικές υπηρεσίες**.

2.1 Πρωτόκολλα σηματοδοσίας στο VoIP

Τα δύο επικρατέστερα πρωτόκολλα σηματοδοσίας στην διαδικτυακή τηλεφωνία (VoIP) είναι το SIP (**Session Initiation Protocol**) και το H.323.

2.1.1 H.323

Το H.323 αποτελεί μια στοίβα πρωτοκόλλων στη ουσία .Σχεδιάστηκε από την ITU (International Telecommunication Union) και η πρώτη του εκδοχή παρουσιάστηκε τον Νοέμβριο του 1996 δίνοντας έμφαση στην βίντεο-σύσκεψη σε ένα τοπικό δίκτυο (LAN). Έχει δανειστεί πολλά χαρακτηριστικά από το H.320 που ήταν σχεδιασμένο για το **ISDN**. Με την πάροδο του χρόνου έχουν γίνει βελτιώσεις και έχουν βγει νέες εκδοχές του με τελευταία την "H.323v7" που δημοσιεύτηκε το Νοέμβριο του 2009.

Πρωτόκολλο	**Περιγραφή**
H.225.0 Εγγραφή, Είσοδος και κατάσταση. (Registration, Admission and Status) **(RAS)**	Το οποίο χρησιμοποιείται μεταξύ ενός H.323 τερματικού και ενός εξυπηρετητή Θυρωρού(Gatekeeper) για να παρέχει ανάλυση διεύθυνσης και υπηρεσίες ελέγχου εισόδου .
H.225.0 Σηματοδοσία Κλήσης .(Call Signaling)	• το οποίο χρησιμοποιείται μεταξύ δύο οποιοσδήποτε H.323 οντοτήτων με σκοπό να εγκαθιδρύσουν επικοινωνία
H.245 Πρωτόκολλο ελέγχου για πολυμεσικές επικοινωνίες	• το οποίο περιγράφει τα μηνύματα και τις διαδικασίες που χρησιμοποιούνται για ανταλλαγή ικανοτήτων , άνοιγμα και κλείσιμο λογικών καναλιών για φωνή , βίντεο και δεδομένα, έλεγχο και ενδείξεις.
Πρωτόκολλο μεταφοράς Πραγματικού χρόνου (Real-time Transport	• το οποίο χρησιμοποιείται για αποστολή και αποδοχή πολυμεσικών πληροφοριών (φωνή , βίντεο , κείμενο) μεταξύ δύο οποιονδήποτε οντοτήτων .

Protocol (**RTP**)),	
Συμπληρωματικά Πρωτόκολλα	
• **H.235**	Περιγράφει την ασφάλεια μέσα στο H.323, περιλαμβάνοντας ασφάλεια για σηματοδοσία αλλά και πολυμέσων
• **H.239**	Περιγράφει τη χρήση διπλής ροής σε βιντεοδιασκέψεις , συνήθως ένα για ζωντανό βίντεο και το άλλο για εικόνες.
• **H.450**	Περιγράφει διάφορες συμπληρωματικές υπηρεσίες.
• **H.460**	Περιγράφει προαιρετικές επεκτάσεις που μπορούν να εφαρμοστούν από ένα τερματικό ή ένα εξυπηρετητή Θυρωρού(Gatekeeper) , περιλαμβάνοντας τις ITU-T υποδείξεις H.460.17,
H.460.18, and **H.460.19**	Για μετάφραση διαδικτυακών διευθύνσεων (Network address translation) (NAT) / Πέρασμα Τείχους ασφαλείας Firewall (FW) traversal.

Πίνακας 4. Στοίβα πρωτοκόλλων του H.323

2.1.2 Πρωτόκολλο Αρχικοποίησης Συνόδου SIP (Session Initiation Protocol)

Το Πρωτόκολλο Αρχικοποίησης Συνόδου SIP (Session Initiation Protocol) είναι ένα πρωτόκολλο σηματοδοσίας που σχεδιάστηκε αρχικά από τον

Henning Schulzrinne και τον Mark Handley το 1996 και η τελευταία εκδοχή του είναι το RFC 3261 σχεδιασμένη από τον IETF(Internet Engineering Task Force) τον Ιούνιο του 2002. Το Νοέμβριο του 2000 αποδέχτηκε ως 3GPP (**3rd Generation Partnership Project) πρωτόκολλο σηματοδοσίας και ως μόνιμο-βασικό στοιχείο της** the IP Multimedia Subsystem (IMS) αρχιτεκτονικής για IP-βασισμένες πολυμεσικές υπηρεσίες σε κυψελωτά συστήματα καθιερώνοντας το κυρίαρχο πρωτόκολλο σηματοδοσίας στα τηλεπικοινωνιακά συστήματα επόμενης γενιάς .

Το SIP αποτελεί ένα από τα πρωτόκολλα του στρώματος εφαρμογής σχεδιασμένο να είναι ανεξάρτητο από το στρώμα μεταφοράς μπορεί να «τρέξει» σε Transmission Control Protocol (TCP), User Datagram Protocol (UDP), ή Stream Control Transmission Protocol (SCTP). Είναι επίσης, ένα πρωτόκολλο βασισμένο στο κείμενο(text-based) που έχει δανειστεί πολλά στοιχεία από το Hypertext Transfer Protocol (HTTP) και το Simple Mail Transfer Protocol (SMTP), καθιστώντας το πιο απλό στη διαχείριση πολυμεσικών εφαρμογών αλλά και στη δημιουργία νέων υπηρεσιών τηλεφωνίας.

Ποιό πολλές λεπτομέρειες θα δούμε στις παρακάτω ενότητες έτσι ώστε να γίνει κατανοητό το πρωτόκολλο και να προχωρήσουμε μετά στα θέματα ασφάλειας του που είναι και βασικό θέμα της πτυχιακής εργασίας.

2.2 Επισκόπηση της λειτουργικότητας του SIP

Το SIP είναι ένα πρωτόκολλο ελέγχου του στρώματος εφαρμογής (application layer) το οποίο μπορεί να δημιουργήσει, να μετατρέψει και να τερματίσει πολυμεσικές συνόδους τέτοιες όπως οι διαδικτυακές τηλεφωνικές κλήσεις (VoIP) και τηλεδιασκέψεις. Μπορεί επίσης να προσκαλέσει χρήστες να λάβουν μέρος σε ήδη υπάρχοντες συνόδους. Επιπλέον, εφαρμογές πολυμέσων μπορούν να προστεθούν ή να αφαιρεθούν από υπάρχοντες συνόδους.

Το SIP μπορεί να υποστηρίξει επανακατεύθυνση υπηρεσιών , ονομαστική απεικόνιση αλλά και προσωπική φορητότητα έτσι ώστε οι χρήστες να διατηρούν ένα μοναδικό εξωτερικά ορατό αριθμό ID – χαρακτηριστικό) ανεξάρτητα από την τοποθεσία του δικτύου τους.

Το SIP υποστηρίζει πέντε βασικές υπηρεσίες – λειτουργίες

Εντοπισμός χρήστη: προσδιορισμός του τελικού συστήματος του χρήστη που θα χρησιμοποιηθεί για την επικοινωνία

Διαθεσιμότητα χρήστη: προσδιορισμός της προθυμίας συμμετοχής του καλούμενου χρήστη στην επικοινωνία

Δυνατότητες χρήστη: προσδιορισμός των μέσων και των παραμέτρων τους των οποίων ο χρήστης μπορεί να χρησιμοποιήσει

Δημιουργία συνόδου: «κλήση», δημιουργία των παραμέτρων συνόδου μεταξύ όλων των χρηστών που συμμετέχουν

Διαχείριση συνόδου: περιλαμβάνει μεταφορά και τερματισμό των συνόδων , μετατροπή των παραμέτρων της συνόδου και επίκληση υπηρεσιών.

¨Όπως είναι φανερό από τα παραπάνω οι τερματικές συσκευές υποστηρίζουν ένα μεγάλο μέρος της απαιτούμενης λειτουργικότητας , δίνοντας έτσι την δυνατότητα ανάπτυξης νέων υπηρεσιών με βάση τον χρήστη.

Το SIP δεν παρέχει ολοκληρωμένες υπηρεσίες αλλά παρέχει τα αρχικά στοιχεία που απαιτούνται για την εφαρμογή διαφόρων υπηρεσιών. Για παράδειγμα το SIP μπορεί να εντοπίσει έναν χρήστη και να παραδώσει ένα αρχικό αντικείμενο στην προσωρινή τοποθεσία του. Εάν αυτό το αρχικό αντικείμενο χρησιμοποιείται για να παραδώσει μια περιγραφή συνόδου γραμμένη σε SDP για παράδειγμα, οι τερματικές συσκευές μπορούν να συμφωνήσουν στις παραμέτρους της συνόδου. Εάν τα ίδια αρχικά στοιχεία χρησιμοποιηθούν για να μεταφέρουν μια φωτογραφία του χρήστη που ξεκίνησε την κλήση ,όπως και στην περιγραφή της συνόδου, μια υπηρεσία σχετικά την ταυτότητα του χρήστη που ξεκίνησε την κλήση μπορεί εύκολα να

εφαρμοστεί. Όπως το παράδειγμα αυτό δείχνει ένα μοναδικό αρχικό στοιχείο μπορεί να χρησιμοποιηθεί για να παρέχει διαφορετικές υπηρεσίες.

Η φύση των υπηρεσιών που παρέχονται κάνουν το θέμα της ασφάλειας ύψιστης σημασίας . Για αυτό το λόγο το SIP παρέχει τεχνικές ασφάλειας οι οποίες περιλαμβάνουν : την αποτροπή της άρνηση υπηρεσίας (denial-of-service) την αυθεντικοποίηση , την προστασία ακεραιότητας , τη κρυπτογράφηση και υπηρεσίες ιδιωτικότητας.

Ακόμα , το SIP χρησιμοποιεί IPv4 αλλά και IPv6

2.3 Οι οντότητες του SIP

Οι οντότητες που συνθέτουν μια SIP αρχιτεκτονική είναι οι πράκτορες χρήστη (User Agents) και οι εξυπηρετητές (Servers).

Οι πράκτορες χρήστη (User Agents-UA) βρίσκονται στις τερματικές συσκευές των χρηστών ενός SIP δικτύου και λειτουργούν εκ μέρους τους, διεκπεραιώνοντας τα αιτήματα τους. Κάθε UA διαφοροποιείται , με βάση τις λειτουργίες που εκτελεί, στα ακόλουθα μέρη:

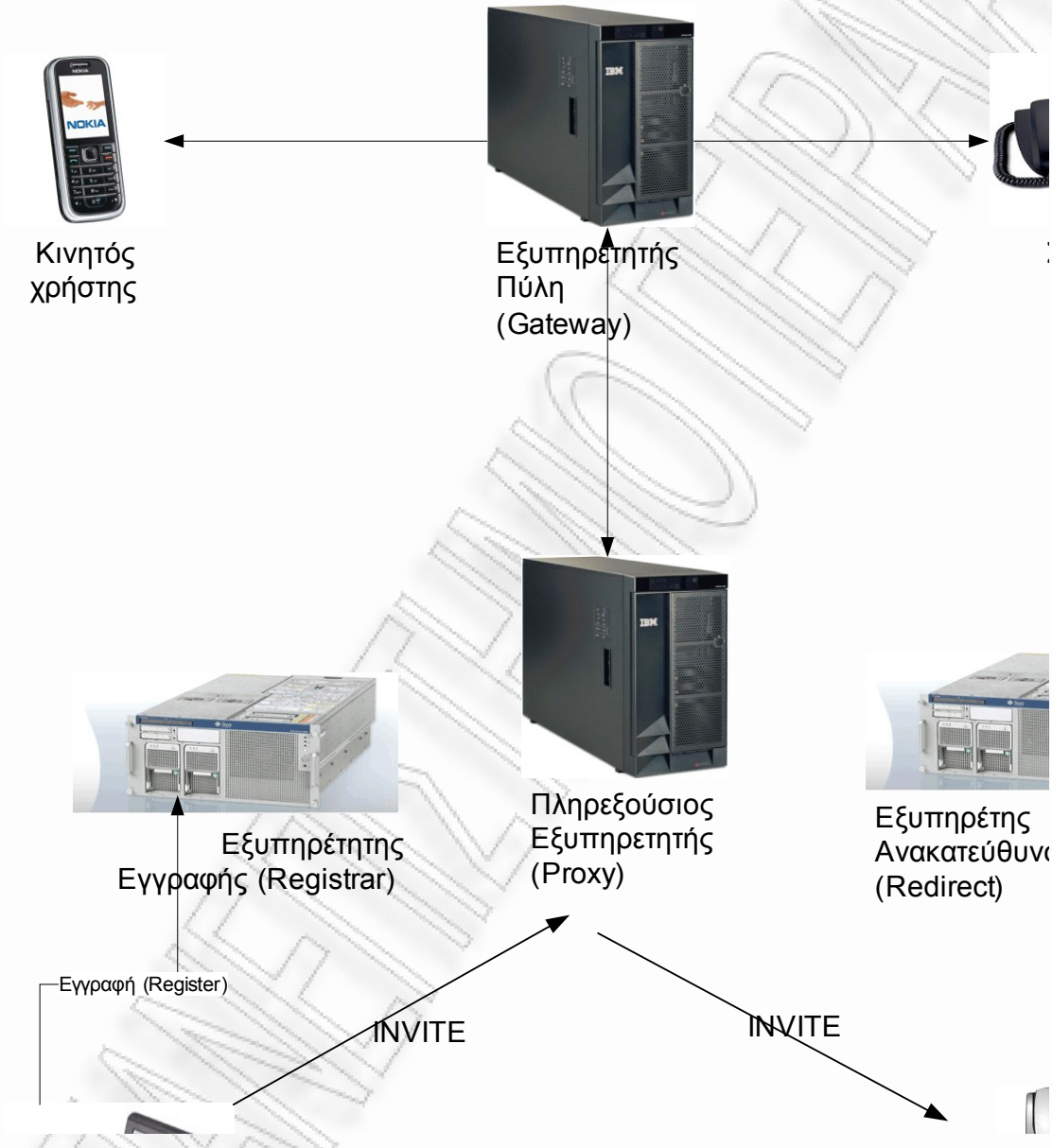
- UA Πελάτης (Client) (UAC): Ο UAC είναι υπεύθυνος για τη δημιουργία των αιτημάτων του χρήστη.
- UA Εξυπηρέτης (Server) (UAS): Ο UAS είναι υπεύθυνος για την επεξεργασία των εισερχόμενων αιτημάτων δημιουργώντας την κατάλληλη απόκριση για κάθε αίτηση που λαμβάνει.

Θα πρέπει να αναφερθεί ότι και οι δύο προαναφερόμενες οντότητες ενσωματώνονται στη SIP συσκευή τελικού χρήστη.

Οι εξυπηρετητές στην αρχιτεκτονική του SIP αποτελούν ενδιάμεσες οντότητες (διαμεσολαβητές) που έχουν σκοπό να παρέχουν επιπρόσθετες υπηρεσίες για την παροχή ολοκληρωμένων λύσεων και υπηρεσιών τηλεφωνίας στο διαδίκτυο. Οι εξυπηρετητές που αξιοποιούνται στην αρχιτεκτονική του SIP είναι οι παρακάτω :

- Εξυπηρετητής Εγγραφής (Registrar)

- Πληρεξούσιος Εξυπηρετητής (Proxy)
- Εξυπηρετητής Ανακατεύθυνσης (Redirect)
- Εξυπηρετητής Πύλη (Gateway)



Σχήμα 1 . Σχέδιο της αρχιτεκτονικής SIP

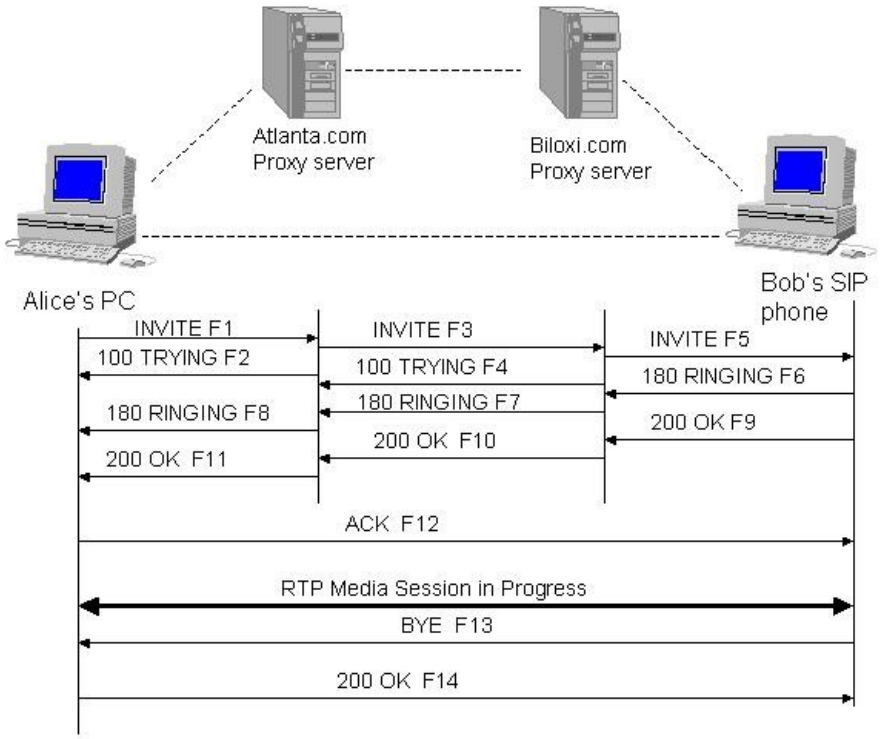
2.4 Πρωτόκολλα πολυμεσικής επικοινωνίας εκτός του SIP

Το SIP δεν αποτελεί ένα ενοποιημένο τηλεπικοινωνιακό σύστημα αλλά ένα στοιχείο το οποίο μαζί με άλλα τηλεπικοινωνιακά πρωτόκολλα του IETF μπορεί να συνθέσει μια ολοκληρωμένη αρχιτεκτονική πολυμεσικής επικοινωνίας.

Μια τέτοια αρχιτεκτονική θα περιλαμβάνει πρωτόκολλα όπως : το πρωτόκολλο μεταφοράς πραγματικού – χρόνου (Real-time Transport Protocol (**RTP**))(RFC 1889 , http://www.ietf.org/rfc/rfc1889.txt) για τη μετάδοση δεδομένων πραγματικού χρόνου και για παροχή αποτελεσμάτων για την ποιότητα υπηρεσίας (**QoS**), επίσης το Πρωτόκολλο Ροής Πραγματικού Χρόνου (Real-Time streaming protocol (**RTSP**)) (RFC 2326 , http://www.ietf.org/rfc/rfc2326.txt) για τον έλεγχο ορθής παράδοσης των πολυμέσων ροής (media streaming), ακόμη το Πρωτόκολλο Ελέγχου των Πολυμεσικών Εξόδων (*Media Gateway Control Protocol* (**MEGACO**)) (RFC 3015) για τον έλεγχο των θυρών διαφυγής (G/Ws) στο παραδοσιακό τηλεφωνικό δίκτυο PSTN, αλλά και το Πρωτόκολλο Περιγραφής Συνόδου (Session Description Protocol (**SDP**)) (RFC 2327 [1]) για την περιγραφή των πολυμεσικών συνόδων.

Για αυτό το SIP θα πρέπει να χρησιμοποιείται σε συνδυασμό των άλλων πρωτοκόλλων με σκοπό να παρέχει ολοκληρωμένες υπηρεσίες στους χρήστες. Όμως , οι βασικές λειτουργίες και χρήσεις του SIP δεν εξαρτώνται από τα άλλα πρωτόκολλα που συνδυάζει για την παροχή των ολοκληρωμένων τηλεπικοινωνιακών υπηρεσιών.

2.5 Προεσκόπιση της Λειτουργίας του SIP



Σχήμα 2. Παράδειγμα του SIP τραπεζοειδούς (SIP trapezoid)

2.5.1 Παράδειγμα SIP κλήσης

Για να γίνει κατανοητή η λειτουργία του πρωτοκόλλου θα εξετάσουμε ένα παράδειγμα.

Στο σχήμα 2 έχουμε ένα τυπικό παράδειγμα μιας ανταλλαγής SIP μηνυμάτων μεταξύ δύο χρηστών του Bob και της Alice. (Κάθε μήνυμα έχει το γράμμα «F» και έναν αριθμό που το χαρακτηρίζει)

Στο παράδειγμα η Alice χρησιμοποιεί ένα τηλέφωνο λογισμικού(soft phone) στον προσωπικό της υπολογιστή ενώ ο Bob χρησιμοποιεί ένα τηλέφωνο SIP μέσω του διαδικτύου . Επίσης, υπάρχουν δύο πληρεξούσιοι εξυπηρετητές (proxy servers) που λειτουργούν για λογαριασμό του Bob και της Alice για να διευκολύνουν την δημιουργία συνόδου. Αυτή η τυπική διαδικασία συχνά αναφέρεται και ως «SIP τραπεζοειδής» ("SIP trapezoid") όπως φαίνεται από το γεωμετρικό σχήμα των διακεκομμένων γραμμών μεταξύ των χρηστών και των εξυπηρετητών τους του παραπάνω σχήματος .

Η Alice καλεί τον Bob χρησιμοποιώντας την SIP αναγνωριστική ταυτότητα , ένα τύπο ομοιόμορφης πηγής αναγνωριστικού (Uniform Resource Identifier (URI)) που ονομάζεται SIP URI. Έχει μια παρόμοια φόρμα όπως και μια διεύθυνση ηλεκτρονικού ταχυδρομείου (email address) . Στην περίπτωσή μας είναι sip:bob@biloxi.com, όπου το biloxi.com είναι ο τομέας (domain) του SIP παρόχου υπηρεσιών που έχει ο Bob . Η Alice έχει την SIP URI sip:alice@atlanta.com. αντίστοιχα το atlanta.com είναι ο τομέας (domain) του SIP παρόχου υπηρεσιών που έχει η Alice. Η Alice μπορεί να έχει πληκτρολογήσει την SIP URI του Bob ή να έχει κλικάρει σε μια υπερσύνδεση (hyperlink) ή σε μια καταχώρηση σε ένα κατάλογο διευθύνσεων για να ξεκινήσει την κλήση. Το SIP επίσης παρέχει ένα ασφαλές URI που ονομάζεται SIPS URI ένα παράδειγμα θα μπορούσε να είναι το : sips:bob@biloxi.com .Μια κλήση που θα γινόταν σε ένα SIPS URI εγγυάται ότι η ασφαλής κρυπτογραφημένη μεταφορά (TLS) χρησιμοποιείται για να μεταφέρει τα SIP μηνύματα από τον χρήστη που ξεκίνησε την κλήση έως τον τομέα(domain) του καλούμενου .Από εκεί και πέρα τα μηνύματα θα σταλθούν στον καλούμενο χρήστη σύμφωνα με τους μηχανισμούς ασφαλείας που εξαρτούνται από την πολιτική που εφαρμόζεται στον τομέα του όπως θα δούμε και σε παρακάτω κεφάλαιο.

2.5.2 Τα μηνύματα στο SIP

Το SIP βασίζεται σε ένα μοντέλο ανταλλαγής-διεξαγωγής αιτήσεων/αποκρίσεων παρόμοιο με το HTTP . Κάθε διεξαγωγή αποτελείται από μια αίτηση που επικαλείται μια συγκεκριμένη μέθοδο ή λειτουργία στον εξυπηρετητή και τουλάχιστον μια απάντηση- απόκριση.

2.5.2.1 SIP Requests αιτήσεις

Στο παράδειγμά μας η διεξαγωγή ξεκινάει με το τηλέφωνο λογισμικού να στέλνει μια αίτηση πρόσκλησης (INVITE) στην SIP URI του Bob. «Η πρόσκληση (INVITE) αποτελεί ένα παράδειγμα μιας SIP μεθόδου που καθορίζει τις ενέργειες που η αιτούσα Alice θέλει ο Bob να εκτελέσει - κάνει . Η αίτηση πρόσκλησης (INVITE) περιέχει έναν αριθμό πεδίων επικεφαλίδων (Headers) . Τα πεδία επικεφαλίδων αποτελούν συγκεκριμένες ιδιότητες που παρέχουν περαιτέρω πληροφορίες σχετικά με το μήνυμα.

Αυτές που υπάρχουν σε μια αίτηση πρόσκλησης (INVITE) περιλαμβάνουν : ένα μοναδικό αναγνωριστικό για την κλήση , μια διεύθυνση προορισμού , την διεύθυνση του χρήστη που ξεκίνησε την κλήση δηλαδή της Alice αλλά και πληροφορίες σχετικά με τον τύπο της συνόδου που θέλει η Alice να εγκαθιδρύσει με τον Bob.

Η πρόσκληση (INVITE) F1 του σχήματος θα είναι κάπως έτσι :

```
 INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
Cess: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
(Alice’s SDP not shown)
```

Η πρώτη γραμμή του κείμενο-κωδικοποιημένου μηνύματος περιέχει το όνομα της μεθόδου δηλαδή πρόσκληση (INVITE). Οι γραμμές που ακολουθούν αποτελούν μια λίστα των πεδίων των επικεφαλίδων οι οποίες θα περιγραφούν παρακάτω:

- Το «Via» (Δια μέσω) περιέχει την διεύθυνση (pc33.atlanta.com) στην οποία η Alice περιμένει να λάβει απάντηση στην αίτηση που έστειλε. Επιπλέον , περιέχει τμηματικές (branch) παραμέτρους που αναγνωρίζουν την διεξαγωγή της κλήσης αυτής.
- Το «To»(Προς) περιέχει τη προβολή του ονόματος Bob καθώς και το SIP ή SIPS URI αναγνωριστικό (sip:bob@biloxi.com) προς το οποίο η αίτηση έχει αρχικά κατευθυνθεί .
- Το «From» (Από) περιέχει επίσης τη προβολή του ονόματος Alice καθώς και το SIP ή SIPS URI αναγνωριστικό (sip:alice@atlanta.com) το οποίο υποδεικνύει τον χρήστη που αρχικά έστειλε την αίτηση. Περιέχεται επίσης μια παράμετρος της ετικέτας (tag) που περιέχει μια τυχαία ακολουθία αριθμών (1928301774) που έχει προστεθεί από το τηλέφωνο λογισμικού και χρησιμοποιείται για αναγνωριστικό σκοπό
- Το «Call-ID» (αναγνωριστικό κλήσης) περιέχει ένα μοναδικό αναγνωριστικό για αυτήν την κλήση , το οποίο δημιουργήθηκε από ένα συνδυασμό μιας τυχαίας ακολουθίας λεξαρίθμων και το όνομα ή την IP διεύθυνση του τηλεφώνου λογισμικού (a84b4c76e66710@pc33.atlanta.com) .

Ο συνδυασμός των παραπάνω ετικετών προσδιορίζει μια άμεση σχέση μεταξύ των δύο χρηστών Alice και Bob και αναφέρεται ως διάλογος.

- Το «Cess ή Command Sequence» (Ακολουθία εντολής)περιέχει έναν ακέραιο αριθμό και το όνομα της μεθόδου (INVITE). Ο αριθμός αυτός είναι αύξοντας για κάθε νέα αίτηση μέσα σε ένα διάλογο και είναι ένας παραδοσιακός αριθμός ακολουθίας.

- Το «`Contact`» (Επαφή)περιέχει ένα SIP ή SIPS URI αναγνωριστικό που αντιπροσωπεύει μια άμεση διαδρομή για την επικοινωνία με την Alice <sip:alice@pc33.atlanta.com>. Συνήθως αποτελείται από το όνομα χρήστη σε μια πλήρως επεξηγηματική του τομέα μορφή (FQDN). Αν και το FQDN προτιμάται πολλά τερματικά συστήματα δεν έχουν εγγεγραμμένα τα ονόματα των τομέων , για αυτό και οι IP διευθύνσεις επιτρέπονται. Ενώ το πεδίο της επικεφαλίδας «Via» δείχνει στις άλλες οντότητες που να στείλουν τις αποκρίσεις το πεδίο της επικεφαλίδας «Contact» δείχνει που να στείλουν τις μελλοντικές αιτήσεις.
- Το «Max-Forwards» (Μέγιστη προώθηση) στην τρίτη γραμμή , εξυπηρετεί στον περιορισμό του αριθμού των βημάτων τα οποία μια αίτηση μπορεί να κάνει στο δρόμο της για τον τελικό προορισμό. Αποτελείται από έναν ακέραιο (70 στην δική μας περίπτωση) που μειώνεται κατά ένα έπειτα από κάθε βήμα.
- Το «`Content-Type`» (Τύπος περιεχομένου) περιέχει μια περιγραφή του σώματος του μηνύματος(στο παράδειγμά μας δεν είναι εμφανής).
- Το «`Content-Length`» (Μέγεθος Περιεχομένου) περιέχει των αριθμό των Bytes (142) του σώματος του μηνύματος

Οι λεπτομέρειες τις συνόδου ,όπως το είδος των μέσων, οι κωδικοποιητές δεν περιγράφονται με τη χρήση του SIP . Αλλά όμως, το σώμα-κύριο μέρος ενός SIP μηνύματος περιέχει την περιγραφή της συνόδους κωδικοποιημένη με τη φόρμα κάποιου άλλου πρωτοκόλλου. ένα τέτοιο πρωτόκολλο είναι το Πρωτόκολλο Περιγραφής Συνόδου (**SDP**) . Το μήνυμα αυτού του πρωτοκόλλου (το οποίο δεν είναι εμφανές στο παράδειγμα μας) μεταφέρεται από το SIP με ένα τρόπο παρόμοιο με τον τρόπο που ένα μήνυμα ηλεκτρονικού ταχυδρομείου επισυνάπτει ένα ηλεκτρονικό έγγραφο , ή όπως μια ιστοσελίδα μεταφέρεται σε ένα HTTP μήνυμα.

Εφόσον, το τηλέφωνο λογισμικού δεν γνωρίζει την τοποθεσία του Bob ή του SIP εξυπηρετητή στον «biloxi.com» τομέα το τηλέφωνο λογισμικού στέλνει την πρόσκληση (INVITE) στον SIP εξυπηρετητή που εξυπηρετεί τον τομέα της

Alice «atlanta.com». Η διεύθυνση του εξυπηρετητή αυτού θα πρέπει να υπάρχει στο τηλέφωνο λογισμικού του χρήστη είτε έπειτα από κάποια δικιά του ή κάποιου τεχνικού χειροκίνητη προσθήκη είτε θα έχει ανακαλυφθεί αυτόματα με τη βοήθεια του πρωτοκόλλου DHCP .

2.5.2.2 SIP Response αποκρίσεις

Η απόκριση 100 (Trying)

Ο «atlanta.com» SIP εξυπηρετητής είναι ένας τύπος εξυπηρετητή γνωστός ως πληρεξούσιου εξυπηρετητή (proxy server). Ο πληρεξούσιος εξυπηρετητής (proxy server) παραλαμβάνει SIP αιτήσεις και τις προωθεί εκ μέρους των χρηστών που τις αιτήθηκαν. Στο παράδειγμά μας ο πληρεξούσιος εξυπηρετητής παραλαμβάνει την αίτηση πρόσκλησης (INVITE) και στέλνει στο τηλέφωνο λογισμικού της Alice την απόκριση : 100 (Trying) .

Η απόκριση 100 (Trying)δείχνει ότι ο πληρεξούσιος έλαβε την πρόσκληση και προσπαθεί εκ μέρους του αποστολέα να την δρομολογήσει στον τελικό παραλήπτη. Οι αποκρίσεις στο SIP χρησιμοποιούνε ένα τριψήφιο κωδικό ακολουθούμενο από μια περιγραφική φράση. Αυτή η απόκριση περιλαμβάνει τα ίδια στοιχεία των επικεφαλίδων «To», «From», «Call-ID», «Cess» και της τμηματικής (branch) παραμέτρου «Via» με την πρόσκληση (INVITE). Τα οποία επιτρέπουν το τηλέφωνο λογισμικού της Alice να συσχετίσει αυτήν την απόκριση με την σταλμένη πρόσκληση. Ο «atlanta.com» πληρεξούσιος εξυπηρετητής εντοπίζει τον πληρεξούσιο εξυπηρετητή «biloxi.com» με τη βοήθεια της υπηρεσίας ονόματος τομέα (DNS) . Έτσι, βρίσκει την IP διεύθυνση του ζητούμενου εξυπηρετητή και προωθεί την αίτηση πρόσκλησης (INVITE) εκεί . Όμως, πριν προωθήσει την αίτηση ο «atlanta.com» πληρεξούσιος προσθέτει ένα επιπλέον δεδομένο στο πεδίο της «Via» (Δια μέσω) επικεφαλίδας, το οποίο είναι η δική του διεύθυνση.

Ο πληρεξούσιος εξυπηρετητής «biloxi.com» παραλαμβάνει την πρόσκληση και απαντάει με μια 100 (Trying) απόκριση στον «atlanta.com» πληρεξούσιο επιβεβαιώνοντας έτσι ότι παρέλαβε την πρόσκληση και την επεξεργάζεται. Ο εξυπηρετητής συμβουλεύεται μια βάση δεδομένων που περιέχει την διεύθυνση του Bob. Έπειτα , προσθέτει στο πεδίο της επικεφαλίδας «Via» την διεύθυνση του και την προωθεί στο SIP τηλέφωνο του Bob.

Η απόκριση 180 (Ringing)

Το SIP τηλέφωνο του Bob παραλαμβάνει την πρόσκληση και τον ειδοποιεί για την εισερχόμενη κλήση της «Alice» έτσι ώστε να αποφασίσει εάν θα απαντήσει στην κλήση ή όχι. Έχουμε δηλαδή το χτύπημα της κλήσης του τηλεφώνου του Bob , το οποίο το δείχνει αυτό με την 180 (Ringing) απόκριση . Η οποία δρομολογείται πίσω στην «Alice» μέσω των πληρεξούσιων εξυπηρετητών οι οποίοι χρησιμοποιούν το πεδίο της επικεφαλίδας «Via» για να προσδιορίσουνε πού θα στείλουνε , αφαιρώντας την δικιά τους διεύθυνση καθώς προωθούν την απόκριση αυτή. Αυτό έχει ως αποτέλεσμα η απόκριση 180 (Ringing) να επιστρέφει στον χρήστη που ξεκίνησε την κλήση χωρίς την χρήση της υπηρεσίας ονόματος τομέα (DNS). Επίσης, κάθε πληρεξούσιος εξυπηρετητής που βλέπει την πρόσκληση θα δει επίσης και όλες τις αποκρίσεις στην πρόσκληση αυτή.
Όταν το λογισμικό τηλέφωνο λάβει την απόκριση 180 (Ringing) μεταφέρει την πληροφορία αυτή μέσω ενός τόνου κλήσης ή με την εμφάνιση ενός μηνύματος στην οθόνη της Alice.

Η απόκριση 200 (OK)

Στο παράδειγμά μας ο Bob απαντάει στην κλήση έτσι όταν σηκώσει το ακουστικό το τηλέφωνό του στέλνει μια 200 (OK) απόκριση που φανερώνει ότι η κλήση έχει απαντηθεί.

Η απόκριση 200 (OK) περιέχει στο σώμα του μηνύματος, με τη φόρμα του SDP, περιγραφή για τον τύπο της συνόδου που ο Bob είναι πρόθυμος να εγκαθιδρύσει με την Alice . Ως αποτέλεσμα υπάρχει μια ανταλλαγή SDP μηνυμάτων δύο φάσεων: Η Alice στέλνει ένα στον Bob και ο Bob ένα στην Alice. Αυτή η ανταλλαγή παρέχει βασικές διαπραγματευτικές ιδιότητες και βασίζεται στο απλό μοντέλο προσφοράς/απάντησης του πρωτοκόλλου SDP.
Εάν ο Bob δεν απαντούσε στην κλήση ή ήταν απασχολημένος μια διαφορετική απόκριση θα είχε σταλθεί αντί της 200 (OK) που θα είχε ως αποτέλεσμα να μην δημιουργηθεί η σύνοδος .
Η σύνταξη του 200 (OK) μηνύματος (F9 στο σχήμα)θα είναι η παρακάτω :

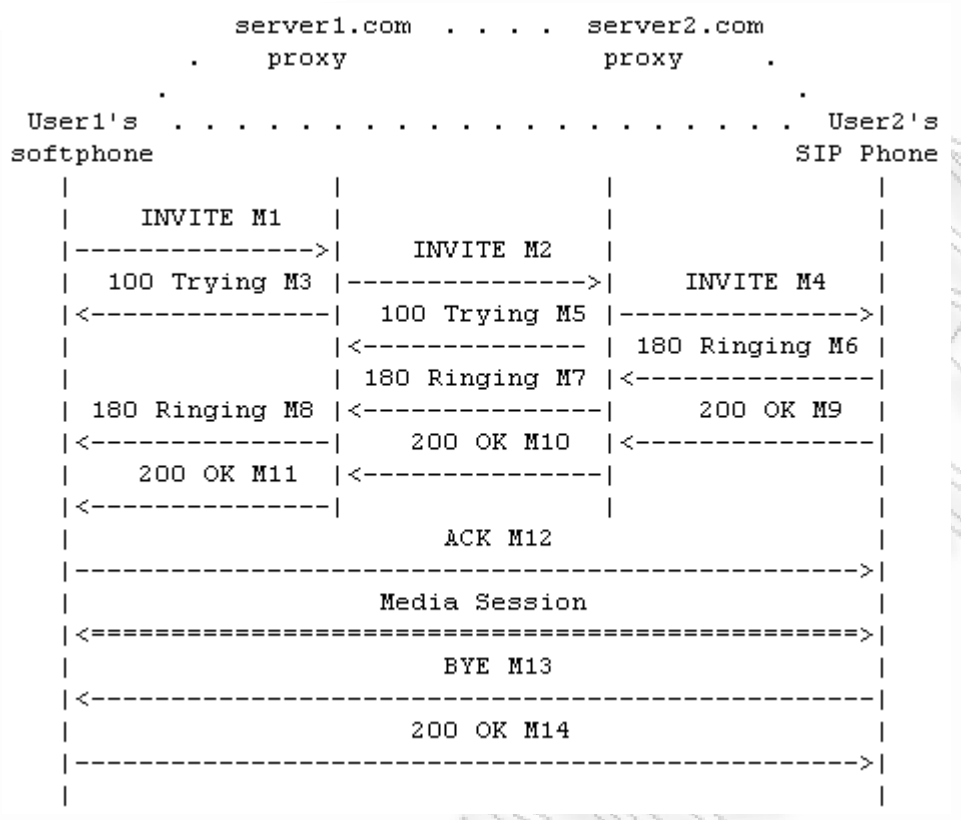
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com
;branch=z9hG4bKnashds8;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com
;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com
;branch=z9hG4bK776asdhds ;received=192.0.2.1
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
Cess: 314159 INVITE
Contact: <sip:bob@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131
(Bob's SDP not shown)
```

Η πρώτη γραμμή της απόκρισης περιέχει τον κωδικό 200 και την φράση «OK» που σημαίνει όλα καλά. Οι επόμενες γραμμές περιέχουν πεδία επικεφαλίδων. Τα επόμενα πεδία επικεφαλίδων «Via», «To», «From», «Call-ID», και «Cess» έχουν αντιγραφεί από την πρόσκληση INVITE . Το SIP τηλέφωνο του Bob έχει προσθέσει μια ετικέτα παραμέτρου (tag=a6c85cf) στο πεδίο επικεφαλίδας «To» . Αυτή η ετικέτα θα χρησιμοποιηθεί και από τις δύο τερματικές συσκευές και θα περιλαμβάνετε σε όλες τις μελλοντικές αιτήσεις και αποκρίσεις αυτής της κλήσης . Η επικεφαλίδα πεδίου «Contact» περιέχει μια URI διεύθυνση (<sip:bob@192.0.2.4>) που αντιπροσωπεύει μια άμεση διαδρομή για την επικοινωνία με τον Bob . Ενώ τα «Content-Type» και «Content-Length»

αναφέρονται στο σώμα του μηνύματος που μεταφέρουν τις SDP πολυμεσικές πληροφορίες του Bob.

Οι πληρεξούσιοι εξυπηρετητές μπορούν να κάνουν ευέλικτες αποφάσεις δρομολόγησης για να αποφασίσουν που να στείλουν την αίτηση. Για παράδειγμα εάν το τηλέφωνο του Bob μιλάει και στείλει την απόκριση 486 (Busy Here)ο biloxi.com πληρεξούσιος εξυπηρετητής μπορεί να στείλει την πρόσκληση στον εξυπηρετητή φωνητικού μηνύματος του Bob. Επίσης, μπορεί να το στείλει σε διαφορετικές τοποθεσίες ταυτόχρονα.

Στην περίπτωσή μας όμως το 200 (OK) δρομολογείται δια μέσω των δύο πληρεξούσιων εξυπηρετητών στο τηλέφωνο της Alice, το οποίο σταματάει τον τόνο κλήσης δείχνοντας ότι η κλήση έχει απαντηθεί. Τελικά, το τηλέφωνο λογισμικού της Alice στέλνει ένα μήνυμα αναγνώρισης , ACK, στο τηλέφωνο του Bob για να επιβεβαιώσει την παραλαβή της τελικής απόκρισης 200 (OK). Στο παράδειγμά μας το μήνυμα αναγνώρισης στέλνεται απευθείας από το ένα τηλέφωνο στο άλλο προσπερνώντας τους δύο πληρεξούσιους . Αυτό συμβαίνει διότι τα τερματικά έχουν μάθει το ένα την διεύθυνση του άλλου από το πεδίο της επικεφαλίδας «Contact» μέσω της ανταλλαγής των μηνυμάτων από την πρόσκληση INVITE έως την απόκριση 200 OK.



Σχήμα 3 : 2 ο Παράδειγμα του SIP τραπεζοειδούς με διαφορετικούς χρήστες και πληρεξούσιους

2.6 Έναρξη πολυμεσικής συνόδου και το πακέτο επανά-πρόσκλησης

Μετά από όλα αυτά η πολυμεσική σύνοδος μεταξύ των δύο χρηστών αρχίζει και στέλνονται πακέτα πολυμέσων με την φόρμα που έχει συμφωνηθεί με την ανταλλαγή SDP μηνυμάτων. Τα πακέτα πολυμέσων ακολουθούν διαφορετικό δρόμο από τα μηνύματα σηματοδοσίας SIP

Κατά την διάρκεια της συνόδου μπορούν να αποφασίσουν οι χρήστες να αλλάξουν τα χαρακτηριστικά της πολυμεσικής συνόδου . Αυτό επιτυγχάνεται στέλνοντας ένα πακέτο επάνα-πρόσκλησης (re-INVITE) το οποίο περιέχει μια καινούργια περιγραφή των πολυμέσων . Αυτό το μήνυμα επάνα-πρόσκλησης (re-INVITE) αναφέρεται στην υπάρχουσα σύνοδο και θα την τροποποιεί αντί να δημιουργήσει μια καινούργια. Ο άλλος χρήστης στέλνει μια 200 (OK) απάντηση που σημαίνει ότι αποδέχτηκε την αλλαγή αυτή. Ενώ ο χρήστης που

αιτήθηκε την αλλαγή απαντάει με μια επιβεβαίωση ACK. Στην περίπτωση που ο άλλος χρήστης δεν δεχτεί την αλλαγή που προτείνει ο πρώτος χρήστης , τότε στέλνει μια απόκριση λάθους όπως την 488 (Not Acceptable Here) , για την οποία ο πρώτος χρήστης απαντάει με μια επιβεβαίωση ACK. Όμως, πρέπει να σημειωθεί ότι η αποτυχία της επάνα-πρόσκλησης (re-INVITE) δεν οδηγεί σε κλείσιμο της κλήσης αλλά η σύνοδος συνεχίζεται με τα χαρακτηριστικά που είχαν διαπραγματευτεί αρχικά.

Κωδικός	Τύπος	Περιγραφή
1xx	Πληροφοριακός (Informational)	Προσδιορίζει την κατάσταση στην οποία βρίσκεται μια μη ολοκληρωμένη κλήση
2xx	Επιτυχίας (Success)	Σηματοδοτεί την επιτυχή διεκπεραίωση της αίτησης.
3xx	Ανακατεύθυνσης (Redirection)	Δείχνει εναλλακτικές τοποθεσίες στις οποίες ο αιτών θα πρέπει να αποστείλει την αίτηση του.
4xx	Σφάλμα τελικού χρήστη (Client error)	Γνωστοποιεί το γεγονός ότι η επεξεργασία της αίτησης απέτυχε λόγω σφάλματος

5xx	Σφάλμα Εξυπηρετητή (Server failure)	Σηματοδοτεί το γεγονός ότι η επεξεργασία της αίτησης απέτυχε λόγω σφάλματος στον εξυπηρετητή. Η αίτηση μπορεί να αποσταλεί σε εναλλακτικό εξυπηρετητή.
6xx	Γενικό Σφάλμα (Global failure)	Σηματοδοτεί το γεγονός ότι η επεξεργασία της αίτησης απέτυχε και δεν επιτρέπεται να υποβληθεί ξανά η αίτηση αυτή.

Πίνακας 5 . Κατηγοριοποίηση SIP αποκρίσεων

2.7 Τερματισμός κλήσης

Στο τέλος της κλήσης ο Bob κλείνει το τηλέφωνο πρώτος και δημιουργεί ένα αποχαιρετιστήριο μήνυμα BYE . Αυτό το μήνυμα δρομολογείται απευθείας στο λογισμικό τηλέφωνο της Alice προσπερνώντας τους πληρεξούσιους εξυπηρετητές. Η Alice επιβεβαιώνει την λήψη του αποχαιρετιστήριου μηνύματος BYE με ένα 200 (OK) μήνυμα το οποίο τερματίζει και την κλήση. Δεν στέλνεται επιβεβαίωση ACK διότι αυτή στέλνεται μόνο σε απάντηση μιας απόκρισης σε μια αίτηση πρόσκλησης INVITE .

Σε κάποιες περιπτώσεις μπορεί να είναι χρήσιμο για τους πληρεξούσιους εξυπηρετητές , στο μονοπάτι της σηματοδοσίας SIP ,να βλέπουν όλα τα μηνύματα μεταξύ των τερματικών συσκευών κατά τη διάρκεια της συνόδου. Για παράδειγμα εάν ο πληρεξούσιος εξυπηρετητής «biloxi.com» επιθυμεί να παραμείνει στο δρόμο των SIP μηνυμάτων πέρα την αρχική πρόσκληση INVITE , θα χρειαστεί να προσθέσει στην πρόσκληση ένα απαιτούμενο πεδίο επικεφαλίδας γνωστό ως εγγραφέα δρομολόγησης «Record- Route» το οποίο περιέχει ένα αναγνωριστικό URI που θα αναλύει το όνομα ή την IP διεύθυνση του εξυπηρετητή αυτού. Αυτή η πληροφορία θα μπορεί να ληφθεί

και από το SIP τηλέφωνο του Bob αλλά και αυτό της Alice και να αποθηκευτεί για τη διάρκεια του διαλόγου. Έτσι ο «biloxi.com» θα μπορεί να λάβει και να δρομολογήσει τα μηνύματα ACK, BYE, και την 200 (OK) απόκριση στο BYE. Κάθε πληρεξούσιος εξυπηρετητής μπορεί ανεξάρτητα να αποφασίσει εάν θα λάβει τέτοιου είδους μηνύματα τα οποία θα περνάνε δια μέσω των πληρεξούσιων εξυπηρετητών που θα επιλέξουν να τα λαμβάνουν.

2.8 Εγγραφή (Registration)

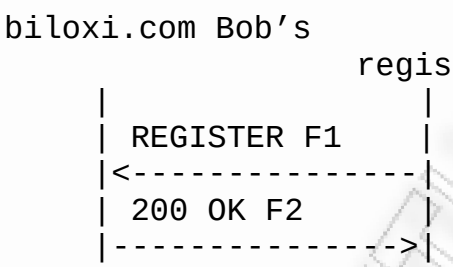
Η Εγγραφή (Registration) αποτελεί άλλη μια συνήθης λειτουργία στο πρωτόκολλο SIP. Είναι ένας τρόπος με τον οποίο ο «biloxi.com» εξυπηρετητής μπορεί να μάθει την τρέχουσα τοποθεσία του Bob. Μετά την αρχικοποίηση της λειτουργίας του SIP τηλεφώνου του Bob και ανά χρονικά διαστήματα το τηλέφωνο στέλνει μηνύματα εγγραφής (REGISTER) σε έναν εξυπηρετητή στον τομέα του «biloxi.com» γνωστό ως εγγραφέα SIP (SIP REGISTAR) . Τα μηνύματα εγγραφής συνδέουν το SIP ή το SIPS URI αναγνωριστικό (sip:bob@biloxi.com) με το μηχάνημα με το οποίο είναι εκείνη την ώρα συνδεδεμένος. Ο εγγραφέας SIP (SIP REGISTAR) καταγράφει αυτή την συσχέτιση (binding)σε μία βάση δεδομένων. Αυτή η υπηρεσία ονομάζεται υπηρεσία τοποθεσίας και μπορεί να χρησιμοποιηθεί από τον πληρεξούσιο στον «biloxi.com» τομέα . Συχνά ένας εγγραφέας SIP εξυπηρετητής βρίσκεται μαζί με τον πληρεξούσιο του τομέα εκείνου. Η διαφορά μεταξύ των τύπων των εξυπηρετητών στο SIP είναι λογική και όχι φυσική, που σημαίνει ότι ένα μηχάνημα μπορεί να χρησιμοποιηθεί για την ύπαρξη διαφόρων τύπων εξυπηρετητών και δεν απαιτείται για κάθε εξυπηρετητή διαφορετικό μηχάνημα.

Ο Bob δεν είναι περιορισμένος να εγγράφεται από μια μόνο συσκευή. Μπορούν για παράδειγμα και η συσκευή στο σπίτι του και αυτή στο γραφείο του να στέλνουν εγγραφές. Αυτή η πληροφορία αποθηκεύεται στην υπηρεσία τοποθεσίας και επιτρέπει στον πληρεξούσιο να ψάχνει με διάφορους τρόπους

για να εντοπίσει τον Bob. Παρομοίως πάνω από ένας χρήστης μπορεί να εγγραφεί από μια συσκευή την ίδια χρονική στιγμή.

Η υπηρεσία τοποθεσίας γενικά περιέχει πληροφορίες που επιτρέπουν τον εξυπηρετητή να δίνει ένα αναγνωριστικό URI και να λαμβάνει ένα ή παραπάνω εάν υπάρχουν URI αναγνωριστικά που θα του υποδεικνύουν που θα στείλει την αίτηση. Οι εγγραφές είναι ένας τρόπος να δημιουργηθούν τέτοιες πληροφορίες αλλά όχι ο μοναδικός, αφού ο διαχειριστής της υπηρεσίας αυτής μπορεί να εισάγει ο ίδιος τέτοιες πληροφορίες.

Στο παρακάτω σχήμα βλέπουμε την ροή του μηνύματος εγγραφής που στέλνεται αρχικά από τον Bob (η αυθεντικοποίηση που απαιτείται συνήθως δεν φαίνεται στο σχήμα αυτό)



Σχήμα 4 : Παράδειγμα εγγραφής SIP Registration

Το μήνυμα εγγραφής : F1 REGISTER Bob -> Registrar

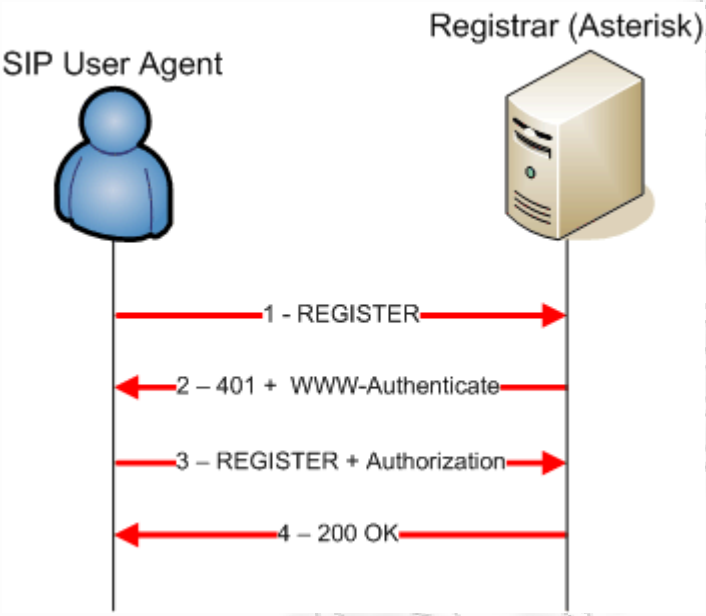
```
REGISTER sip:registrar.biloxi.com SIP/2.0
Via:                                              SIP/2.0/UDP
bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Bob <sip:bob@biloxi.com>;tag=456248
Call-ID: 843817637684230@998sdasdh09
Cess: 1826 REGISTER
Contact: <sip:bob@192.0.2.4>
Expires: 7200
Content-Length: 0
```

Η απόκριση 200 OK του εγγραφέα :

```
F2 200 OK Registrar -> Bob

SIP/2.0 200 OK
```

```
Via:                                                SIP/2.0/UDP
bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
;received=192.0.2.4
To: Bob <sip:bob@biloxi.com>;tag=2493k59kd
From: Bob <sip:bob@biloxi.com>;tag=456248
Call-ID: 8438176376842300998sdasdh09
Cess: 1826 REGISTER
Contact: <sip:bob@192.0.2.4>
Expires: 7200
Content-Length: 0
```



Σχήμα 5 . Παράδειγμα εγγραφής SIP με αυθεντικοποίηση

3.1 Θέματα ασφαλείας και επιθέσεις στα SIP συστήματα

3.1.1 Γενικά

Στην καθημερινότητα , με τον όρο ασφάλεια εννοούμε την κατάσταση εκείνη στην οποία υπάρχει η αίσθηση ότι δεν υφίσταται κάποιος κίνδυνος ή απειλή . Εννοούμε επίσης , την αποτροπή κινδύνου ή απειλής ή εξασφάλιση σιγουριάς και βεβαιότητας .

Σε κάθε επαγγελματικό κλάδο το περιεχόμενο της ασφάλειας είναι κάπως διαφορετικό . Όμως σε όλες τις περιπτώσεις αυτοί που ασχολούνται με θέματα ασφαλείας έχουν ως σκοπό την αποτροπή απειλής και κινδύνου και την εξασφάλιση της σιγουριάς και βεβαιότητας κατά την άσκηση του έργου τους.

Στον κλάδο των τηλεπικοινωνιών η ασφάλεια αποτελεί θέμα μεγίστης σημασίας για κάθε χώρα , επιχείρηση , αλλά και για μεμονωμένα άτομα. Στη χώρα μας , αλλά και σε αρκετές άλλες, έχουν έρθει κατά καιρούς στο φώς της δημοσιότητας σκάνδαλα με υποκλοπές και παραβίαση του τηλεπικοινωνιακού απορρήτου ,που έχουν συγκλονίσει και προβληματίσει τους πολίτες. Για αυτό τον λόγο είναι απαραίτητο στο σχεδιασμό των τηλεπικοινωνιακών συστημάτων να λαμβάνονται υπόψη οι πιθανές απειλές και οι αδυναμίες του συστήματος ώστε να αντιμετωπίζονται οι οποιεσδήποτε επιθέσεις στο σύστημα αυτό. Διαφυλάσσοντας έτσι την ασφάλεια επικοινωνιών για όλους τους πολίτες.

3.2 Απειλές και αδυναμίες στα συστήματα SIP

Το Εθνικό λεξικό της ασφάλειας πληροφοριών των Η.Π.Α. (**U.S. National Information Assurance Glossary)** δίνει τον ορισμό της απειλής σε πληροφοριακά συστήματα ως εξής :

Κάθε κατάσταση ή συμβάν που ενδέχεται να επηρεάσει δυσμενώς ένα πληροφοριακό σύστημα μέσω μη εγκεκριμένης πρόσβασης , καταστροφής, αποκάλυψης, τροποποίησης δεδομένων και/ή άρνηση υπηρεσίας.

Όσον αναφορά την αδυναμία – ευπάθεια των πληροφοριακών – τηλ/κων συστημάτων το **RFC 3067** την καθορίζει ως εξής :
Μια αδυναμία ή ελάττωμα στο σχεδιασμό , στην εφαρμογή , ή στη λειτουργία και διαχείριση ενός συστήματος η οποία μπορεί να εκμεταλλευτεί από κάποιον για να παραβιάσει την πολιτική ασφαλείας του συστήματος αυτού.

Ο όρος της επίθεσης δίνεται από την εθνική υπηρεσία ασφαλειών των Η.Π.Α.(National Security Agency) ως εξής :
Μια προσπάθεια να διαπεραστούν οι έλεγχοι ασφαλείας ενός συστήματος . Η επίθεση μπορεί να αλλάξει, να εκλύσει ή να αρνηθεί δεδομένα. Εάν μια επίθεση επιτύχει εξαρτάται από τις αδυναμίες του συστήματος την αποτελεσματικότητα των αντίμετρων ασφαλείας που έχει το σύστημα, αλλά και τις ικανότητες και τα εργαλεία που χρησιμοποιούν αυτοί που την εξαπολύουν.

Οι απειλές αλλά και οι επιθέσεις μπορούν να κατηγοριοποιηθούν ως ενεργές και ως παθητικές ανάλογα εάν οι επιθέσεις και οι απειλές αυτές απαιτούν αλλαγές στη συμπεριφορά του συστήματος ή του δικτύου. Για παράδειγμα μια επίθεση υποκλοπής και ανάλυση της τηλεπικοινωνιακής κυκλοφορίας είναι συνήθως παθητική(passive) ενώ η άρνηση υπηρεσίας(DoS) είναι ενεργή(active).
Τον Αύγουστο του 2006 ο S. Niccolini παράθεσε στον IETF μια ταξινόμηση των απειλών στην διαδικτυακή τηλεφωνία. Ένα χρόνο νωρίτερα ο VOIPSA είχε δημιουργήσει μια τεράστια κατηγοριοποίηση των απειλών και επιθέσεων στην διαδικτυακή τηλεφωνία(VoIP). Αν και κάποιος μπορεί να συμφωνήσει ότι κάθε στοιχείο συμπεριλαμβάνοντας και τα υποστηρικτικά μέρη ή πρωτόκολλα σε μια ανάπτυξη διαδικτυακής τηλεφωνίας μπορούν να εισάγουν αδυναμίες, είναι σχετικά δύσκολο να προβλέψεις κάθε πιθανή μελλοντική επίθεση και να προστατέψεις κάθε εφαρμογή του VoIP. Για αυτό , η εστίαση της ανάλυσης ασφαλείας στο VoIP στρώμα εφαρμογής είναι μια

λογική συνέχεια λαμβάνοντας υπόψη τις υπάρχουσες θεμελιώδεις πρακτικές και διαδικασίες διαδικτυακής προστασίας.

Οι κατηγορίες των απειλών που υπάρχουν στο IETF προσχέδιο που αναφέρθηκε παραπάνω είναι οι εξής :

- Απειλές υποκλοπής και τροποποίησης (Interception and modification threats)
- Απειλές παρεμβολής της υπηρεσίας (Interruption-of-service threats)
- Απειλές κατάχρησης υπηρεσίας (Abuse-of-service threats)
- Κοινωνικές απειλές (Social threats)

Στη συνέχεια της εργασίας θα δοθεί αναλυτική περιγραφή των πιθανών επιθέσεων που είναι δυνατόν να εμφανιστούν στη διαδικτυακή τηλεφωνία, δίνοντας ιδιαίτερο βάρος στις υπηρεσίες που αξιοποιούν το πρωτόκολλο σηματοδοσίας SIP. Χρειάζεται να αναφερθεί ότι δεν θα αναλυθούν περιπτώσεις επιθέσεων που προέρχονται από τις βασικές υποδομές του διαδικτύου αλλά αυτές που δημιουργούνται κυρίως από το πρωτόκολλο SIP που χρησιμοποιείται στη διαδικτυακή τηλεφωνία. Αντίστοιχες επιθέσεις, πιθανόν με κάποιες μικρές διαφοροποιήσεις μπορούν να εμφανισθούν και σε δίκτυα-υπηρεσίες τηλεφωνίας που αξιοποιούν εναλλακτικά πρωτόκολλα σηματοδοσίας.

3.3 Επιθέσεις στα συστήματα SIP

3.3.1 Επιθέσεις Υποκλοπών Κλήσεων(Eavesdropping) στη Διαδικτυακή Τηλεφωνία

Η υποκλοπή συνδιαλέξεων – κλήσεων αποτελεί μια από τις πιο διαδεδομένες επιθέσεις σε όλα τα τηλεπικοινωνιακά συστήματα . Στη διαδικτυακή

τηλεφωνία «θύμα» των υποκλοπών είναι εκτός από τις φωνητικές συνομιλίες και τα δεδομένα σηματοδοσίας (signaling) .

Στα μηνύματα σηματοδοσίας SIP όπως είδαμε και στις παραπάνω ενότητες υπάρχουν πληροφορίες για τα αναγνωριστικά «ID's»(SIP ή SIPS URI) των χρηστών , διευθύνσεις επαφών και άλλες βασικές παράμετροι που χρειάζονται για την επίτευξη σύνδεσης και επικοινωνίας μεταξύ δύο ή και περισσοτέρων χρηστών. Όλες αυτές οι πληροφορίες είναι απαραίτητο να παραμένουν εμπιστευτικές. Όμως, το γεγονός ότι υπάρχουν διάφορα ανεπτυγμένα εργαλεία υποκλοπής διαδικτύου όπως το «wireshark» (http://www.wireshark.org/) , το «snort» (http://www.snort.org) από τη μία και το γεγονός ότι μηνύματα που χρησιμοποιούνται στο SIP είναι μηνύματα κειμένου (text based) από την άλλη κάνουν την επίθεση υποκλοπής σχετικά εύκολη υπόθεση. Επιπλέον, είναι γεγονός ότι τα μηνύματα αυτά δρομολογούνται μέσω διαφορετικών εξυπηρετητών (οι οποίοι προσθέτουν τη δική τους διεύθυνση στο πεδίο της «Via» (Δια μέσω) επικεφαλίδας του μηνύματος), ώσπου να φτάσουν στον τελικό προορισμό τους. Κάνοντας έτσι την εφαρμογή μηχανισμών εμπιστευτικότητας μεταξύ τελικών χρηστών αρκετά δύσκολη [1,2]. Εάν για παράδειγμα υποθέσουμε ότι ένας κακόβουλος χρήστης υποκλέψει κάποια μηνύματα SIP REGISTER, τότε ο κακόβουλος αυτός χρήστης ενημερώνεται για όλες τις παραμέτρους του μηνύματος που χρησιμοποιούνται για την επικοινωνία. Εάν υποκλέψει και άλλα τέτοια μηνύματα μπορεί να πραγματοποιήσει ανάλυση κίνησης έτσι ώστε να «σπάσει» το συνθηματικό κωδικό του χρήστη.

Στην περίπτωση που τα δεδομένα της σηματοδοσίας είναι κρυπτογραφημένα (SIPS) έτσι ώστε να εξασφαλίσουν την εμπιστευτικότητα των μηνυμάτων είναι βέβαιο ότι ο κακόβουλος χρήστης θα προσπαθήσει με κατάλληλους μεθόδους αποκρυπτογράφησης να παραβιάσει την εμπιστευτικότητα αυτή.

Οι επιθέσεις υποκλοπής όμως παραβιάζουν και άλλες υπηρεσίες ασφαλείας όπως την ακεραιότητα και την διαθεσιμότητα αφού αποτελούν τα πρώτα βήματα για άλλου είδους επίθεσης στην διαδικτυακή τηλεφωνία

3.3.2 Επιθέσεις προς SIP (Parser)Αναλυτές Μηνυμάτων

Ένας SIP(parser) [3] αναλυτής χρησιμοποιείται για την επεξεργασία κατάλληλων SIP μηνυμάτων . Υπάρχουν επιθέσεις σε αναλυτές που χρησιμοποιούν πλήρως συμβατά μηνύματα με τις προδιαγραφές , αλλά και άλλες που χρησιμοποιούν μη συμβατά μηνύματα. Θα δούμε παρακάτω και τις δύο αυτές κατηγορίες.

3.3.3 Επιθέσεις που Χρησιμοποιούν Μη Συμβατά Μηνύματα

Η ορθή ανάλυση και επεξεργασία των SIP μηνυμάτων έχει μεγάλη σημασία διότι αποτελεί μέρος όλων των οντοτήτων της SIP αρχιτεκτονικής . Οι περισσότεροι αναλυτές μηνυμάτων έχουν σχεδιαστεί έτσι ώστε να επεξεργάζονται μηνύματα SIP που είναι συμβατά με τις προδιαγραφές του . Στην περίπτωση όμως που λάβουν κάποιο κακόβουλο μήνυμα μη συμβατό με τις προδιαγραφές του SIP συνήθως το απορρίπτουν στο αρχικό στάδιο της επεξεργασίας του. Εάν όμως προχωρήσει η επεξεργασία τέτοιων μηνυμάτων θα οδηγηθεί η SIP αυτή οντότητα στις παρακάτω καταστάσεις :

- Άρνηση παροχής υπηρεσίας (Denial of Service)-(DoS)
- Μη σταθερή λειτουργία (Unstable operation)
- Μη εξουσιοδοτημένη πρόσβαση (unauthorized access)

Το γεγονός ότι , όπως έχει αναφερθεί, τα SIP μηνύματα έχουν την μορφή κειμένου προσελκύει τους κακόβουλους χρήστες να αναζητήσουν διάφορους τρόπους ώστε να προκαλέσουν κάποια από τις παραπάνω επιθέσεις. Ας δούμε για παράδειγμα το παρακάτω SIP REGISTER μήνυμα που δεν είναι βασισμένο στις προδιαγραφές του πρωτοκόλλου :

```
REGISTER sip:I want to destroy sip proxies SIP/2.0
```

```
Via:                                                SIP/2.0/UDP
bobspc.biloxi.com:5060;branch=z9hG4bKnashds7
Max-Forwards: 70
To: NULL
From: NULL
Call-ID: 8438176376842308@998sdasdh09
Cess: 1826 REGISTER
Contact: NULL
Expires: 7200
Content-Length: 0
```

Παράδειγμα 5 Μη συμβατό μήνυμα SIP REGISTER

Όπως μπορούμε να διακρίνουμε οι κεφαλίδες «To, From, Contact» δεν περιλαμβάνουν δεδομένα . Γεγονός που καθιστά το μήνυμα αυτό μη έγκυρο και πολύ πιθανό να δημιουργήσει προβλήματα στον αναλυτή που θα το επεξεργαστεί, εφόσον τα δεδομένα για αυτές τις επικεφαλίδες είναι απαραίτητα.

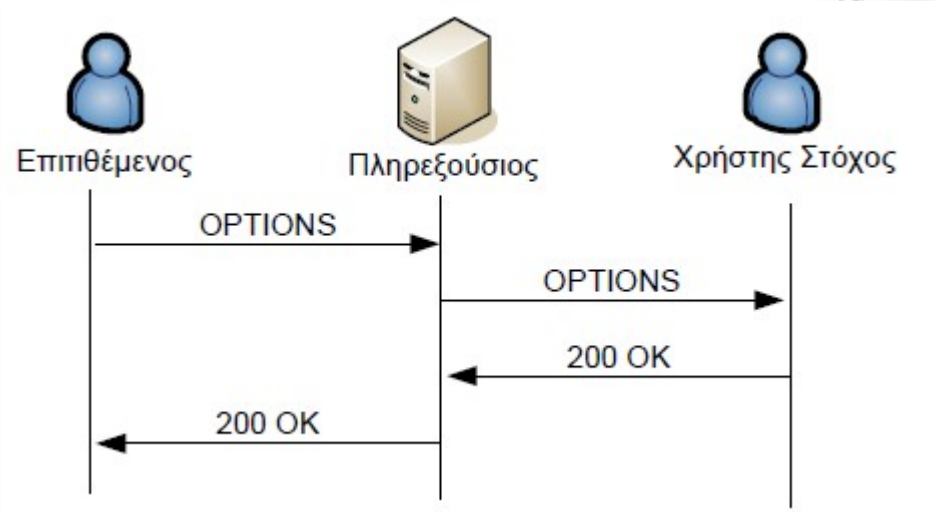
Όπως μπορούμε να υποθέσουμε, τέτοιου είδους μηνύματα που έχει τη δυνατότητα ένας κακόβουλος χρήστης να δημιουργήσει είναι πάρα πολλά. Είναι δυνατόν για παράδειγμα να χρησιμοποιήσει την μέθοδο εξαντλητικής αναζήτησης δημιουργώντας διαφορετικούς συνδυασμούς μη συμβατών μηνυμάτων με σκοπό να αποκτήσει πρόσβαση στην SIP οντότητα που θέλει. Επίσης , ένας κακόβουλος χρήστης μπορεί να ελέγξει τη στιβαρότητα-ρωμαλεότητα ενός SIP αναλυτή εντοπίζοντας ποία μηνύματα δεν υποστηρίζει έτσι ώστε να στέλνει τέτοια μη υποστηριζόμενα – μη συμβατά μηνύματα για να παρατηρήσει την αντίδρασή του σε αυτή την κατάσταση.

Μια SIP οντότητα υποστηρίζει μηνύματα SIP REGISTER όσο και SIP OPTIONS.

Τα SIP OPTIONS είναι μηνύματα που μπορούν να σταλθούν από μια SIP οντότητα σε έναν χρήστη ή έναν εξυπηρετητή για να πληροφορηθεί τις δυνατότητες που υποστηρίζει ο χρήστης ή ο εξυπηρετητής όπως : υποστηριζόμενες μεθόδους, κωδικοποιητές , τύποι περιεχομένων, προεκτάσεις κ.α. , χωρίς να γίνει κλήση.

Συνεπώς, ο κακόβουλος χρήστης μπορεί είτε να υποκλέψει το SIP REGISTER κατά την αρχικοποίηση της εγγραφής του χρήστη στόχου, είτε να αποστείλει

στο θύμα – στόχο μήνυμα SIP OPTIONS ώστε να πληροφορηθεί τα μηνύματα που υποστηρίζει το θύμα. Αυτήν την πληροφορία θα την χρησιμοποιήσει για να στείλει στο θύμα στη συνέχεια τα μη υποστηριζόμενα – μη συμβατά μηνύματα και να μελετήσει την αντίδρασή του.



Σχήμα 6. Διαδικασία Εύρεσης Υποστηριζόμενων SIP μηνυμάτων

Βεβαίως εάν μια τέτοια αδυναμία σε μια οντότητα SIP ανιχνευθεί από κάποιον πάροχο υπηρεσιών ή κάποια εταιρία που ασχολείται με την διαδικτυακή ασφάλεια γνωστοποιείται ώστε να ληθφούν τα κατάλληλα μέτρα.

Θα δούμε για παράδειγμα [5] ότι το SIP λογισμικό τηλέφωνο Counter Path X-Lite, συμβατό για τα λειτουργικά συστήματα Microsoft Windows and Mac OS X , έχει ευπάθεια στην επίθεση της άρνηση υπηρεσίας (DoS) διότι η εφαρμογή αυτή αποτυγχάνει να διαχειριστεί μη συμβατά SIP μηνύματα.

Πιο συγκεκριμένα αυτή η ευπάθεια εμφανίζεται όταν λάβει ένα μη συμβατό SIP μήνυμα πρόσκλησης (INVITE) χωρίς να έχει δεδομένα το πεδίο της επικεφαλίδας «Content-type». Αυτό έχει ως αποτέλεσμα να καταρρέει η εφαρμογή του λογισμικού τηλεφώνου δίνοντας δηλαδή τις συνθήκες της άρνησης υπηρεσίας.

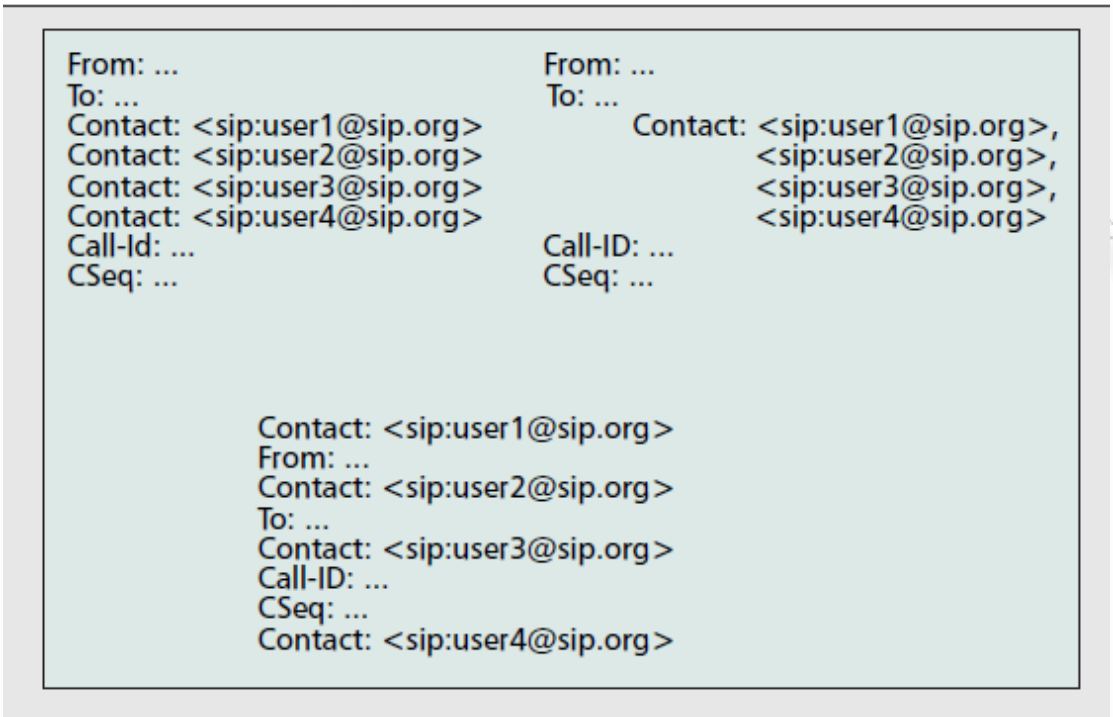
```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
Cess: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: NULL
Content-Length: 142
```

Παράδειγμα μηνύματος που προκαλεί άρνηση υπηρεσίας στο Counter Path X-Lite λογισμικό τηλέφωνο

3.3.4 Επιθέσεις με Συμβατά SIP Μηνύματα

Υπάρχει το ενδεχόμενο ακόμα και ένα συμβατό SIP μήνυμα να δημιουργήσει προβλήματα κατά την επεξεργασία και ανάλυση του [4] από μία SIP οντότητα. Για παράδειγμα, μπορεί ο κακόβουλος χρήστης να δημιουργήσει μεγάλου μήκους μηνύματα προσθέτοντας μη αναγκαίες επικεφαλίδες για την επεξεργασία του μηνύματος και/ή να συμπεριλάβει πολλά μη αναγκαία δεδομένα στο κύριο σώμα του μηνύματος.

Επίσης, ο επιτιθέμενος χρήστης μπορεί να δημιουργήσει μηνύματα τα οποία έχουν πολλαπλές τιμές (multiple values) που διαχωρίζονται αντίστοιχα σε πολλαπλές κεφαλίδες και κάθε μια από αυτές περιέχει μια μοναδική τιμή . ¨Ένα τέτοιο παράδειγμα φαίνεται και στο παρακάτω σχήμα με πολλαπλές τιμές στην επικεφαλίδα Contact. Τέτοια μηνύματα είναι απολύτως συμβατά με τις προδιαγραφές του πρωτοκόλλου SIP.



Σχήμα 7. Παραδείγματα Σύνταξης SIP Μηνυμάτων με Πολλαπλές Κεφαλίδες «Contact»

Αντίστοιχα μηνύματα μπορούν να δημιουργηθούν με χρήση των παρακάτω επικεφαλίδων : *Accept-Encoding,*
Accept-Language, Alert-Info, Allow, Authentication-Info, Call-Info, Contact, Content Encoding, Content-Language, Error-Info, In-Reply-To, Proxy-Require, Record-Route, Require, Route, Supported, Unsupported, User-Agent, Via, Warning.
Κάποιες επικεφαλίδες όπως το «*Via*» και το «*Route*» περιέχουν πληροφορίες για την δρομολόγηση του μηνύματος . Στην περίπτωση που αυτές τοποθετούνται στο τέλος του μηνύματος είναι σίγουρο ότι θα προκαλέσουν μεγαλύτερη επεξεργαστική πολυπλοκότητα, αφού οι απαραίτητες πληροφορίες για την ορθή δρομολόγηση του μηνύματος αναζητούνται στις αρχικές επικεφαλίδες.
Όλες οι παραπάνω περιπτώσεις μηνυμάτων εκτός της αυξημένης διαδικτυακής κίνησης (λόγω του μήκους τους), θα προκαλέσουν επιπρόσθετη επιβάρυνση στην επεξεργαστική ισχύ και μεγαλύτερη κατανάλωση μνήμης εξαιτίας της πολυπλοκότητας που θα απαιτηθεί για τη συντακτική τους

ανάλυση. Με τελικό σκοπό από τον κακόβουλο χρήστη την κατάρρευση των λειτουργιών των SIP στόχων.

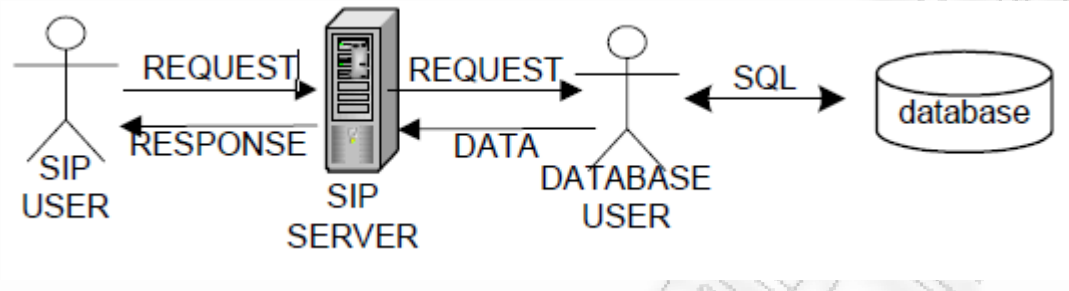
3.3.5 Επιθέσεις Εισαγωγής Κώδικα σε SIP μηνύματα

Οι επιθέσεις εισαγωγής κώδικα (injection code attacks)[13] στις υπηρεσίες του διαδικτύου μπορούν να πραγματοποιηθούν με τη βοήθεια διαφόρων μεθόδων, όπως για παράδειγμα με την υπερχείλιση καταχωρητών (buffer overflows) [6], την εισαγωγή κακόβουλου κώδικα σε περιγραφή ηλεκτρονικών σεναρίων (scripts) που ενσωματώνονται σε ιστοσελίδες [7] ή σε HTTP αιτήματα [8],[9]. Ένα από τα πιο χαρακτηριστικά παραδείγματα εισαγωγής κακόβουλου κώδικα σε HTTP αιτήματα, είναι η εισαγωγή SQL εντολών [8],[10] που έχουν ως στόχο τη μη εξουσιοδοτημένη πρόσβαση ή τροποποίηση δεδομένων που βρίσκονται αποθηκευμένα στη βάση δεδομένων του αντίστοιχου ιστοτόπου. Εξαιτίας του γεγονότος ότι η διεπαφή που αξιοποιείται για την επικοινωνία με τη βάση δεδομένων σε κάθε περίπτωση δεν εξαρτάται από τη προσφερόμενη υπηρεσία, παρόμοιες επιθέσεις είναι δυνατόν να εκδηλωθούν σε οποιαδήποτε υπηρεσία συνδέεται με βάσεις δεδομένων στο διαδίκτυο.

Συμπεραίνουμε δηλαδή ότι οι υπηρεσίες διαδικτυακής τηλεφωνίας έχουν ευπάθεια σε τέτοιου είδους επιθέσεις , καθώς δεδομένα των χρηστών όπως διαπιστευτήρια (credentials) και χρεώσεις λογαριασμών (billing) αποθηκεύονται σε βάσεις δεδομένων όπως Oracle, MySQL, Postgress.

Υπάρχουν υλοποιήσεις πληρεξούσιων εξυπηρετητών όπως ο SIP Express Router (SER) [11], και ο εξυπηρετητής που προσφέρεται από τη VoVida [12], προσφέρουν τις κατάλληλες ενότητες (modules) για τη διασφάλιση της επικοινωνίας με τις αντίστοιχες βάσεις δεδομένων για την κάλυψη των

διαφόρων αναγκών των υπηρεσιών διαδικτυακής τηλεφωνίας, αξιοποιώντας την αρχιτεκτονική που βλέπουμε στα παρακάτω σχήματα:



Σχήμα 8. Αρχιτεκτονική Διασυνεδεσιμότητας μεταξύ Πληρεξούσιου & Βάσης Δεδομένων

Επιθέσεις εισαγωγής κώδικα SQL σε συστήματα SIP είναι δυνατό να συμβούν σε κάθε περίπτωση όπου απαιτείται επικοινωνία με τη βάση δεδομένων. Μια τέτοια επικοινωνία γίνεται κυρίως όταν έχουμε αυθεντικοποίηση ενός αιτήματος. Σε μια τέτοια περίπτωση ο επιτιθέμενος εκτός των δεδομένων αυθεντικοποίησης έχει τη δυνατότητα να εισάγει και τον SQL κώδικα του παρακάτω πίνακα με την έντονη γραφή:

```
REGISTER sip:dgentele.com SIP/2.0
Via: SIP/2.0/UDP 81.0.7.124:5070
From: <sip:3400001586@dgentele.com;user=phone>;tag=3199572059
To: <sip:3400001586@dgentele.com;user=phone>
Call-ID: 3021094946@81.0.7.124
CSeq: 2 REGISTER
Contact: <sip:3400001586@81.0.7.124:5070;user=phone;transport=udp>;expires=300
User-Agent: Cisco ATA 186  v3.1.0 atasip (040211A)
Authorization: Digest username="3400001586'; UPDATE accounting set duration='200'
                        where username =340001586';--",
                       realm="dgentele.com",
                       nonce="426302039afdf717c6687e28f6c7d39c4fdb9f08",
                       uri="sip:voztele.com",response="af0d725596c8f06f370f8c80ade67b05"
Content-Length: 0
```

Σχήμα 9. Παράδειγμα Εισαγωγής Κώδικας SQL σε μήνυμα SIP Register

Με την επεξεργασία του παραπάνω μηνύματος από έναν πληρεξούσιο εξυπηρέτητη θα είχαμε την δημιουργία και εκτέλεση των παρακάτω εντολών SQL:

- Select password From subscriber where username ='3400001586';
- Update accounting set duration=200 where username= '3400001586'; --

Όπως μπορούμε να παρατηρήσουμε , η εκτέλεση των SQL εντολών και κυρίως της 2ης εντολής θα έχει ως αποτέλεσμα την μη εξουσιοδοτημένη τροποποίηση της διάρκειας των κλήσεων που έχει πραγματοποιήσει ο χρήστης με το αναγνωριστικό «340001586» στη τιμή «200». Το γεγονός ότι τα δεδομένα που βρίσκονται στο πεδίο «username» της κεφαλίδας «Authorization» αν και εκλαμβάνονται ως το πλήρες αναγνωριστικό του χρήστη, έχουν κατατμηθεί από τον επιτιθέμενο σε δύο τμήματα κάνοντας χρήση των χαρακτήρων «**';**» έχει ως αποτέλεσμα την εκτέλεση της 2ης εντολής. Οι χαρακτήρες αυτοί είναι ειδικοί (special characters) για τη γλώσσα SQL. Ο πρώτος χρησιμοποιείται για τον τερματισμό των αλφαριθμητικών σε όλες τις SQL εντολές, με αποτέλεσμα στο παραπάνω παράδειγμα να τερματίζει το «usernmame» του χρήστη που αξιοποιείται στην εντολή SQL Select (βλέπε εντολή 1). Ο δεύτερος χαρακτήρας ολοκληρώνει την εκτέλεση της αρχικής εντολής, δίνοντας με αυτό τον τρόπο τη δυνατότητα εκτέλεσης της δεύτερης εντολής. Ότι ακολουθεί μετά από τους χαρακτήρες «**--**» θεωρείται σχόλιο. Έτσι ακόμα και στην περίπτωση όπου η αρχική SQL εντολή μετά το πεδίο «username» είχε και άλλες παραμέτρους, αυτές παραλείπονται και η εκτέλεση των εντολών SQL ολοκληρώνεται.

Οι επιθέσεις εισαγωγής κώδικα SQL είναι ανεξάρτητες από τη βάση δεδομένων (Oracle, MySQL κ.α.) και την αντίστοιχη υλοποίηση του πληρεξούσιου εξυπηρέτητη. Ο μόνος περιορισμός παρουσιάζεται στη διεπαφή προγραμματισμού εφαρμογής (Application Programming Interface– (API)) που χρησιμοποιείται για την επικοινωνία με τη βάση δεδομένων.

Τέλος, είναι σημαντικό να αναφέρουμε ότι οι επιθέσεις εισαγωγής SQL κώδικα σε μηνύματα SIP δεν εκμεταλλεύονται κάποια συγκεκριμένη ευπάθεια αλλά το τρόπο που συνδέεται η υπηρεσίας διαδικτυακής τηλεφωνίας με τη βάση δεδομένων. Η έλλειψη μηχανισμών που διασφαλίζουν την ακεραιότητα των δεδομένων , δίνουν στους κακόβουλους χρήστες τη δυνατότητα να στέλνουν ανεξέλεγκτα δεδομένα στους εξυπηρετητές του SIP και να τροποποιούν τα μηνύματα άλλων χρηστών εισάγοντας τον κώδικα που θέλουν .

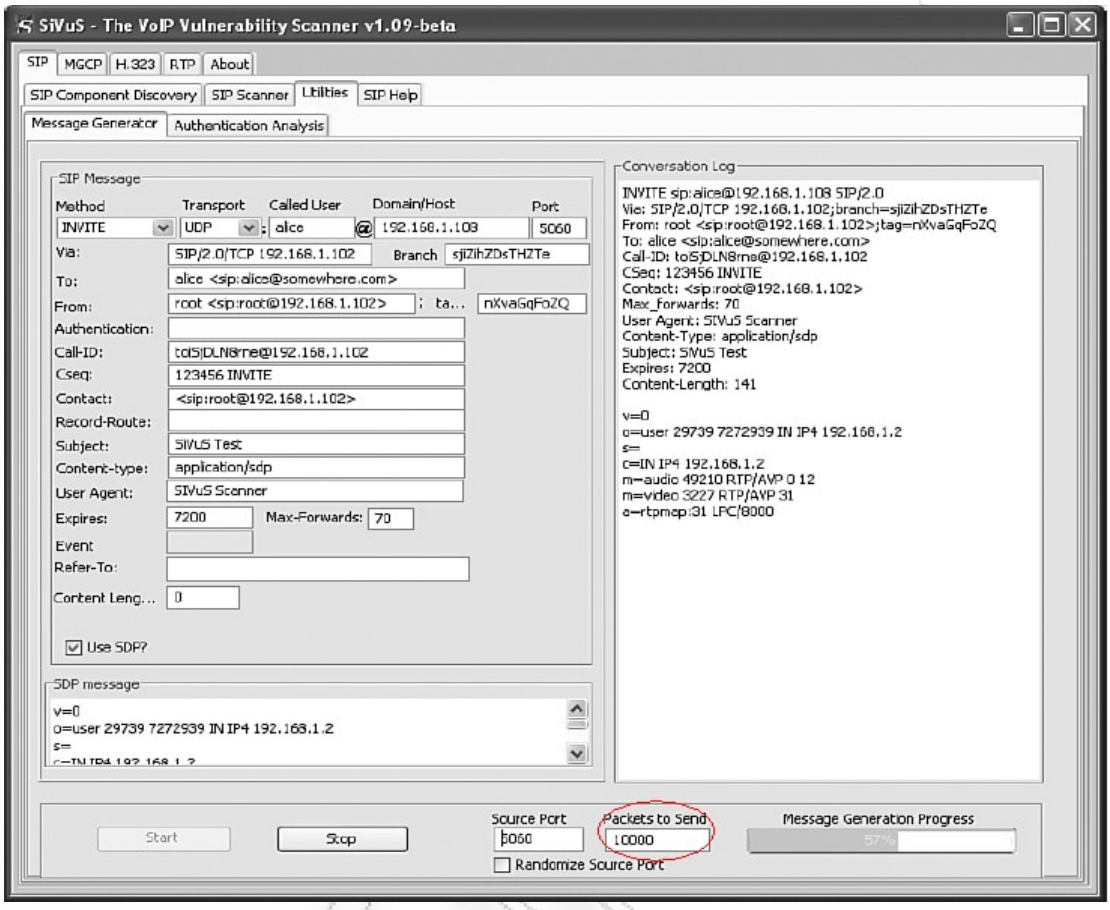
Παράδειγμα μιας τέτοιας περίπτωσης έχει ανιχνευθεί [15] στο σύστημα : Avaya SIP Enablement Services (SES). Όπου ένας κακόβουλος χρήστης μπορούσε να στείλει αιτήματα SIP στον εξυπηρετητή με ειδικά εισηγμένο κώδικα SQL ώστε να καταφέρει να δει , να προσθέσει, να τροποποιήσει ή να διαγράψει πληροφορίες στη τελική βάση δεδομένων

3.3.6 Επιθέσεις Πλημμύρας SIP μηνυμάτων

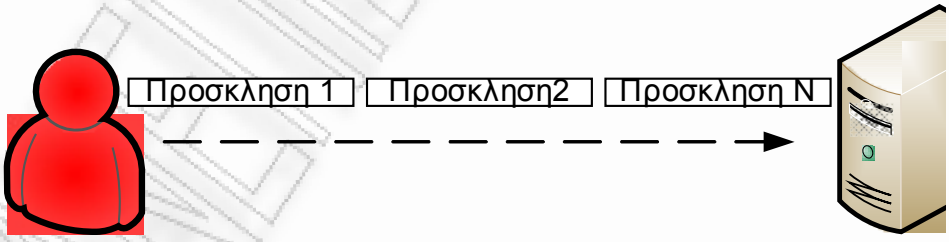
Μία από τις πιο γνωστές και αποτελεσματικές επιθέσεις άρνησης υπηρεσίας (DoS) στο διαδίκτυο και στη διαδικτυακή τηλεφωνία είναι αυτή της πλημμύρας μηνυμάτων. Ο κακόβουλος χρήστης δημιουργεί χιλιάδες μηνυμάτων που θα αποστείλει στο στοχοποιημένο δίκτυο, συσκευή η υπηρεσία. Με σκοπό την εξάντληση των υπολογιστικών και επικοινωνιακών πόρων, καθιστώντας την υπηρεσία μη διαθέσιμη . Επίσης, ο διαχωρισμός μεταξύ φυσιολογικής και επιτιθέμενης κίνησης είναι δύσκολος, αφού και στις δύο περιπτώσεις τα μηνύματα που αποστέλλονται είναι συμβατά με τις προδιαγραφές του SIP πρωτοκόλλου.

Στο παρακάτω σχήμα βλέπουμε την δημιουργία 1000 μηνυμάτων με τη βοήθεια του εργαλείου SiVus[14]. Η επίθεση αυτή προκαλεί το απομακρυσμένο τηλέφωνο να χτυπάει συνεχώς και αυτό εμποδίζει τον χρήστη του τηλεφώνου αυτού να κάνει κάποια κλήση. Επιπρόσθετα, ο πληρεξούσιος SIP εξυπηρετητής έχει απασχολήσει αρκετούς υπολογιστικούς

πόρους για να υποστηρίξει την επεξεργασία όλων των προσκλήσεων INVITE που λαμβάνει αλλά και την προώθησή τους στον προορισμό τους.



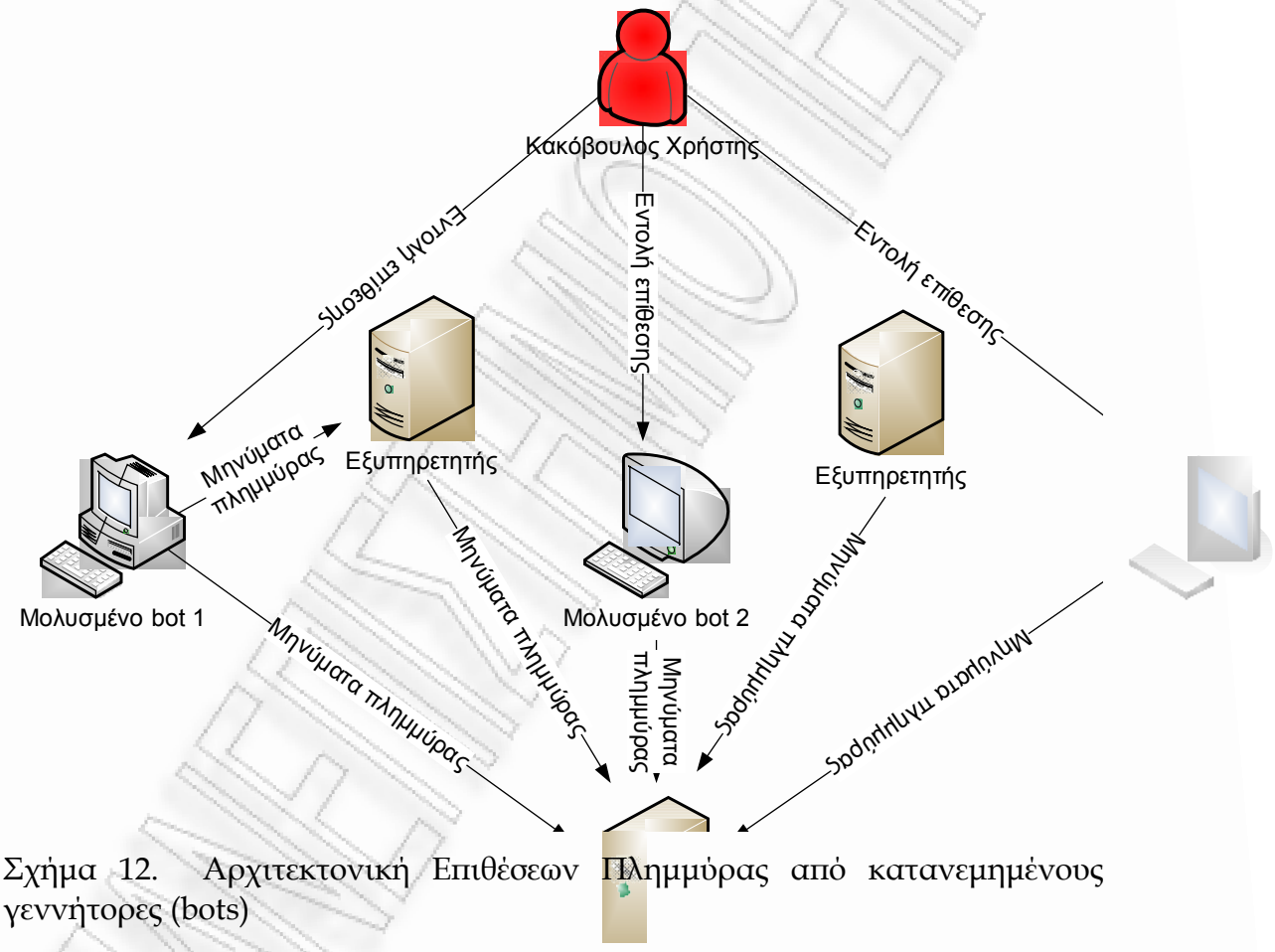
Σχήμα 10. Επίθεση πλημμύρας μηνυμάτων SIP με το εργαλείο SiVus



Σχήμα 11. Αρχιτεκτονική Επιθέσεων Πλημμύρας από έναν Κακόβουλο Χρήστη

Μια ειδική περίπτωση για τις επιθέσεις πλημμύρας είναι οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS). Τα δίκτυα διαδικτυακής τηλεφωνίας μπορεί να είναι και γεννήτορες και στόχοι τέτοιων επιθέσεων. Αποτελούνται από μολυσμένα αυτόνομα λογισμικά ρομπότ (bots) ,όπως

βλέπουμε και στο παρακάτω σχήμα και το δίκτυο με τα μολυσμένα αυτά μηχανήματα λέγεται «botnet» . Οι κατανεμημένοι γεννήτορες μηνυμάτων πλημμύρας κάνουν αυτό το είδος επίθεσης πιο αποτελεσματικό και επίσης ,πιο δύσκολο να ανιχνευθεί ο κακόβουλος χρήστης που ξεκίνησε την επίθεση αυτή. Κάποιες από τις επιθέσεις κατανεμημένων γεννητόρων είναι οι επιθέσεις πλημμύρας τύπου SYN [16],[17] και οι επιθέσεις πλημμύρας τύπου ανάκλασης (Reflection DoS) [18].



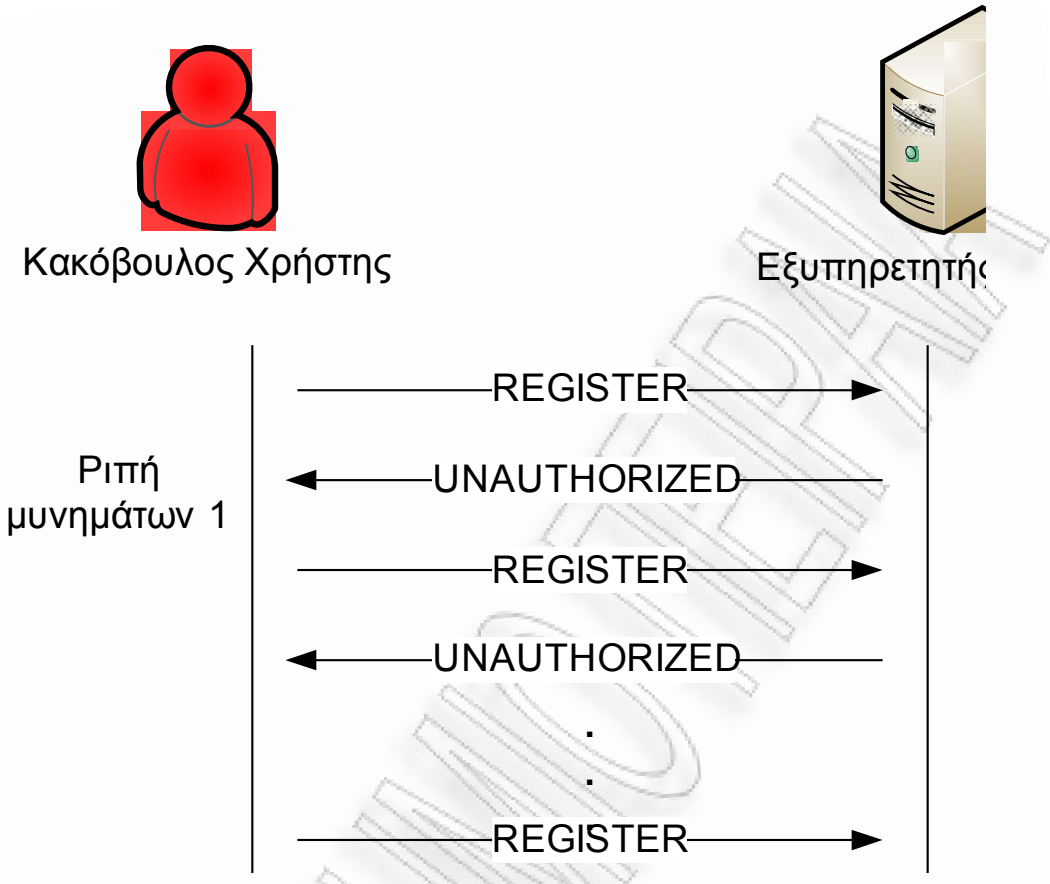
Σχήμα 12. Αρχιτεκτονική Επιθέσεων Πλημμύρας από κατανεμημένους γεννήτορες (bots)

3.3.7 Επιθέσεις Πλημμύρας προς Εξυπηρετητές Εγγραφής

Στην περίπτωση που έχουμε επιθέσεις πλημμύρας προς τους εξυπηρετητές εγγραφής, ο κακόβουλος χρήστης αποσκοπεί στην πρόκληση άρνηση παροχής υπηρεσίας αποστέλλοντας μεγάλο αριθμό μηνυμάτων εγγραφής SIP

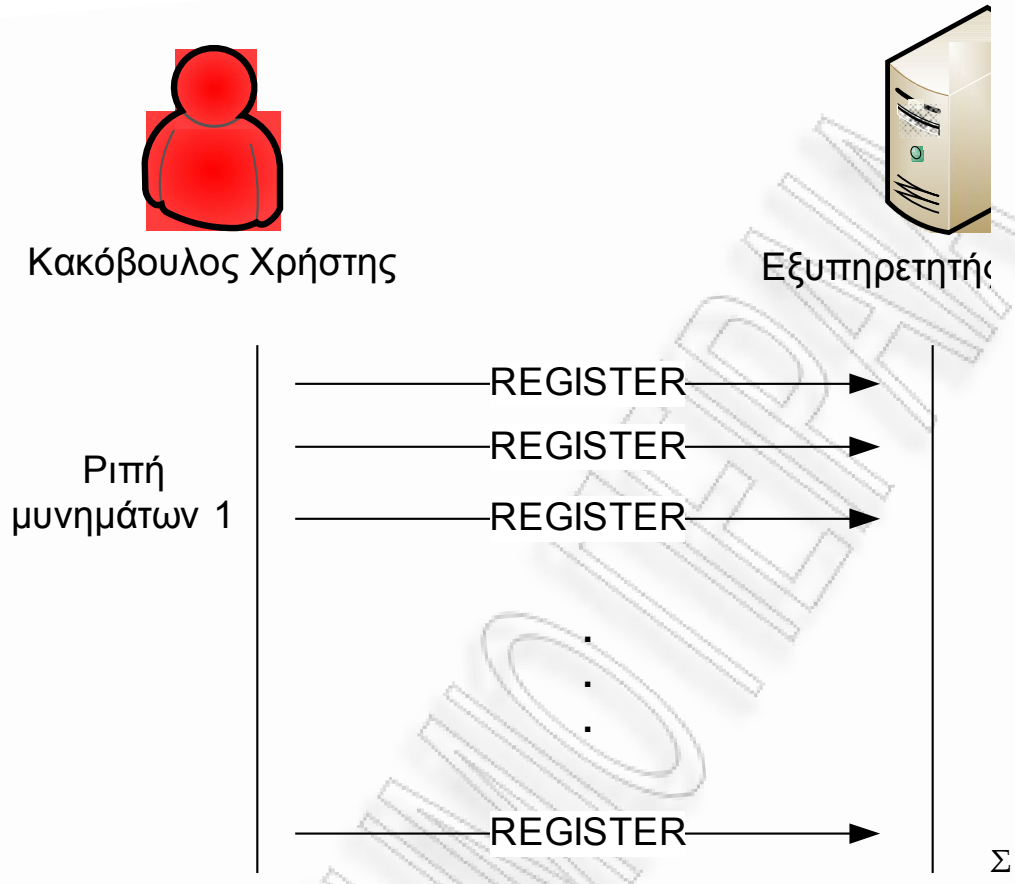
REGISTER . Αυτό έχει ως αποτέλεσμα την αύξηση του υπολογιστικού φορτίου του στοχοποιημένου συστήματος. Η αύξηση αυτή είναι ακόμα πιο μεγάλη στην περίπτωση που χρησιμοποιείται αυθεντικοποίηση κατά την εγγραφή . Αυτό συμβαίνει διότι ο εξυπηρετητής εγγραφής θα αναγκαστεί να εκτελέσει κρυπτογραφικές διαδικασίες για τις αυθεντικοποίηση που θα απαιτηθούν αυξάνοντας έτσι την επεξεργαστική ισχύ του εξυπηρετητή.

Ο χρήστης αποστέλλει μια αίτηση SIP REGISTER περιλαμβάνοντας την ή τις διευθύνσεις στις οποίες θα είναι διαθέσιμος. Στην περίπτωση που χρησιμοποιήσει αυθεντικοποίηση χρησιμοποιεί το μηχανισμό HTTP Digest [19] για τον υπολογισμό των αντίστοιχων πιστοποιητικών. Άρα ο κακόβουλος χρήστης που εκτελεί επίθεση πλημμύρας εκτός την πρόκληση άρνηση της υπηρεσίας εγγραφής αποσκοπεί και στην ανίχνευση του κωδικού κάποιου χρήστη. Τα αποσταλμένα μηνύματα μπορεί να μην είναι ακριβώς τα ίδια αφού ο επιτιθέμενος μπορεί τροποποιώντας κάποιες παραμέτρους του αρχικού μηνύματος να δημιουργήσει διαφορετικά. Στο παρακάτω σχήμα βλέπουμε ένα παράδειγμα επίθεσης πλημμύρας προς εξυπηρετητή εγγραφής.



Σχήμα 13. Επίθεση πλημμύρας προς εξυπηρετητή εγγραφής

Ο κακόβουλος χρήστης μπορεί επίσης να στέλνει συνεχόμενα ριπές μηνυμάτων εγγραφής χωρίς να απαντάει στις αποκρίσεις του εξυπηρετητή εγγραφής όπως βλέπουμε στο παρακάτω σχήμα.



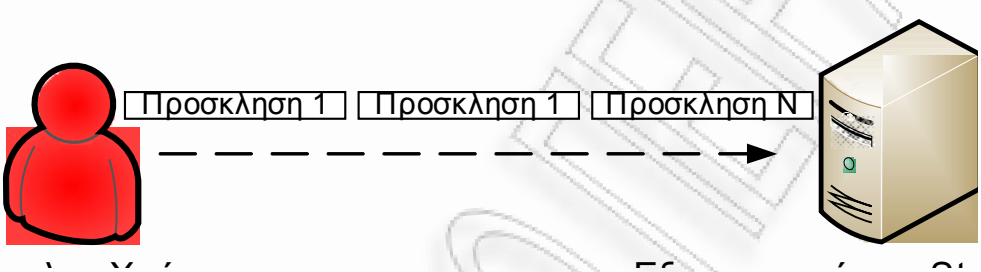
χήμα 14. Εναλλακτική επίθεση πλημμύρας προς εξυπηρετητή εγγραφής

3.3.8 Επιθέσεις Πλημμύρας προς Πληρεξούσιους εξυπηρετητές

Εκτός από τα μηνύματα εγγραφής τα υπόλοιπα SIP μηνύματα τα επεξεργάζονται και λαμβάνουν οι πληρεξούσιοι εξυπηρετητές. Οι εξυπηρετητές αυτοί λειτουργούν σε κατάσταση δίχως μνήμη (stateless mode) , αλλά και σε «κατάσταση μνήμης (stateful mode) όπου εκτός την κατάλληλη προώθηση του μηνύματος που λαμβάνουν, που πραγματοποιούν οι εξυπηρετητές σε κατάσταση δίχως μνήμη, διαχειρίζονται την κατάσταση της κλήσης συσχετίζοντας τα μηνύματα αιτήσεων και αποκρίσεων. Άρα μπορούμε να συμπεράνουμε ότι οι εξυπηρετητές στην κατάσταση μνήμης απαιτούν μεγαλύτερη επεξεργαστική ισχύ για τη διαχείριση των μηνυμάτων. Αυτό όμως, τους κάνει προτιμώμενους στόχους σε επιθέσεις πλημμύρας από τους κακόβουλους χρήστες.

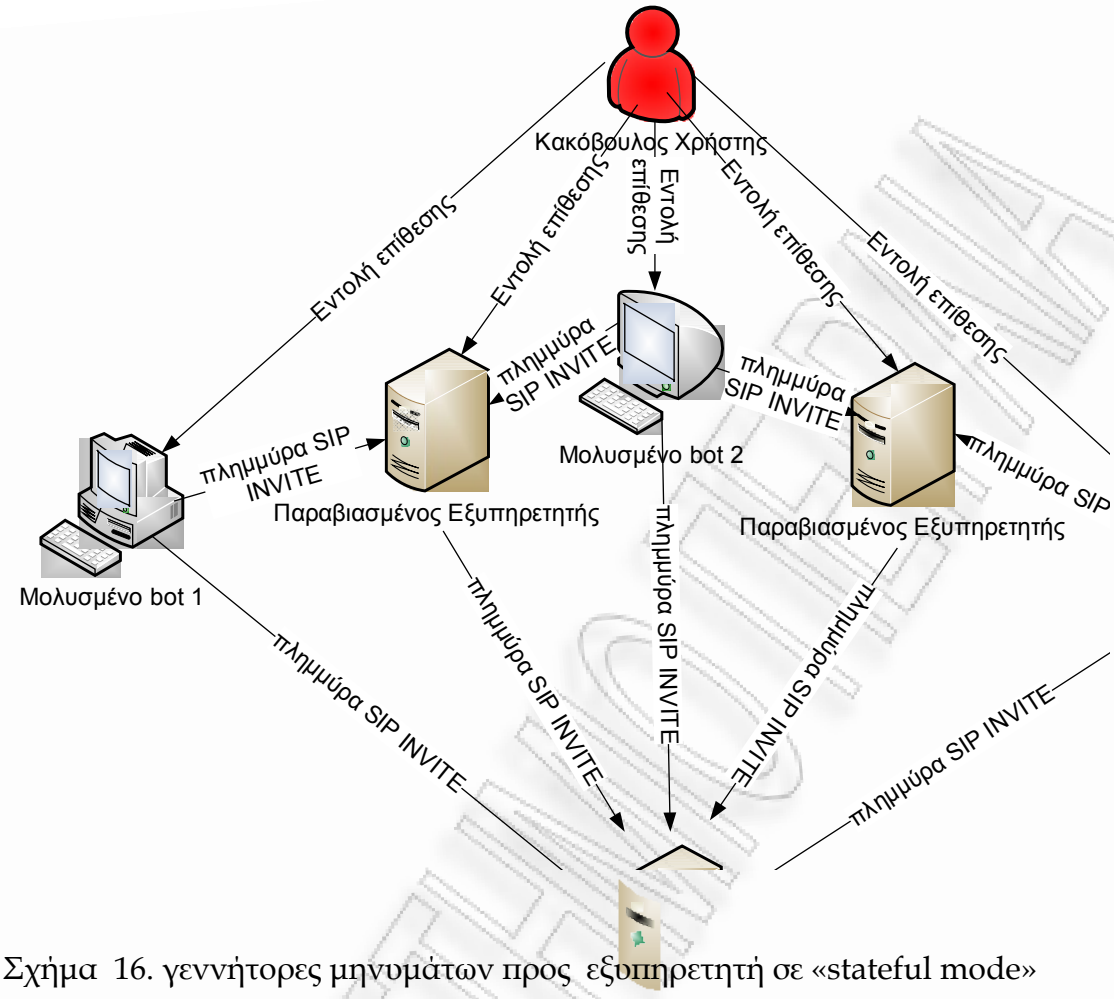
Τα μηνύματα SIP INVITE χρησιμοποιούνται σε μεγάλο βαθμό στα SIP συστήματα και επιλέγονται από τους κακόβουλους χρήστες για τις επιθέσεις πλημμύρας , χωρίς αυτό να σημαίνει ότι δεν χρησιμοποιούν και άλλα μηνύματα.

Στο παρακάτω σχήμα βλέπουμε την επίθεση σε έναν εξυπηρετητή «stateful mode» από έναν γεννήτορα διαφορετικών SIP INVITE μηνυμάτων.



Σχήμα 15. Επίθεση σε έναν εξυπηρετητή «stateful mode»

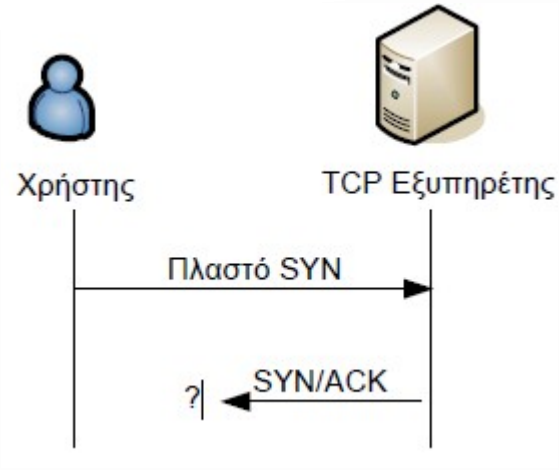
Όπως αναφέρθηκε και παραπάνω μια επίθεση από ένα «στρατό» γεννητόρων «bots» μπορεί να έχει ακόμα καλύτερα αποτελέσματα. Ο κακόβουλος χρήστης θα προσπαθήσει να παραβιάσει την ασφάλεια των εξυπηρετητών και να τους χρησιμοποιήσει και αυτούς ως γεννήτορες μηνυμάτων προς το στοχοποιημένο σύστημα που μπορεί να είναι ένας εξυπηρετητής σε «stateful mode» όπως βλέπουμε και στο παρακάτω σχήμα.



Σχήμα 16. γεννήτορες μηνυμάτων προς εξυπηρετητή σε «stateful mode»

Μία εναλλακτική μέθοδος για να αξιοποιηθεί αυτή η αρχιτεκτονική για την επίθεση πλημμύρας είναι η χρησιμοποίηση ανύπαρκτων και μη επιλύσιμων διευθύνσεων (irresolvable address) στα μηνύματα SIP INVITE. Έτσι ο πληρεξούσιος εξυπηρετητής θα αναγκαστεί να περιμένει απάντηση από τον εξυπηρετητή της υπηρεσίας του ονόματος τομέα (DNS) αυξάνοντας την επεξεργαστική ισχύ . [20],[21].

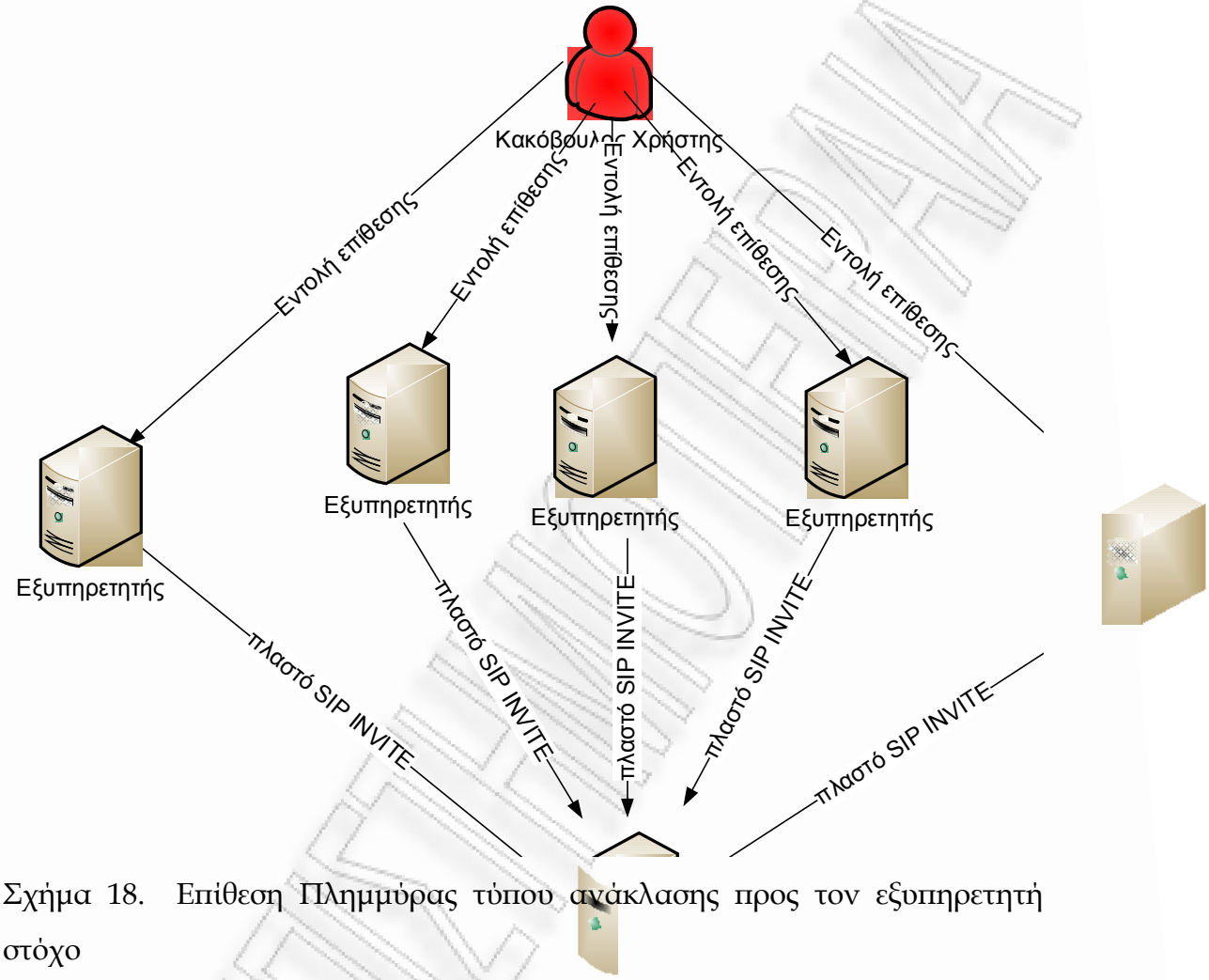
Επίσης, μπορούμε να έχουμε μια επίθεση στο SIP παρόμοια με τη TCP –SYN στο πρωτόκολλο TCP .



Σχήμα 17. επίθεση TCP –SYN

Ο κακόβουλος χρήστης δημιουργεί στην περίπτωση αυτή ένα SIP INVITE μήνυμα το οποίο περιέχει πλαστή ταυτότητα αποστολέα. Ο πληρεξούσιος εξυπηρετητής με το που λάβει το μήνυμα αυτό δεσμεύει τους αντίστοιχους υπολογιστικούς πόρους για τη διαχείριση της συνόδου και στέλνει την αίτηση στον καλούμενο. Ο καλούμενος στην περίπτωση που είναι διαθέσιμος και αποδέχεται την κλήση στέλνει στον πληρεξούσιο την απάντηση «200 OK». Ο πληρεξούσιος πρέπει να στείλει την απάντηση του καλούμενου στον επιτιθέμενο αλλά εφόσον το μήνυμα έχει πλαστή ταυτότητα αποστολέα δεν τον βρίσκει. Ο εξυπηρετητής θα κάνει κάποιες προσπάθειες μέχρι την ολοκλήρωση της διαδικασίας. . Έτσι , ένας κακόβουλος χρήστης μπορεί να στείλει πλημμύρα τέτοιων μηνυμάτων με σκοπό την υπερφόρτωση των επεξεργαστικών πόρων κάποιου στοχοποιημένου συστήματος.

Μια παραλλαγή της επίθεσης TCP –SYN είναι αυτή στην οποία οι εξυπηρετητές λειτουργούν ως προωθητές – ανακλαστήρες τέτοιων μηνυμάτων προς το στόχο. Τα μηνύματα αυτά όμως έχουν ως ταυτότητα αποστολέα την διεύθυνση του συστήματος στόχου με αποτέλεσμα όλοι οι εξυπηρετητές , όπως μπορούμε να δούμε και στο παρακάτω σχήμα, να στέλνουνε τις αποκρίσεις στον εξυπηρετητή στόχο.

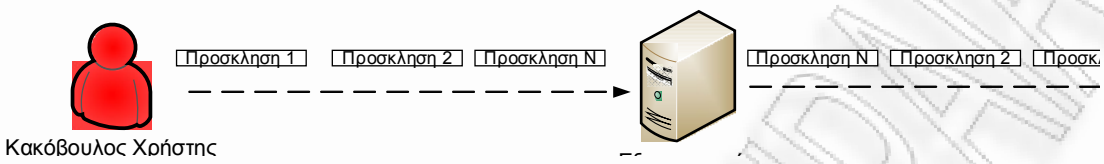


Σχήμα 18. Επίθεση Πλημμύρας τύπου ανάκλασης προς τον εξυπηρετητή στόχο

3.3.9 Επιθέσεις Πλημμύρας προς Τελικούς Χρήστες

Όπως είναι αναμενόμενο οι επιθέσεις πλημμύρας έχουν στόχους εξυπηρετητές έτσι ώστε να δημιουργείται μεγαλύτερη ζημιά σε ένα SIP τηλεπικοινωνιακό σύστημα. Όμως , οι τερματικές συσκευές χρηστών μπορούν να γίνουν εύκολος στόχος αφού έχουν περιορισμένες δυνατότητες επεξεργασίας πολλαπλών αιτήσεων και κλήσεων. Αυτό έχει ως αποτέλεσμα μετά από έναν ορισμένο αριθμό αιτημάτων να μην είναι λειτουργικές και να προκαλούν άρνηση παροχής υπηρεσίας.

Η διαφορά τέτοιου είδους επίθεσης με την επίθεση σε εξυπηρετητές είναι ότι τα SIP INVITE μηνύματα έχουν τον ίδιο προορισμό δηλαδή τον στόχο, αλλά και ότι ο ρυθμός ριπής τέτοιων μηνυμάτων είναι σαφώς μικρότερος.



Σχήμα 19. Επίθεση σε τελικό χρήστη

3.3.10 Επίθεση ενόχλησης

Μπορούμε να θεωρήσουμε ότι επίθεση ενόχλησης είναι οποιαδήποτε κλήση ή μήνυμα που ενοχλεί τον καλούμενο ή δεν του δίνει τη δυνατότητα να την απορρίψει. Τέτοια μηνύματα είναι πολύ γνωστά στους χρήστες του ηλεκτρονικού ταχυδρομείου(SPAM). Πολλά περιέχουν διαφημιστικές πληροφορίες, άλλα πολιτικές αλλά και κάποιες φορές μολυσμένα αρχεία.
Σε ένα SIP σύστημα ,που δεν έχει ρυθμιστεί σωστά η διαχείριση μηνυμάτων εκπομπής (broadcast, multicast), μπορεί να γίνει εκπομπή SIP INVITE μηνυμάτων σε μια περιοχή εκπομπής (broadcast area) έτσι ώστε όλα τα τηλέφωνα αυτής της περιοχής να λαμβάνουν τις ενοχλητικές κλήσεις ή μηνύματα.

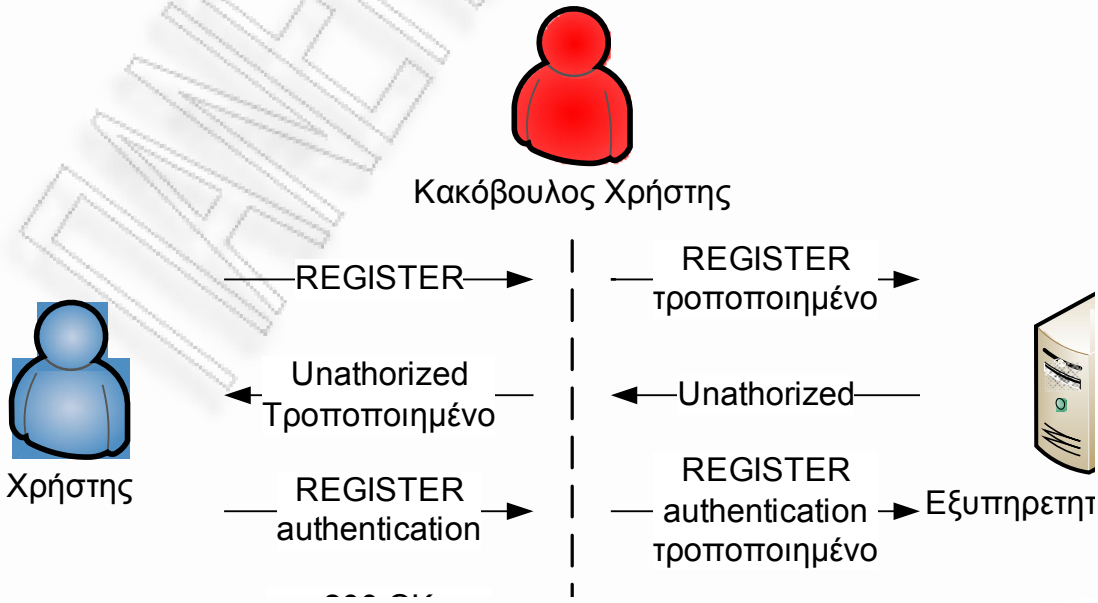
3.3.11 Επιθέσεις Ενδιάμεσου Κακόβουλου Χρήστη

Στο SIP πρωτόκολλο υπάρχουν διάφορα μηνύματα για την κατάσταση μιας συνόδου. Ένας κακόβουλος χρήστης μπορεί να προσπαθήσει να μπει ενδιάμεσα μιας κλήσης και να υποκλέψει, να τροποποιήσει κάποια από τα μηνύματα αυτά αλλά και να αποστείλει μηνύματα για να δημιουργήσει

άρνηση παροχής υπηρεσίας ή να αποκτήσει πρόσβαση χωρίς εξουσιοδότηση σε κάποια υπηρεσία.

3.3.12 Επιθέσεις Ενδιάμεσου Κατά τη Φάση Εγγραφής

Η Εγγραφή (Registration) αποτελεί μια συνήθης λειτουργία στο πρωτόκολλο SIP η οποία αποτελεί στόχο επιθέσεων. Σκοπός του κακόβουλου χρήστη μπορεί να είναι να προσποιηθεί κάποιον εξουσιοδοτημένο χρήστη. Αυτό μπορεί να το επιτύχει είτε με επίθεση ενδιάμεσου είτε υποκλέπτοντας κάποιο μήνυμα με το οποίο θα μπορέσει να βρει τους κωδικούς – πιστοποιητικά του εξουσιοδοτημένου χρήστη. Με την επίθεση ενδιάμεσου ο κακόβουλος χρήστης έχει τη δυνατότητα να τροποποιήσει τη διεύθυνση επαφής του αρχικού μηνύματος με σκοπό οι κλήσεις να περνάνε μέσω του επιτιθέμενου. Επίσης, μπορεί να τροποποιήσει τα δεδομένα του μηνύματος έτσι ώστε να μην εγγραφεί ο χρήστης. Στο παρακάτω σχέδιο βλέπουμε τον επιτιθέμενο να τροποποιεί τα στοιχεία των μηνυμάτων εγγραφής καθώς και των μηνυμάτων με τα πιστοποιητικά αυθεντικοποίησης.

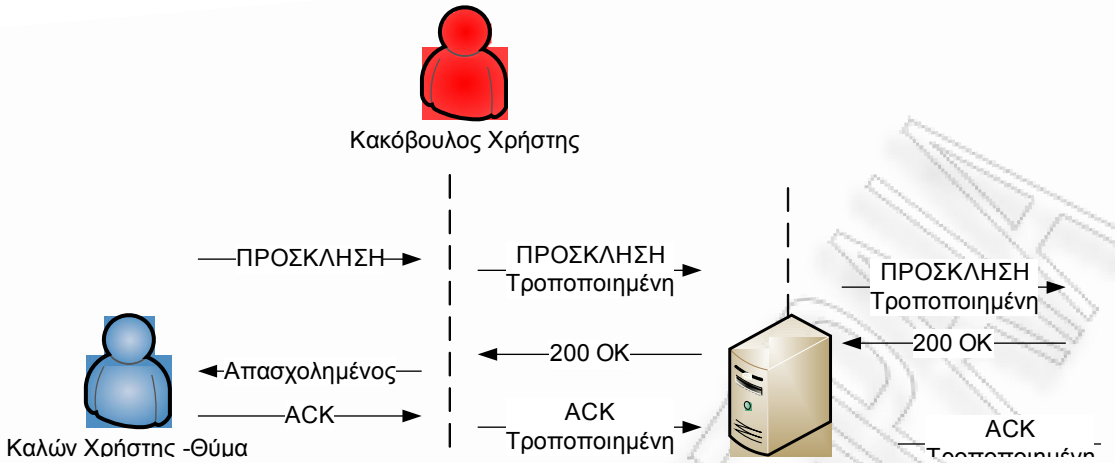


Σχήμα 20. Επίθεση Ενδιάμεσου κατά τη διαδικασία Εγγραφής με διαπιστευτήρια

Στην περίπτωση που ο κακόβουλος χρήστης υποκλέψει μηνύματα μπορεί να πραγματοποιήσει επίθεση επανάληψης (replay attack) εφόσον έχει τα πιστοποιητικά και το αρχικό μήνυμα εγγραφής του χρήστη . Εάν η υπηρεσία εγγραφής δεν έχει αντίμετρα για ένα τέτοιο τύπο επίθεσης ο κακόβουλος χρήστης θα μπορέσει να έχει πρόσβαση σε ότι υπηρεσία έχει και ο εξουσιοδοτημένος χρήστης χωρίς να γίνει αντιληπτός.

3.3.13 Επιθέσεις Ενδιάμεσου κατά την έναρξη κλήσης

Ο ενδιάμεσος κακόβουλος χρήστης μπορεί να επιτεθεί και κατά τη διαδικασία έναρξης μιας συνόδου. Στην περίπτωση αυτή ο επιτιθέμενος τροποποιεί από το αρχικό μήνυμα πρόσκλησης SIP INVITE που αποστέλλει ο χρήστης-θύμα, το πεδίο της διεύθυνσης επαφής και το στέλνει στον πληρεξούσιο εξυπηρετητή. Ο εξυπηρετητής από την πλευρά του το προωθεί στον καλούμενο χρήστη ο οποίος αποδέχεται την κλήση και στέλνει μια απόκριση 200 OK. Μόλις ληθφεί το μήνυμα αυτό από τον κακόβουλο χρήστη μέσω του εξυπηρετητή, αυτός στέλνει στον πρώτο χρήστη-θύμα απάντηση ότι είναι απασχολημένος . Έτσι, ο πρώτος χρήστης-θύμα απαντάει με το μήνυμα SIP ACK και τερματίζει την κλήση θεωρώντας τον καλούμενο μη διαθέσιμο. Άλλα αυτό που συμβαίνει είναι ότι ο κακόβουλος χρήστης βρίσκεται σε σύνοδο με τον καλούμενο χωρίς να έχει γίνει κάτι τέτοιο αντιληπτό . Παρακάτω μπορούμε να δούμε στο σχήμα την επίθεση αυτή.

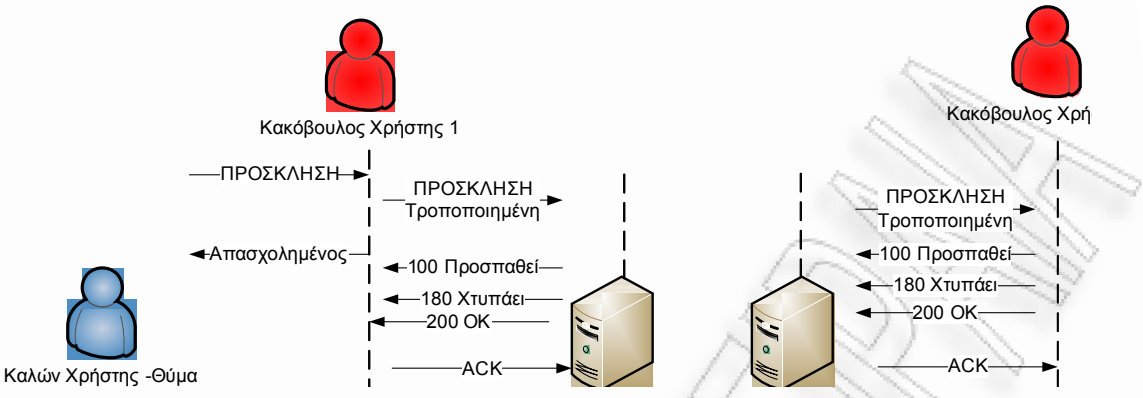


Σχήμα 21. Επίθεση ενδιάμεσου κατά την έναρξη συνόδου

Με αυτό τον τρόπο μπορεί επίσης ο κακόβουλος χρήστης να προσποιηθεί την υπηρεσία ανακατεύθυνσης στέλνοντας έτσι τα δεδομένα χρηστών – θυμάτων μέσω μη εξουσιοδοτημένων εξυπηρετητών των οποίων θα έχει και την διαχείριση.

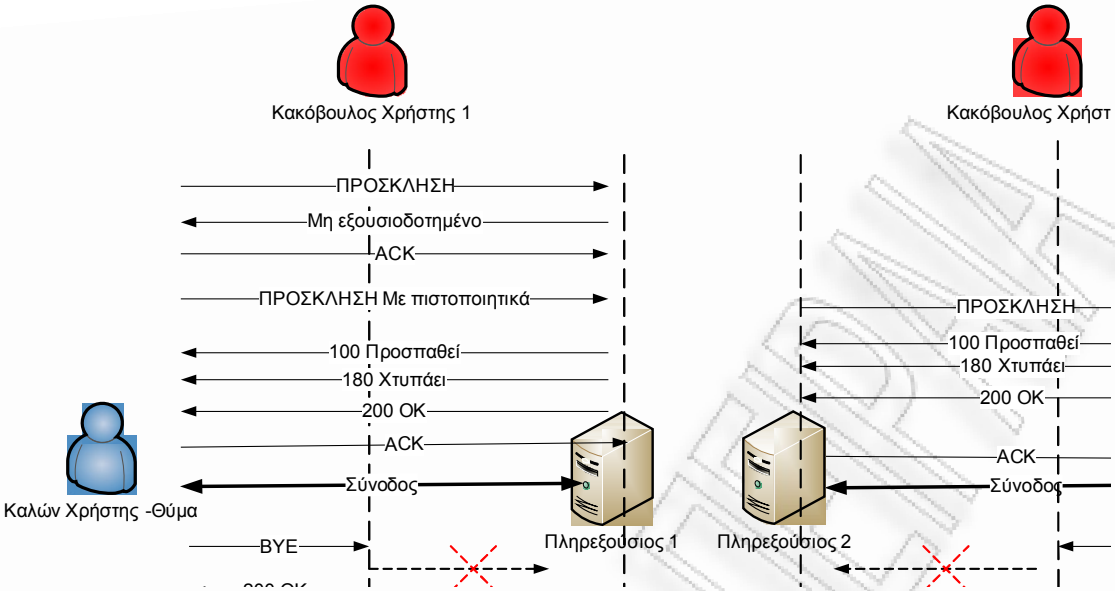
3.3.14 Επιθέσεις Απάτης Χρεώσεων

Η διαφορά στις επιθέσεις απάτης χρεώσεων («FakeBusy, ByeDelay, ByeDrop, InviteReplay») από την επίθεση ενδιάμεσου είναι ότι υπάρχει και δεύτερος κακόβουλος χρήστης από την πλευρά του καλούμενου χρήστη. Ο πρώτος κακόβουλος χρήστης που βρίσκεται ανάμεσα στον πρώτο χρήστη που αρχικοποιεί την κλήση και τον εξυπηρετητή του, τροποποιεί την πρόσκλησης SIP INVITE όπως στην παραπάνω περίπτωση επίθεσης με αποτέλεσμα ο χρήστης θύμα να νομίζει ότι ο κληθέντας χρήστης είναι απασχολημένος. Ο δεύτερος κακόβουλος χρήστης που βρίσκεται ανάμεσα στον καλούμενο χρήστη και τον εξυπηρετητή του δεν επιτρέπει την αποστολή μηνυμάτων στον καλούμενο αλλά απαντάει στα μηνύματα για λογαριασμό του. Αυτό έχει ως αποτέλεσμα την εγκαθίδρυση συνόδου μεταξύ των δύο κακόβουλων χρηστών χωρίς να γίνει αντιληπτή από τις άλλες SIP οντότητες όπως βλέπουμε και στο παρακάτω σχήμα.



Σχήμα 22. Επίθεση Απάτης Χρέωσης «Fake Busy» (χωρίς αυθεντικοποίηση της Πρόσκλησης)

Στην περίπτωση των επιθέσεων «ByeDelay» και «ByeDrop» υπάρχουν επίσης δύο κακόβουλοι χρήστες στα ίδια σημεία με την παραπάνω περίπτωση , αλλά αφού γίνει η κλήση μεταξύ δύο χρηστών – θυμάτων και τερματιστεί για αυτούς, οι κακόβουλοι χρήστες χρησιμοποιούν τις παραμέτρους αυτής της κλήσης για να επικοινωνήσουν μεταξύ τους χρεώνοντας τον χρήστη που ξεκίνησε την κλήση. Στο παρακάτω σχήμα μπορούμε να δούμε ένα τέτοιο παράδειγμα .

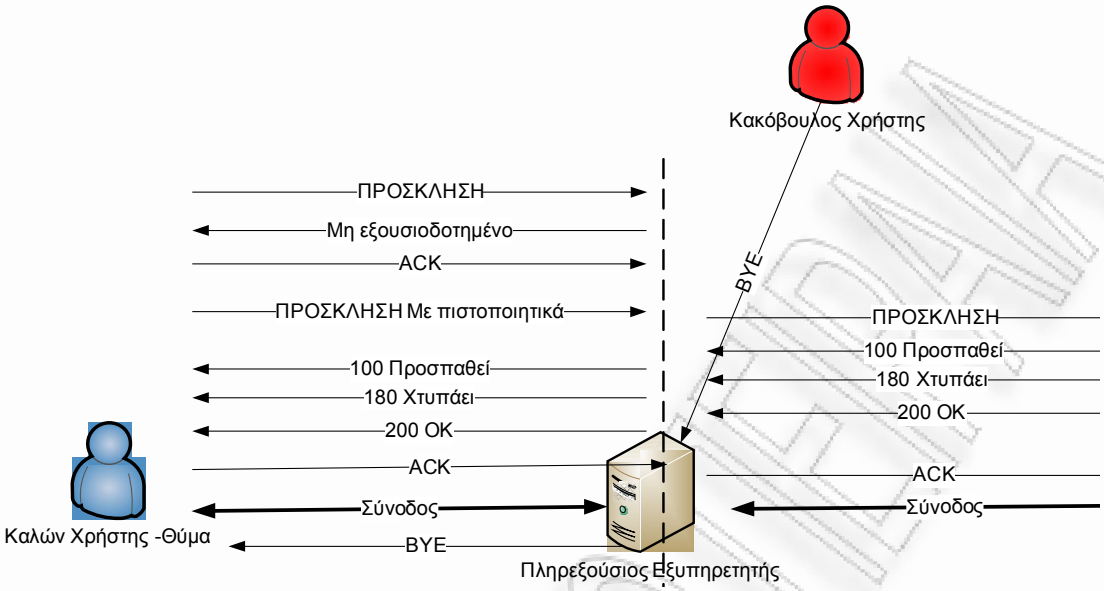


Σχήμα 23. Επίθεση Απάτης Χρέωσης «ByeDelay» και «ByeDrop» (με αυθεντικοποίηση της Πρόσκλησης)

Όσο αναφορά την επίθεση «InviteReplay» μπορούμε να την θεωρήσουμε αντίστοιχη με την επίθεση επανάληψης κατά τη διαδικασία εγγραφής που έχουμε δει παραπάνω. Ένας κακόβουλος χρήστης που έχει υποκλέψει κάποιο SIP INVITE μήνυμα, το οποίο συμπεριλαμβάνει τα αντίστοιχα πιστοποιητικά , (εάν χρησιμοποιείται η αυθεντικοποίηση στα μηνύματα SIP INVITE), έχει τη δυνατότητα να το χρησιμοποιήσει μελλοντικά για την έναρξη κλήσης με κάποιον χρήστη της αρεσκείας του, χρεώνοντας την κλήση αυτή στον αρχικό χρήστη – θύμα που δημιούργησε το μήνυμα πρόσκλησης αυτό.

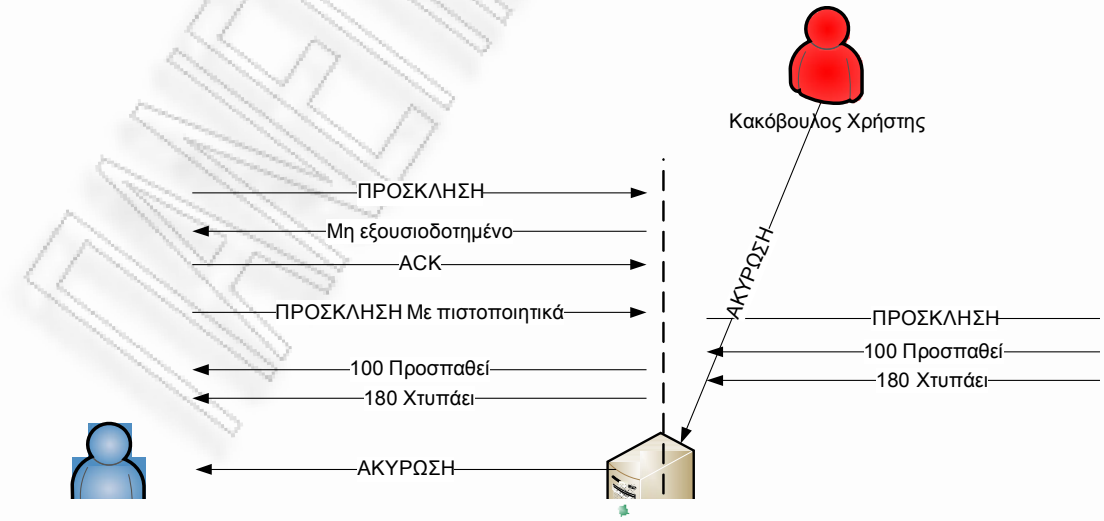
3.3.15 Επιθέσεις Ενδιαμέσου Τερματισμού Κλήσεων

Ένας κακόβουλος χρήστης έχοντας υποκλέψει αρχικά μηνύματα μιας συνόδου μπορεί στη συνέχεια να εισάγει μηνύματα SIP ώστε να προκαλέσει άρνηση παροχής υπηρεσίας . Αυτό μπορεί να το επιτύχει με την εισαγωγή ενός μηνύματος SIP BYE στη σύνοδο αυτή προκαλώντας μη εξουσιοδοτημένο τερματισμό της κλήσης του θύματος.



Σχήμα 24. Επίθεσης Ενδιαμέσου τερματισμού κλήσης BYE (πρόσκληση με αυθεντικοποίηση)

Επίσης, ο κακόβουλος χρήστης αντί του BYE μπορεί να χρησιμοποιήσει το μήνυμα SIP CANCEL για να ακυρώσει μια κλήση που είναι σε εξέλιξη όπως φαίνεται και στο παρακάτω σχήμα.

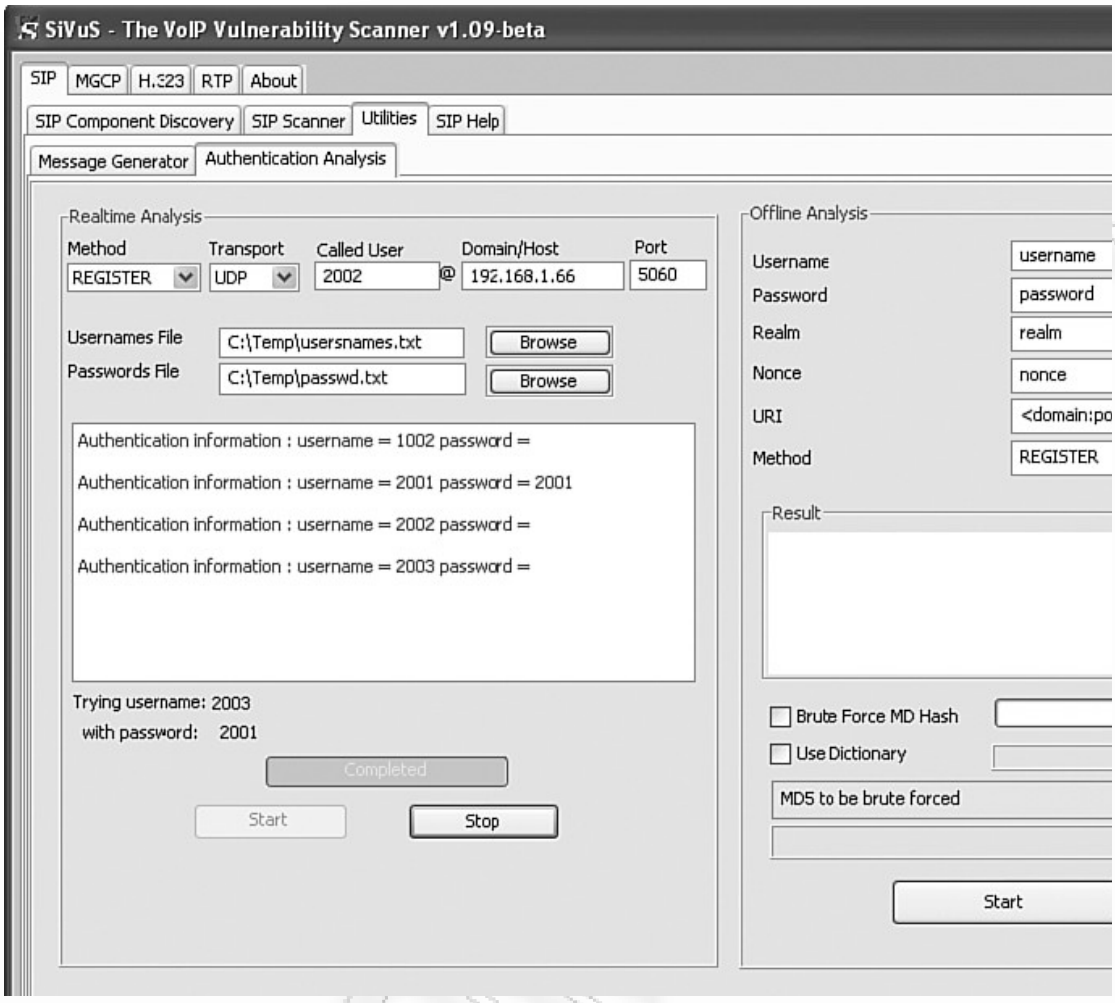


Σχήμα 25. Επίθεσης Ενδιαμέσου ακύρωσης κλήσης SIP CANCEL (πρόσκληση με αυθεντικοποίηση)

Ακόμη , ο κακόβουλος χρήστης έχει τη δυνατότητα να τροποποιήσει τις παραμέτρους μιας κλήσης στέλνοντας ένα SIP re-INITE, ή ένα SIP UPDATE μήνυμα προσδοκώντας έτσι την ανακατεύθυνση ή την υποβάθμιση της ποιότητας επικοινωνίας που θα συντελέσει στην άρνηση παροχής υπηρεσίας.

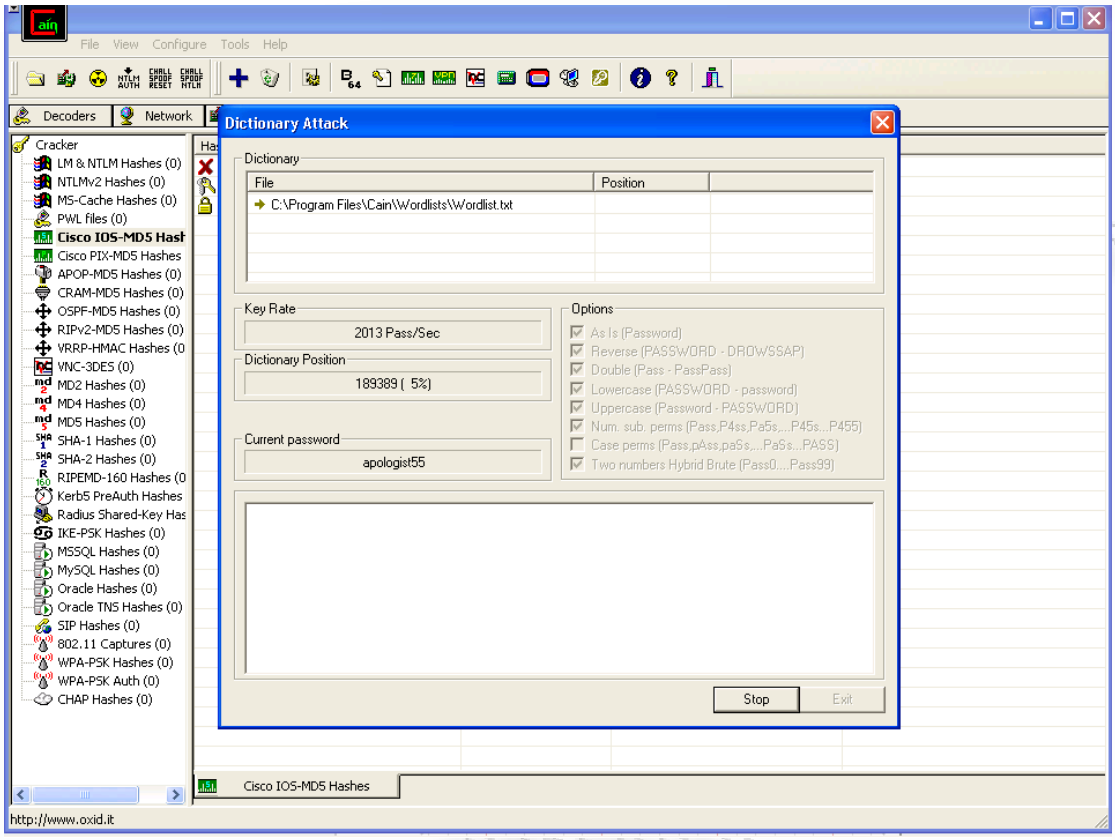
3.3.16 Επίθεση λεξικού και βίαιης δύναμης σε SIP αυθεντικοποίηση

Μία από τις μεθόδους για να αποκτήσει κάποιος πρόσβαση σε SIP υπηρεσίες είναι μαντεύοντας τα πιστοποιητικά ενός εξουσιοδοτημένου χρήστη. Για να το πετύχει αυτό ένας κακόβουλος χρήστης θα χρησιμοποιήσει την επίθεση βίαιης δύναμης (brute-force) ή λεξικού [22]σε κάποιο κωδικό. Το μήνυμα εγγραφής SIP REGISTER αποτελεί και σε αυτή την περίπτωση την πρώτη γραμμή που θα προσπαθήσει να σπάσει ο επιτιθέμενος. Ένα παράδειγμα επίθεσης βίαιης δύναμης στο SIP βλέπουμε παρακάτω όπου ο επιτιθέμενος στέλνει πολλαπλά μηνύματα REGISTER χρησιμοποιώντας ένα συνδυασμό ονόματος χρηστών και κωδικού που παίρνει από ένα ειδικό αρχείο λεξικού που ονομάζεται και πίνακες ουρανίου τόξου [23]. Το εργαλείο που χρησιμοποιείται είναι το SIVuS που είδαμε και πιο μπροστά.



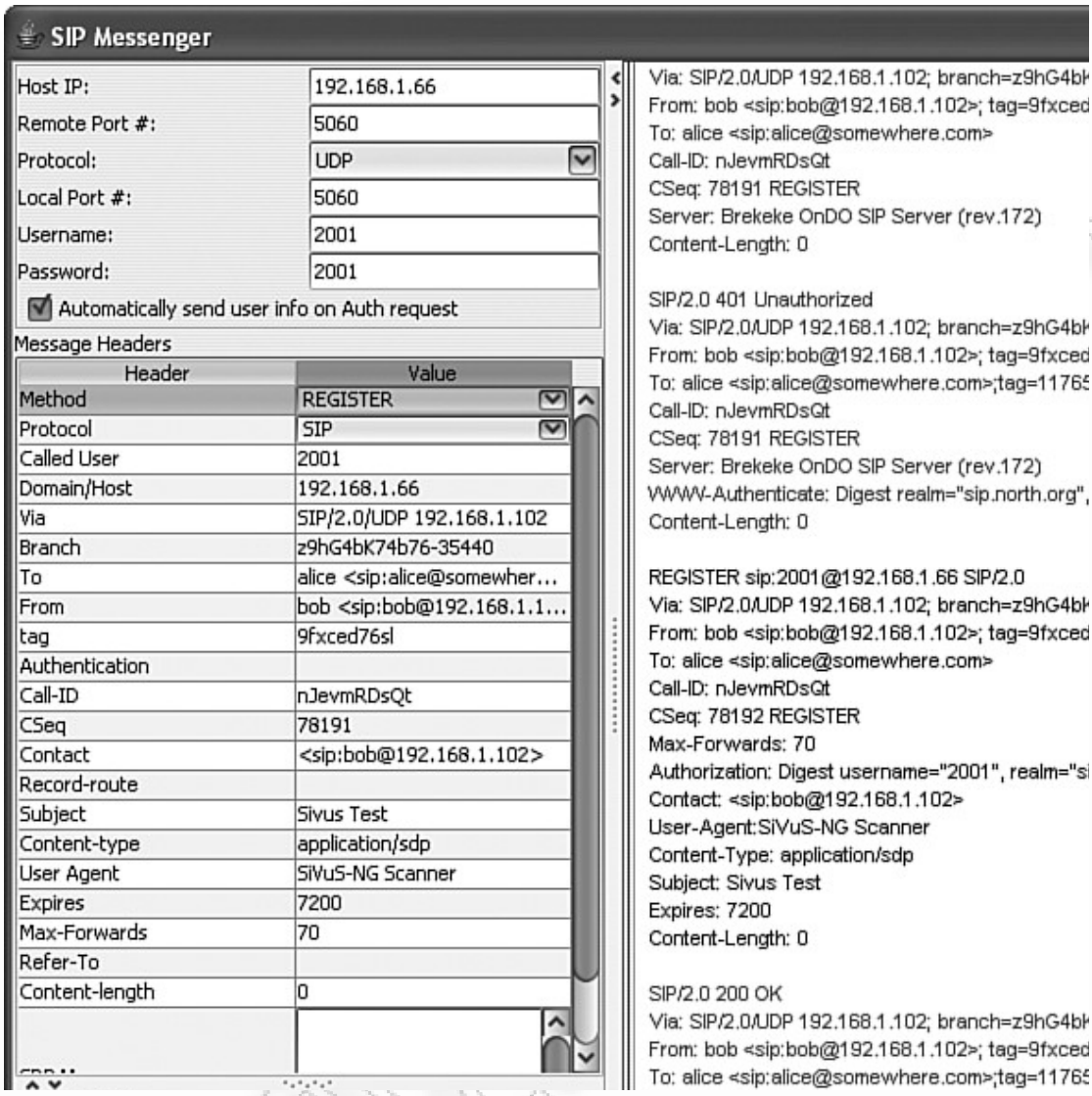
Σχήμα 26. Επίθεση στην αυθεντικοποίηση εγγραφής SIP χρησιμοποιώντας βίαιης δύναμης επίθεση με το SIVuS

Ο κακόβουλος χρήστης μπορεί επίσης να χρησιμοποιήσει και την επίθεση λεξικού (dictionary attack) η οποία μπορεί ευκολότερα να σπάσει κάποιο πιο απλό κωδικό και χρησιμοποιεί και σε αυτή την περίπτωση προϋπολογισμένους κωδικούς. Παρακάτω βλέπουμε ένα παράδειγμα μιας τέτοια επίθεσης με το εργαλείο Cain που χρησιμοποιεί το λεξικό Wordlist.txt.



Σχήμα 27. Επίθεση Λεξικού (Dictionary Attack) με το λογισμικό Cain.

Μόλις ο κακόβουλος χρήστης σπάσει τα πιστοποιητικά ενός χρήστη μπορεί να τα χρησιμοποιήσει για να εγγραφεί και να χρησιμοποιήσει τις υπηρεσίες του όπως βλέπουμε και στην παρακάτω εικόνα.



Σχήμα 28. SIP Messenger που χρησιμοποιείται για εγγραφή παραβιασμένων με τη μέθοδο βίαιη δύναμης πιστοποιητικών χρήστη

3.3.17 Επιθέσεις κοινωνικής μηχανικής και Ψάρεμα (Voice Phishing)

Η κοινωνική μηχανική είναι μια διαδικασία στην οποία ο κακόβουλος χρήστης προσπαθεί να εκμεταλλευτεί και να παραπλανήσει κάποιον χρήστη ,ο οποίος δεν έχει συνήθως μεγάλη εμπειρία σε θέματα ασφάλειας , έτσι ώστε να του αποκαλύψει εμπιστευτικά στοιχεία λογαριασμών του. Ο στόχος είναι συχνά τηλεφωνικά κέντρα στα οποία προσπαθεί ο επιτιθέμενος

επανειλημμένα να βρει κάποιο μη έμπειρο άτομο να κερδίσει την εμπιστοσύνη του και να πάρει τα δεδομένα που θέλει που στην περίπτωση του SIP μπορεί να είναι τα πιστοποιητικά ενός χρήστη. Το ψάρεμα (Voice Phishing) είναι ανάλογο με αυτό στα μηνύματα ηλεκτρονικού ταχυδρομείου , στην περίπτωση του SIP μπορεί κάποιο φωνητικό ή γραπτό μήνυμα να οδηγήσει τον χρήστη να πληκτρολογήσει τους κωδικούς του σε ένα περιβάλλον όπου ο κακόβουλος χρήστης θα μπορεί να τα υποκλέψει για παράδειγμα μια παραποιημένη HTTP σελίδα.

4. Οι Μηχανισμοί ασφαλείας στο Πρωτόκολλο SIP

Οι βασικές υπηρεσίες ασφαλείας που απαιτούνται στο πρωτόκολλο SIP σύμφωνα και με τις απειλές που είδαμε στα παραπάνω κεφάλαια είναι :

- Η διαφύλαξη της εμπιστευτικότητας και της ακεραιότητας των μηνυμάτων
- Η αποφυγή επιθέσεων επανάληψης(replay attacks) και η παραποίηση μηνυμάτων (message spoofing)
- Παροχή μηχανισμών αυθεντικοποίησης και προστασίας της ιδιωτικότητας αυτών που συμμετέχουν σε μία σύνοδος
- Αποφυγή της επίθεσης άρνησης υπηρεσίας

Όμως, αντί να προσδιοριστούν νέοι μηχανισμοί ασφαλείας ειδικά για το SIP, το SIP χρησιμοποιεί τους ήδη υπάρχοντες μηχανισμούς ασφαλείας στα πρωτόκολλα HTTP και SMTP.
Η πλήρης κρυπτογράφηση των μηνυμάτων παρέχει το καλύτερο τρόπο ώστε να διατηρείται η εμπιστευτικότητα των μηνυμάτων ενώ εγγυάται ότι τα μηνύματα δεν θα τροποποιηθούν από κακόβουλους ενδιάμεσους. Όμως , οι αιτήσεις και οι αποκρίσεις στο SIP δεν μπορούν να είναι τελείως κρυπτογραφημένες διότι κάποια πεδία των μηνυμάτων όπως το αναγνωριστικό «Request-URI», η διαδρομή «Route», το δια μέσω «Via» χρειάζεται να είναι ορατά στους πληρεξούσιους εξυπηρετητές στις περισσότερες δικτυακές αρχιτεκτονικές , έτσι ώστε να δρομολογούνται σωστά.

Επίσης, οι πληρεξούσιοι εξυπηρετητές χρειάζεται να τροποποιήσουν κάποια μέρη του μηνύματος , πιο συγκεκριμένα να προσθέσουν την διεύθυνση τους στο πεδίο της επικεφαλίδας δια μέσω «Via», ώστε να λειτουργήσει σωστά το SIP. Οι πληρεξούσιοι πρέπει να είναι αξιόπιστοι σε κάποιο βαθμό από τους χρήστες. Για το λόγο αυτό χαμηλού – στρώματος μηχανισμοί ασφαλείας προτείνονται για το SIP, οι οποίοι θα κρυπτογραφήσουν τις αποκρίσεις και τα αιτήματα στο καλώδιο σε μια βήμα-βήμα βάση, ώστε να μπορέσουν οι τερματικοί χρήστες να επιβεβαιώσουν την ταυτότητα των πληρεξούσιων εξυπηρετητών και σε ποιούς στέλνουν τις αιτήσεις τους. Οι SIP οντότητες χρειάζονται επίσης να αναγνωρίσουν η μια την άλλη με ασφαλές τρόπο. Όταν ένα τερματικό SIP επιβεβαιώνει την ταυτότητα του χρήστη του σε ένα άλλο τερματικό SIP ή σε ένα πληρεξούσιο εξυπηρετητή , αυτή η ταυτότητα πρέπει με κάποιο τρόπο να είναι επαληθεύσιμη. Ένας μηχανισμός κρυπτογραφικής αυθεντικοποίησης παρέχεται στο SIP για να καλύψει αυτήν την απαίτηση. Ένας ανεξάρτητος μηχανισμός ασφάλειας για το σώμα ενός SIP μηνύματος παρέχει μια εναλλακτική έννοια της αρχής μέχρι τέλους αμοιβαίας αυθεντικοποίησης , ενώ παρέχει επίσης ένα όριο στο βαθμό τον οποίο οι χρήστες πρέπει να εμπιστεύονται του ενδιάμεσους.

4.1 Ασφάλεια στο επίπεδο μεταφοράς και δικτύου

Για την ασφάλεια στο επίπεδο μεταφοράς και δικτύου κρυπτογραφείται η κίνηση σηματοδοσίας , διασφαλίζοντας έτσι την ακεραιότητα και εμπιστευτικότητα των μηνυμάτων. Συχνά , χρησιμοποιούνται πιστοποιητικά για την δημιουργία ασφάλειας χαμηλού επιπέδου(layer) . Δυο δημοφιλείς μέθοδοι για την παροχή ασφάλειας στο επίπεδο μεταφοράς κα δικτύου είναι η «TLS» και το «IPsec».

4.1.1Το ασφαλές IP (IPsec)

Το **ασφαλές IP (IPsec)** αποτελείται από ένα σύνολο εργαλείων από το πρωτόκολλο του επιπέδου δικτύου τα οποία συνολικά μπορούν να χρησιμοποιηθούν ως αντικατάσταση ασφαλείας του παραδοσιακού πλέον IP πρωτοκόλλου.

Το ασφαλές IP (IPsec) συνήθως εφαρμόζεται σε αρχιτεκτονικές στις οποίες ένα σύνολο χρηστών ή διαχειριστικών τομέων έχουν μια προϋπάρχουσα σχέση εμπιστοσύνης μεταξύ τους. Επίσης, συνήθως εφαρμόζεται στο επίπεδο λειτουργικού συστήματος του χρήστη , ή σε μια έξοδος ασφαλείας η οποία παρέχει εμπιστευτικότητα και ακεραιότητα για όλη την κίνηση που λαμβάνει από μια συγκεκριμένη διεπαφή (όπως στην αρχιτεκτονική του VPN).

Σε πολλές αρχιτεκτονικές του SIP για το ασφαλές IP δεν απαιτούνται κάποιες ιδιαίτερες τροποποιήσεις ενσωμάτωση του . Πιθανώς να ταιριάζει καλύτερα σε υλοποιήσεις στις οποίες είναι δύσκολο να προσθέσεις διάφορους μηχανισμούς ασφαλείας ανωτέρων επιπέδων πάνω στις τερματικές συσκευές. Πάντως τερματικές συσκευές που έχουν σχέσεις ασφαλείας (διαμοιρασμένου κλειδιού) με τον πληρεξούσιο του πρώτου βήματος αποτελούν καλούς υποψηφίους για τη χρήση του IPsec. Τέλος, κάθε υλοποίηση SIP απαιτεί ένα προφίλ IPsec που να περιγράφει τα εργαλεία πρωτοκόλλου που χρειάζονται για να ασφαλιστεί το SIP.

Το **«TLS»** παρέχει ασφάλεια στο επίπεδο της μεταφοράς πάνω από σύνδεσμο-στραφή πρωτόκολλα όπως το TCP (και όχι το UDP). Το «TLS» μπορεί να προσδιοριστεί ως το επιθυμητό πρωτόκολλο μεταφοράς για την επικεφαλίδα του πεδίου «Via» ή για το αναγνωριστικό SIP-URI . Επίσης, είναι κατάλληλο κυρίως για αρχιτεκτονικές στις οποίες η ασφάλεια βήμα-βήμα απαιτείται μεταξύ οντοτήτων οι οποίες δεν έχουν προϋπάρχοντες σχέσεις εμπιστοσύνης. Για παράδειγμα , η Alice εμπιστεύεται τον τοπικό της πληρεξούσιο εξυπηρετητή , ο οποίος μετά από ανταλλαγή πιστοποιητικών εμπιστεύεται τον τοπικό πληρεξούσιο εξυπηρετητή του Bob (TLS) τον οποίο εμπιστεύεται ο Bob , για αυτό η επικοινωνία μεταξύ Alice και Bob είναι ασφαλής. Το «TLS» πρέπει να είναι στενά συνδεδεμένο με μια εφαρμογή SIP . Οι μηχανισμοί

μεταφοράς είναι σε μια βήμα –προς –βήμα βάση στο SIP , για αυτό όταν ένας χρήστης στέλνει μια αίτηση πάνω από «TLS» σε ένα πληρεξούσιο εξυπηρετητή δεν έχει κάποια διαβεβαίωση ότι το «TLS» θα χρησιμοποιηθεί έως το τέλος. Η κρυπτογράφηση TLS_RSA_WITH_AES_128_CBC_SHA πρέπει να υποστηρίζεται τουλάχιστον ως ελάχιστη απαίτηση από τις οντότητες SIP που χρησιμοποιούν αυτή τη μέθοδο ασφάλειας . Για λόγους συμβατότητας οι πληρεξούσιοι εξυπηρετητές , οι εξυπηρετητές ανακατεύθυνσης και εξυπηρετητές εγγραφής θα πρέπει να υποστηρίζουν την εξής κρυπτογράφηση : TLS_RSA_WITH_3DES_EDE_CBC_SHA

4.1.2 Το αναγνωριστικό SIPS URI

Το αναγνωριστικό SIPS URI κληρονομεί τη σύνταξη του από το SIP URI που είδαμε σε παραπάνω κεφάλαια.

Μπορεί να χρησιμοποιηθεί ως διεύθυνση καταγραφής για συγκεκριμένους χρήστες ,δηλαδή το αναγνωριστικό URI με το οποίο είναι γνωστός ο χρήστης, στο πεδίο της επικεφαλίδας «FROM» των αιτήσεων του και στο πεδίο της επικεφαλίδας «To» της αίτησης εγγραφής (παράδειγμα sips:bob@biloxi.com).

Όταν χρησιμοποιείται ως αναγνωριστικό URI μιας αίτησης , το SIPS σχήμα υποδεικνύει ότι κάθε βήμα πάνω από το οποίο η αίτηση προωθείται , έως ότου φθάσει στην SIP οντότητα που είναι υπεύθυνη για το τμήμα του τομέα(domain) της αίτησης URI, πρέπει να είναι διασφαλισμένο με TLS. Με το που φθάσει στην οντότητα αυτή, η αίτηση μεταχειρίζεται σε συμφωνία της τοπικής πολιτικής ασφάλειας και δρομολόγησης της οντότητας. Το πιο πιθανό είναι να χρησιμοποιηθεί το «TLS» έως το τελευταίο βήμα του τερματικού αποδέκτη.

Το SIPS αναγνωριστικό είναι εφαρμόσιμο και σε άλλα πεδία επικεφαλίδων επιπλέον όπως το «Contact» και το «Route». Σε κάθε περίπτωση το SIPS URI

επιτρέπει στα υπάρχοντα πεδία να καθορίσουν ασφάλεια με την χρήση του TLS.

Η χρήση του SIPS URI προϋποθέτει την αμοιβαία αυθεντικοποίηση μέσω TLS η οποία πρέπει να χρησιμοποιεί την κρυπτογράφηση TLS_RSA_WITH_AES_128_CBC_SHA. Τα πιστοποιητικά που λαμβάνονται κατά τη διαδικασία αυθεντικοποίησης θα πρέπει να πιστοποιούνται σε σχέση με αρχικά πιστοποιητικά που έχουν ανταλλαγεί και σε περίπτωσης μη πιστοποίησης θα τερματίζεται η αίτηση. Επιπλέον , πρέπει να σημειωθεί ότι στο SIPS URI η μεταφορά είναι ανεξάρτητη από το TLS δηλαδή μπορούν να χρησιμοποιηθούν τα πρωτόκολλα μεταφοράς TCP και SCTP (όχι όμως το UDP) όπως βλέπουμε στα παρακάτω παραδείγματα :

"sips:alice@atlanta.com;transport=tcp"

"sips:alice@atlanta.com;transport=sctp"

Οι χρήστες που στέλνουν μηνύματα με SIPS URI αναγνωριστικά συνήθως επιλέγουν να χρησιμοποιούν συσκευές που αρνούνται την ανταλλαγή αιτήσεων πάνω από μη ασφαλή μονοπάτια μεταφοράς.

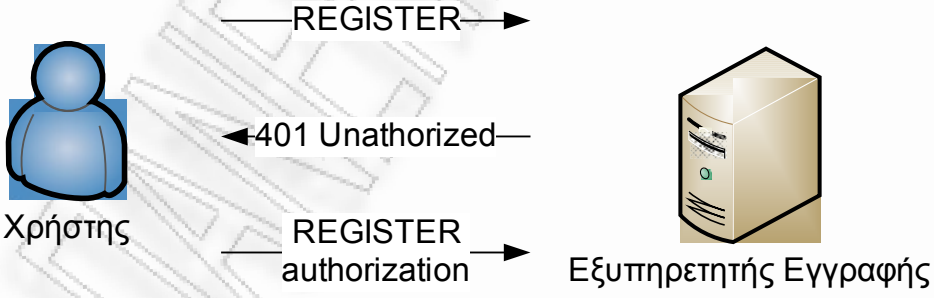
4.1.3 HTTP Αυθεντικοποίηση

Το SIP παρέχει την δυνατότητα πρόκλησης-απάντησης, βασισμένη στην HTTP αυθεντικοποίηση , που στηρίζεται στους κωδικούς των αποκρίσεων 401 και 407 όπως και στα πεδία επικεφαλίδας για τη μεταφορά εμπιστευτικών κωδικών. Χωρίς σημαντικές διαφοροποιήσεις , η χρησιμοποίηση της HTTP Digest αυθεντικοποίησης στο SIP επιτρέπει την προστασία από επίθεση επανάληψης και επίσης την ενός δρόμου αυθεντικοποίηση .

Στην εφαρμογή αυτής της μεθόδου απαιτείται ύπαρξη εμπιστοσύνης μεταξύ των οντοτήτων που εμπλέκονται στην ανταλλαγή πιστοποιητικών και λοιπών συνθηματικών και επίσης η ασφαλής διαφύλαξη των πιστοποιητικών από τους κατάλληλους εξυπηρετητές.

Η διαδικασία που απαιτείται για την αυθεντικοποίηση μηνυμάτων είναι η παρακάτω :

- Ο χρήστης στέλνει μια αίτηση SIP (για παράδειγμα εγγραφής) προς τον αρμόδιο πληρεξούσιο εξυπηρετητή.
- Ο πληρεξούσιος εξυπηρετητής (εγγραφής) απαιτεί αυθεντικοποίηση της αίτησης που λαμβάνει και αποκρίνεται με ένα μήνυμα απόκριση «401unauthorized» στο οποίο περιλαμβάνονται τα δεδομένα για τη δημιουργία πιστοποιητικών αυθεντικοποίησης
- Με το που λαμβάνει αυτή την απάντηση ο χρήστης στέλνει ένα νέο αίτημα (εγγραφής στο παράδειγμα μας) με τα πιστοποιητικά που δημιούργησε βάση των δεδομένων που έλαβε από το «401unauthorized» μήνυμα.
- Ο πληρεξούσιος εξυπηρετητής (εγγραφής) τελικά υπολογίζει εάν τα πιστοποιητικά είναι έγκυρα και στέλνει το μήνυμα επιτυχίας «200 OK».



Σχήμα 29. Αυθεντικοποίηση σε αίτημα εγγραφής

Ο συγκεκριμένος μηχανισμός ασφάλειας μπορεί να χρησιμοποιηθεί σε όλα τα μηνύματα SIP εκτός των SIP CANCEL και SIP ACK, στα οποία απαιτείται διαφορετική μέθοδο διαχείρισης.

4.1.4 S/MIME Secure Multipurpose Internet Mail Extension

Η κρυπτογράφηση ολόκληρων των SIP μηνυμάτων από αρχή μέχρι τέλος , όπως ειπώθηκε και παραπάνω, δεν είναι κατάλληλη διότι οι ενδιάμεσοι πληρεξούσιοι εξυπηρετητές πρέπει να έχουν πρόσβαση σε συγκεκριμένα πεδία επικεφαλίδων ώστε να γίνεται η σωστή δρομολόγηση των μηνυμάτων αυτών.

Όμως , το SIP δίνει την δυνατότητα να δημιουργούνται μηνύματα τα οποία στο κύριο μέρος να περιέχουν επιπρόσθετα MIME μηνύματα τα οποία μπορούν να χρησιμοποιηθούν και για την προστασία των μηνυμάτων SIP .

S/MIME μέθοδος 1η

Αυτό μπορεί να επιτευχθεί με κρυπτογράφηση του MIME κυρίους μέρους παρέχοντας από την αρχή έως το τέλος εμπιστευτικότητα και ακεραιότητά του , καθώς και αμοιβαία αυθεντικοποίηση. Δηλαδή , ένα τμήμα ή ολόκληρο του SIP μηνύματος ενσωματώνεται στο MIME μέρος του SIP μηνύματος το οποίο έχει την ηλεκτρονική υπογραφή του χρήστη με την χρήση του ηλεκτρονικού κλειδιού. Η ηλεκτρονική υπογραφή ενσωματώνεται στο κύριο μέρος του μηνύματος μαζί με το MIME μέρος. Η ελάχιστη απαίτηση για τον αλγόριθμο της ψηφιακής υπογραφής είναι ο SHA1 , ενώ για την κρυπτογράφηση ο 3DES. Κάθε S/MIME μέρος θα πρέπει να έχει μια μόνο ηλεκτρονική υπογραφή και παράλληλες υπογραφές δεν πρέπει να χρησιμοποιούνται. Ένα παράδειγμα βλέπουμε παρακάτω (οι αστερίσκοι υποδηλώνουν το κρυπτογραφημένο μέρος) :

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Disposition: attachment; filename=smime.p7m
handling=required
**********************************************************
```

```
* Content-Type: application/sdp                          *
*                                                        *
* v=0                                                    *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com    *
* s=-                                                    *
* t=0 0                                                  *
* c=IN IP4 pc33.atlanta.com                              *
* m=audio 3456 RTP/AVP 0 1 3 99                          *
* a=rtpmap:0 PCMU/8000                                   *
**********************************************************
```

S/MIME μέθοδος 2η

Επίσης είναι δυνατό να επιτευχθεί με τη χρήση του S/MIME ένα είδος ακεραιότητας και εμπιστευτικότητας για τα πεδία των SIP επικεφαλίδων μέσω τούνελ – διόδου. Αυτό μπορεί να συμβεί με το να συμπεριληφθούν στο κύριο μέρος του μηνύματος τα πεδία που πρέπει να προστατευτούν. Τα πεδία αυτά δεν θα παρουσιαστούν στις κεφαλίδες του μηνύματος αλλά και ακόμα που χρειαστεί να εμφανιστούν θα διατηρούν την ανωνυμία τους όπως πχ. «`From: Anonymous <sip:anonymous@atlanta.com>;`». Όμως η πραγματική ταυτότητα βρίσκεται κρυπτογραφημένη στο MIME σώμα. Παρακάτω βλέπουμε ένα τέτοιο μήνυμα (οι αστερίσκοι υποδηλώνουν το κρυπτογραφημένο μέρος):

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Anonymous <sip:anonymous@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Date: Thu, 21 Feb 2002 13:02:03 GMT
Contact: <sip:pc33.atlanta.com>
Content-Type: multipart/signed;
protocol="application/pkcs7-signature";
micalg=sha1; boundary=boundary42
Content-Length: 568
--boundary42
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
handling=required
Content-Length: 231
**********************************************************
* Content-Type: message/sip                              *
*                                                        *
* INVITE sip:bob@biloxi.com SIP/2.0                      *
* Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8  *
* To: Bob <bob@biloxi.com>                               *
```

```
* From: Alice <alice@atlanta.com>;tag=1928301774                *
* Call-ID: a84b4c76e66710                                       *
* CSeq: 314159 INVITE                                           *
* Max-Forwards: 70                                              *
* Date: Thu, 21 Feb 2002 13:02:03 GMT                           *
* Contact: <sip:alice@pc33.atlanta.com>                         *
*                                                               *
* Content-Type: application/sdp                                 *
*                                                               *
* v=0                                                           *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com           *
* s=Session SDP                                                 *
* t=0 0                                                         *
* c=IN IP4 pc33.atlanta.com                                     *
* m=audio 3456 RTP/AVP 0 1 3 99                                 *
* a=rtpmap:0 PCMU/8000                                          *
*****************************************************************

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s;
handling=required
ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756
--boundary42-
```

4.2 Περιορισμοί των υπαρχόντων μηχανισμών ασφαλείας

Αν και οι υπάρχοντες μηχανισμοί ασφάλειας όταν εφαρμοστούν σωστά αντιμετωπίζουν τις απειλές σε κάποιο βαθμό , υπάρχουν περιορισμοί που πρέπει να είναι αντιληπτοί για την ομαλή λειτουργία ενός SIP συστήματος.

Όσο αναφορά την μέθοδο **HTTP Digest** αυθεντικοποίησης ένας περιορισμός εντοπίζεται στο ότι ο μηχανισμός ακεραιότητας δεν λειτουργεί πολύ καλά για το SIP . Πιο συγκεκριμένα , παρέχεται προστασία στην αίτηση του αναγνωριστικού URI και στην μέθοδο του μηνύματος αλλά όχι και στα άλλα πεδία των επικεφαλίδων που πιθανώς να θέλει να προστατέψει ο χρήστης. Ένας άλλος περιορισμός είναι η μη αποτελεσματική προστασία σε επιθέσεις

επανάληψης . Επίσης , αυτή η μέθοδος είναι χρήσιμη όταν ο χρήστης θέλει να κάνει αυθεντικοποίηση με μια πηγή η οποία έχει ήδη σχέσεις εμπιστοσύνης μεταξύ του, όπως για παράδειγμα ένας χρήστης με τον πάροχο της υπηρεσίας του.

Στην περίπτωση του **IPSec** έχουμε παροχή υπηρεσιών ακεραιότητας , εμπιστευτικότητας και αυθεντικότητας από βήμα σε βήμα με μεγαλύτερη επιτυχία από την μέθοδο **HTTP Digest.** Όμως και σε αυτή την περίπτωση υπάρχει το θέμα της προϋπαρξης σχέσεων εμπιστοσύνης μεταξύ των κόμβων που επικοινωνούν. Ένα άλλο πρόβλημα είναι ότι για να εφαρμοστεί σωστά στο SIP απαιτείται σαφής μηχανισμός ορθής διαχείρισης κλειδιών .

Σχετικά με το «**TLS»** ο πιο συνηθισμένος περιορισμός είναι ότι δεν μπορεί να τρέξει με το πρωτόκολλο **UDP** το οποίο χρησιμοποιείται σε μεγάλο βαθμό για την μεταφορά πολυμεσικών δεδομένων διότι παρόλο που δεν είναι τόσο αξιόπιστο όσο το TCP είναι πιο γρήγορο . Επίσης μπορεί να είναι δύσκολο επεξεργαστικά για κάποιον εξυπηρετητή να διατηρήσει μακράς διάρκειας κλήσεις «TLS» με πολλούς συνδρομητές. Ακόμα, το «TLS» επιτρέπει τις οντότητες SIP να αυθεντικοποιούνται μόνο μεταξύ γειτονικών οντοτήτων, αφού επιτρέπει την βήμα-βήμα ασφάλεια.

Σχετικά με το **SIPS URI** αναγνωριστικό χρησιμοποιεί το «TLS» για να διαφυλάξει το ένα μέρος του μονοπατιού , αλλά στο τελευταίο βήμα για την παράδοση στο τελικό αποδέκτη χρησιμοποιούνται διαφορετικοί μηχανισμοί ασφαλείας. Για το λόγο αυτό δεν μπορεί να εγγυηθεί το SIPS URI ότι η χρήση του «TLS» θα γίνεται σε όλη την διαδρομή του μηνύματος. Επίσης , είναι πολύ πιθανό να μην υποστηρίζουνε και αρκετές τερματικές συσκευές το «TLS».

(Κάποια από τα λογισμικά που υποστηρίζουνε TLS και ενσωματώνονται σε προσωπικούς υπολογιστές ή τηλέφωνα είναι τα εξής : Το Bria (από το 2.4) λογισμικό τηλέφωνο , το λογισμικό Symbian S60 σε τηλέφωνα Nokia N95, N82, E51, E71, E72 και άλλα, το τηλέφωνο SNOM 190,αλλά και άλλων σειρών

όπως τα snom300 series, snom800 series, snomMP, snomM9, snomPA1 , με το τηλέφωνο Polycom SoundPointIP 501, Linksys SPA942 και SPA962 [http://wiki.freeswitch.org/wiki/SIP_TLS])

Το Ασφαλές MIME **(S/MIME)** θεωρείται ένας από τους πιο ολοκληρωμένους μηχανισμούς ασφαλείας, που είναι ικανός να υποστηρίξει υπηρεσίες ασφάλειας για αυθεντικότητα, ακεραιότητα, εμπιστευτικότητα με μεγάλη επιτυχία. Η βασική αδυναμία του μηχανισμού αυτού είναι η έλλειψη κατάλληλων υποδομών δημοσίου κλειδιού για τελικούς χρήστες. Εάν τα πιστοποιητικά δεν μπορούν να είναι πιστοποιημένα από έναν από τους συμμετέχοντες στη συνομιλία υπάρχει ο κίνδυνος της επίθεσης ενδιάμεσου κακόβουλου χρήστη ο οποίος μπορεί να τροποποιήσει και να αποκωδικοποιήσει το σώμα του S/MIME. Ο κακόβουλος χρήστης μπορεί να υποκλέψει τα κλειδιά από την αρχική ανταλλαγή μεταξύ των δύο οντοτήτων τροποποιώντας κατάλληλα τις ηλεκτρονικές υπογραφές. Έτσι, ενώ κάθε πλευρά θα πιστεύει ότι έχει ανταλλάξει με ασφάλεια κλειδιά , στην πραγματικότητα έχει το δημόσιο κλειδί του επιτιθέμενου ενδιάμεσου. Είναι σημαντικό να αναφέρουμε ότι για να επιτύχει ο ενδιάμεσος κακόβουλος χρήστης αυτήν την επίθεση , χρειάζεται να υποκλέψει τα κλειδιά στην αρχική ανταλλαγή αλλιώς η προσπάθεια του να παραποιήσει το κλειδί μπορεί να γίνει αντιληπτή από τους τελικούς χρήστες. Επίσης , η επιβάρυνση στο υπολογιστικό και δικτυακό φόρτο μπορεί να είναι αρκετά μεγάλη εξαιτίας του μεγάλου μεγέθους των μηνυμάτων και της κρυπτογράφησης που χρησιμοποιείται. Άλλη μια σημαντική αδυναμία του S/MIME μηχανισμού βρίσκεται στις τερματικές συσκευές . Στην περίπτωση που ένας χρήστης που με τον οποίο είναι συνδεδεμένο ένα κλειδί μετακινηθεί σε μια άλλη συσκευή θα είναι δύσκολο να μεταφερθεί το κλειδί αυτό με ασφάλεια . Επιπλέον, οι τερματικές συσκευές που υποστηρίζουν το μηχανισμό αυτό είναι ελάχιστες . Από τα έξυπνα κινητά τηλέφωνα μόνο το «Blackberry» προς το παρόν το υποστηρίζει.

(http://us.blackberry.com/ataglance/security/products/smime.jsp)

5. Η λύση των Οριακών Ελεγκτών Συνόδου SBC(session border controllers)

Ένας **session border controller** (SBC) είναι μια συσκευή που χρησιμοποιείται κυρίως στα VoIP δίκτυα ώστε να εξασφαλιστεί ο έλεγχος στην σηματοδοσία αλλά και στα πολυμέσα κατά την αρχικοποίηση , διάρκεια και τερματισμό μιας διαδικτυακής κλήσης.

Εικόνα: Οριακός Ελεγκτης Συνόδου «SBC» Acme Packet's Net-Net 4250

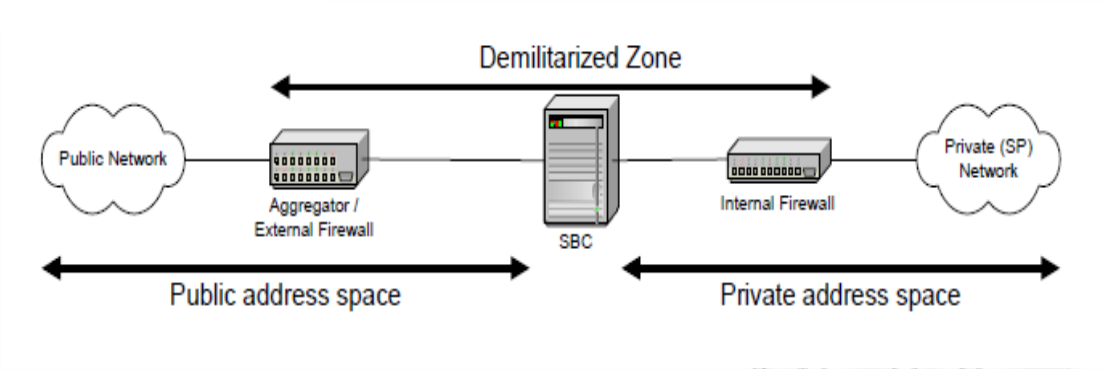
5.1 Επισκόπηση λειτουργίας των SBC

Σε αυτό το κεφάλαιο θα περιγράφει το εύρος λειτουργίας που παρέχεται σήμερα από τους SBCs ή που στοχεύετε να αναπτυχθεί στο κοντινό μέλλον. Δεν εκτελούν όλα τα SBCs που κυκλοφορούν στην αγορά όλες αυτές τις λειτουργίες. Πράγματι, υπάρχουν σχεδόν τόσες διαφορετικές ομάδες λειτουργιών όσα προϊόντα SBC.

5.1.1 Ανάπτυξη της αποστρατικοποιημένης ζώνης (demilitarized zone)DMZ

Το SBC εκτελεί διάφορες λειτουργίες για να εξασφαλίσει τα όρια του δικτύου του παρόχου υπηρεσιών (Service Provider).

- Λειτουργεί σαν μεταφραστής της διεύθυνσης δικτύου [NAT] για τον πάροχο.
- Μπορεί επίσης να δρα σαν τείχος προστασίας ή να συνεργάζεται με υπάρχουσες διατάξεις-μηχανισμούς προστασίας στη DMZ. Μπορεί να ανοίγει «τρυπούλες» στο τείχος προστασίας για να επιτρέψει στη σηματοδοσία του VoIP και των πολυμέσων για να περάσουν [ή εναλλακτικά , να είναι στατικά σχεδιασμένο έτσι ώστε να το επιτρέπει].
- Εκτελεί λειτουργία απόκρυψης τοπολογίας για να εμποδίσει τους συνδρομητές ή άλλους παρόχους από το να μαθαίνουν λεπτομέρειες για το πώς είναι διαμορφωμένο το δίκτυο, ή πως δρομολογούνται οι κλήσεις μέσω του παρόχου . Το κάνει αυτό με την επανεγγραφή των μηνυμάτων κλήσεων VoIP που το διασχίζουν [για παράδειγμα, με τη διαγραφή των SIP Via επικεφαλίδων.]
- Εξαλείφει κακόβουλη σηματοδοσία VoIP και πρωτόκολλα πολυμέσων στα όρια του δικτύου. Αυτό λειτουργικά προσφέρεται από όλα τα SBCs.



Σχήμα 30. Αποστρατικοποιημένης Ζώνης (DMZ)

5.1.2 Διάβαση τείχους προστασίας και NAT

Το SBC κάνει τη σηματοδοσία και τα media του VoIP να ληφθούν και να διευθυνθούν σε μια συσκευή πίσω από ένα τείχος προστασίας και ένα NAT {Network Address Translator} στα όρια ενός γειτονικού δικτύου, χωρίς να χρειαστεί παραμετροποίηση ή αναβάθμιση της συσκευής ή του τείχους προστασίας. Εν συντομία, το SBC επιτυγχάνει αυτό με την επανεγγραφή της διεύθυνσης IP και των θυρών στις επικεφαλίδες της σηματοδοσίας των κλήσεων και των SDP προστιθέμενα σε αυτά τα μηνύματα. Αυτή η λειτουργικότητα προσφέρεται επίσης από όλα τα SBCs.

5.1.3 Αποδοχή ελέγχου κλήσης «call admission control CAC» και προστασία άρνησης υπηρεσίας «DoS»

Η συσκευή ενός οριακού ελεγκτή συνόδου – σηματοδοσίας «SBC-SIG ελέγχει ποιες κλήσεις μπορούν να σηματοδοτηθούν μέσω του δικτύου, και απορρίπτει κλήσεις που δεν είναι αναγκαίες. Αυτό χρησιμεύει στην προστασία του παρόχου ,και ειδικά των τηλεφωνικών κέντρων-«soft switches» στο δίκτυο των παρόχων, από τα ακόλουθα:

• Διάφορους τύπους επιθέσεις άρνησης υπηρεσίας «Denial-of-Service» [DoS] που μπορεί να διαπράττονται στο δίκτυο

• Μαζικές αυξήσεις στον ρυθμό αιτήσεων ρύθμισης των εισερχομένων κλήσεων, που μπορεί να είναι αποτέλεσμα κατακλυσμικών γεγονότων, διαγωνισμών στην «TV» ή το ραδιόφωνο κ.ο.κ

• Γενική συμφόρηση στο δίκτυο

Η συσκευή του «SBC-SIG» το επιτυγχάνει αυτό με την μείωση της ροής των κλήσεων που γίνονται μέσα από αυτή, ανά συνδρομητή και ανά ομάδα συνδρομητών , και επίσης με τη μείωση του ρυθμού των απαγορευμένων κλήσεων σε συγκεκριμένους αριθμούς.

Η «CAC» επίσης, επιτρέπει στον οριακό ελεγκτή συνόδου – σηματοδοσίας «SBC-SIG» να εγγυηθεί και να επιβλέψει τη συμφωνία επιπέδου υπηρεσίας «service level agreement SLA» που τηρούν οι πάροχοι , και να βεβαιώσει ότι οι συνδρομητές κρατούν τις ρυθμίσεις των κλήσεών τους εντός ορίων που μπορεί να χειριστεί το σύστημα.

Επιπλέον, παρακολουθεί το εύρος ζώνης που καταναλώνεται ανά συνδρομητή στο δίκτυο πρόσβασης. Απορρίπτει νέες κλήσεις από εκείνο τον συνδρομητή αν αυτές ξεπερνούν το όριο εύρους που τίθεται από την συμφωνία επιπέδου υπηρεσίας «SLA» τους.

Ακόμη, επιβλέπει τον συνολικό αριθμό των κλήσεων ανά συνδρομητή , ξανά για να εμποδίσει τον συνδρομητή να ξεπεράσει τα όρια που υπάρχουν στην «SLA» τους.

Ο «SBC-SIG» μπορεί επίσης να σχεδιασθεί να επιτρέπει ορισμένους αριθμούς{ π.χ. αριθμούς επειγόντων υπηρεσιών}, έτσι ώστε να επιτρέπουν αυτές τις κλήσεις από το δίκτυο. Μπορεί προληπτικά να απορρίπτει μη επείγουσες κλήσεις για να εξασφαλίσει ότι ικανοποιητικοί πόροι του δικτύου μπορούν να αφιερωθούν σε μία επείγουσα κλήση.

Η αποδοχή ελέγχου κλήσης «CAC» είναι βασική λειτουργία που προσφέρεται από όλες τις «SBC's» {αν και , μέχρι σήμερα, η ποιότητα και ευελιξία της CAC

που προσφέρεται από τις συσκευές «SBC» είναι αρκετά μειωμένη, και αφήνει αρκετά περιθώρια για βελτίωση στις διατάξεις του μέλλοντος }.

Η λειτουργία αποδοχή ελέγχου κλήσης «CAC» είναι πρωτίστως αυτό που διαφοροποιεί τις «SBC's» από τις Πύλες Στρώματος Εφαρμογής «ALGs».

5.1.4 Ποιότητα υπηρεσίας «QoS»

Ο «SBC» χρησιμοποιεί τις υπηρεσίες των στοιχείων του δικτύου του παρόχου για να διαχειρίζεται τις κλήσεις που δημιουργούνται. Υπάρχουν πολλοί τρόποι με τους οποίους η SBC μπορεί να το κάνει αυτό :

- Μπορεί να θέσει τον κωδικό Diff Serv στις επικεφαλίδες IP των πακέτων media που προωθούνται στο δίκτυο .
- Μπορεί να χρησιμοποιήσει μεθόδους όπως «MPLS (Multiprotocol Label Switching) LSP (Label Swithed Path)» για να μεταβάλει τις στάθμες QoS , και να χρησιμοποιήσει τις «LSPs» για την ομαδοποίηση των κλήσεων και την μεταφορά τους κατά μήκος του δικτύου.

Ο οριακός ελεγκτής συνόδου «SBC» επίσης εξοικονομεί το εύρος σηματοδοσίας «signaling bandwidth» για επείγουσες κλήσεις [δηλ. πιστοποιεί ότι ο εξυπηρετητής – «soft switch» πίσω από αυτόν έχει πάντα την ικανότητα να χειρίζεται δεδομένο αριθμό επειγόντων υπηρεσιακών κλήσεων],και δίνει προτεραιότητα σε αυτές τις κλήσεις καταλλήλως [δηλ. τις επιτρέπει μέσα από το «Call Admission Control» , ακόμη και αν άλλες κλήσεις απορρίπτονται].

Κάποιοι «SBCs» παρέχουν αυτή τη λειτουργία ,αλλά όχι όλοι.

5.1.5 Γεφύρωση πολυμέσων

Ο «SBC» πάντα δρομολογεί τα πολυμέσα για κλήσεις που χειρίζεται μέσω της διάταξης «SBC-MEDIA» που μπορεί να περιλαμβάνεται στην ίδια συσκευή με το «SBC-SIG» (single box) ή να βρίσκεται σε ξεχωριστή συσκευή (dual box). Αυτό επιτρέπει στο «SBC» να ελέγχει την απορρόφηση εύρους ζώνης, που απαιτείται για την αστυνόμευση των συμφωνιών «SLAs» και να εμποδίζει την κλοπή του εύρους ζώνης. Οι συσκευές «SBC-SIG» ξαναγράφουν τα «SDP» στα μηνύματα που προωθούν, για να βεβαιώσουν ότι το μήνυμα μιας κλήσης δρομολογείται μέσω της κατάλληλης συσκευής «SBC-MEDIA». Αυτή είναι τότε υπεύθυνη για τη γεφύρωση της ροής των πολυμέσων- «media» στα δύο άκρα της κλήσης.

Η γεφύρωση των πολυμέσων περιλαμβάνει [κατά ελάχιστον] επανεγγραφή των επικεφαλίδων IP στην ροή τους , και μπορεί επίσης να απαιτεί επανακωδικοποίηση τους για να κάνει δυνατή την δια λειτουργία μεταξύ συσκευών ή άλλων ζεύξεων που χρησιμοποιούν διαφορετικές προδιαγραφές.

Αυτή η έντονη λειτουργία του επεξεργαστή λαμβάνει χώρα απευθείας στην κρίσιμη περιοχή υψηλής λειτουργίας μιας διαδρομής δεδομένων , έτσι πρέπει να γίνει πολύ ικανοποιητικά.

Για αυτό , οι συσκευές «SBC-MEDIA» κανονικά χρησιμοποιούν επεξεργαστές δικτύου αφιερωμένους στη γεφύρωση πολυμέσων , και πακέτα προγραμματιζόμενων φίλτρων που εκτελούν τουλάχιστον την επανεγγραφή του τμήματος της «IP» επικεφαλίδας σε αυτή τη διαδικασία.

Σχεδόν όλοι οι «SBCs» παρέχουν αυτή τη λειτουργία, με μερικές σπάνιες εξαιρέσεις .

Γεφύρωση «Voice over IP media»

Τα «media» «VoIP» μεταφέρονται από το πρωτόκολλο «RTP», και έτσι η συσκευή «SBC-MEDIA» πρέπει να υποστηρίζει το RTP, και ειδικά , να εξυπηρετήσει τα πακέτα πολυμέσων RTP.

Το πρωτόκολλο ελέγχου RTCP της RTP ,πρέπει να εξετασθεί από τον SBC ώστε να του επιτρέψει να ελέγχει την χρήση του εύρους ζώνης και τα χαρακτηριστικά ποιότητος στη ροή των πληροφοριών VoIP . Υπάρχουσες διατάξεις SBC-MEDIA υποστηρίζουν μια μεγάλη ποικιλία codecs [κωδικοποιητών- αποκωδικοποιητών]. Για παράδειγμα ο G.711 και ο G.729 [όπως καθορίζεται από την ITU-T] είναι δύο codecs που συνήθως υποστηρίζονται. Κάποιοι επίσης υποστηρίζουν την επανακωδικοποίηση για την ενδοδιεργασία του codec.

Γεφύρωση Fax over IP media

Οι περισσότερες συσκευές SBC-MEDIA τώρα υποστηρίζουν δύο τύπους Fax πάνω στην εκπομπή IP , όπως καθορίζεται στις ακόλουθες προδιαγραφές.

- Η προδιαγραφή ITU-T , T.38
- Το πρωτόκολλο της Cisco proprietary Fax Relay

Η έλλειψη υποστήριξης Fax over IP ήταν εμπόδιο στην απορρόφηση πολλών SBC όταν κυκλοφόρησαν αρχικά στην αγορά . Είναι κάπως διαφορετικό από το να υποστηρίζει το Voice over IP,επειδή το Fax over IP media δεν μεταφέρεται από το RTP.

Στην T.38 το Fax media μεταφέρεται χρησιμοποιώντας

- Το UDP-TL, που είναι ένα ελαφρύ πρωτόκολλο για fax media που τρέχει στην UDP,ή
- Μεταφερόμενα media πάνω στη TCP, χρησιμοποιώντας επικεφαλίδες TPKT που παρέχουν το framing.

Κατά την δημιουργία της κλήσης οι συσκευές αποφασίζουν ποια από τα πρωτόκολλα μεταφοράς θα χρησιμοποιήσουν , και επίσης ποιες διευθύνσεις και πόρτες θα χρησιμοποιήσουν για την αποστολή και λήψη της πληροφορίας. Οι SBCs που υποστηρίζουν την T.38 πρέπει να υποστηρίζουν το ένα ή και τα δύο αυτά τα πρωτόκολλα μεταφοράς.

Τα T38 μπορούν να σηματοδοτηθούν από τις H.323,SIP,ή H.248. Στις δυο τελευταίες περιπτώσεις υπάρχουν κάποιες σχετικές προεκτάσεις στο πρωτόκολλο SDP, που καθορίζονται στην T.38. Αυτές οι προεκτάσεις επιτρέπουν στις εφαρμογές να διαπραγματεύονται διάφορες παραμέτρους ειδικές για φάξ ,καθώς και η επιλογή της TCP ή UDP ,και η επιλογή της διεύθυνσης IP και της θύρας για μεταφορά των media.

Γεφύρωση Modem over IP media

Παρομοίως, οι περισσότεροι SBCs υποστηρίζουν το Modem over IP, όπως καθορίζεται στην οδηγία V.150.1 της ITU-T. Πάλι αυτό διαφέρει από την κυκλοφορία φωνής στο ότι modem των media δεν μεταφέρεται από το RTP. Αντί αυτού, μεταφέρεται από ένα προσαρμοσμένο πρωτόκολλο μεταφοράς [που καθορίζεται στην V.150.1 ειδικά για αυτό το λόγο] και ονομάζεται SPRT [Simple Packet Relay Transport].

Επιπροσθέτως ,η V.150.1 απαιτεί ότι η υποστήριξη του SBC

- Η μεταφορά των DTMF, τόνων τηλεφωνίας και τηλεφωνικών σημάτων in-band εντός των RTP media [RFC2833] παράλληλα με τα modem media, και
- ένα ταιριαστό πρωτόκολλο σηματοδοσίας μέσα στη μπάντα που καθορίζεται στη V.150.1 και ονομάζεται State Signaling Event Protocol [SSEP], που λειτουργεί στο RTP με παραπλήσιο τρόπο με αυτόν που καθορίστηκε στο RFC 2833.

Έχουν γίνει συζητήσεις στην ITU-T και στην TIA [Telecommunications Industry Association] σχετικά με το να επιτρέπεται ενδολειτουργία μεταξύ των media streams V.150.1 και T.38 . Για αυτό το λόγο, είναι επιθυμητό για τη μετατροπή ενός codec που υποστηρίζει ένας SBC επίσης να υποστηρίζει μεθόδους για ενδολειτουργία των V.150.1 – T.38.

5.1.6 Ανοχή σφάλματος «Fault Tolerance»

Τα πιο πολλά «SBCs» έχουν ανοχή στα σφάλματα υλικού.

• Στην πλειοψηφία των αναπτύξεων, υπάρχουν εφεδρικές συσκευές «SBC» για κάθε δίκτυο πρόσβασης . Όλοι οι SBCs παρέχουν μηχανισμό εφεδρείας 1/1, και οι περισσότεροι φορείς θέλουν οι SBC τους να υποστηρίζουν μηχανισμό εφεδρείας 1/N

• Κάποια «SBCs» δυναμικά επαναλαμβάνουν την πληροφορία κατάστασης ο ένας στον άλλον, για παράδειγμα τις διευθύνσεις των «pinholes» στο εξωτερικό των τειχών προστασίας του πελάτη. Αυτό για να συνεχίσει να επιτρέπει την κυκλοφορία «VoIP» να περνάει το τείχος προστασίας του πελάτη πριν ανανεωθεί το «pinhole» του τείχους προστασίας έτσι ώστε να προσφέρει αδιάκοπη λειτουργία στον πελάτη.

• Οι «SBCs» επίσης πρέπει να εφαρμόζουν κάποιο μηχανισμό για να αποφασίζει ποια συσκευή είναι η κύρια, δηλαδή ποια συσκευή έχει τη διεύθυνση IP για το κοινό στην οποία οι πελάτες απευθύνουν τις κλήσεις. Αυτό μπορεί να γίνει ή μέσω κάποιας διεπαφής , ή μέσω ενός σταθερού πρωτοκόλλου εφεδρείας-διαθεσιμότητας όπως το «VRRP» [Virtual Router Redundancy Protocol].

• Κάποιοι «SBCs» υποστηρίζουν την αναβάθμιση λογισμικού ενώ είναι σε λειτουργία ([HSU] Hot Software Upgrade και το [HSD] Downgrade).

Όταν ένας «SBC» εμφανίσει πρόβλημα λειτουργίας οι υπάρχουσες κλήσεις πρέπει να διατηρηθούν ,και η βλάβη να μη γίνει αισθητή από τον χρήστη της υπηρεσίας , ενώ οι κλήσεις σε εξέλιξη απορρίπτονται.

Οι Φορείς απαιτούν οι «SBCs» τους να παρέχουν διαθεσιμότητα 99.999% [πέντε εννιάρια]. Κάθε συσκευή SBC επιπέδου- φορέα πρέπει να καλύπτει αυτή τη διαθεσιμότητα.

5.1.7 Πολιτική δρομολόγησης των κλήσεων

Κάποιοι «SBCs» της αγοράς παρέχουν διεπαφή που επιτρέπει κλήσεις που δεν χρειάζεται να προωθηθούν από τα στοιχεία του δικτύου των παρόχων , αλλά να δρομολογηθούν έξυπνα σε μια έξοδο από το δίκτυο [π.χ. σε ένα από διάφορους υποψήφιους φορείς για κλήσεις μεγάλης απόστασης , και εξαρτάται από το ποιος από τους φορείς είναι φθηνότερος για αυτή την κλήση συγκεκριμένη ώρα της ημέρας].

Αυτή η λειτουργία είναι ισοδύναμη με αυτή που προσφέρεται από ένα τηλεφωνικό κέντρο –«soft switch» . Οι «SBCs» που το κάνουν αυτό βρίσκονται στη «DMZ» του δικτύου και δρομολογούν ορισμένες κλήσεις έξω από το δίκτυο όσο μπορούν πιο γρήγορα, έτσι ώστε οι εξυπηρετητές «soft switches» στον πυρήνα του δικτύου να μην έχουν να αντιμετωπίσουν το φορτίο αυτό.

5.1.8 Δια λειτουργία των πρωτοκόλλων σηματοδοσίας

Όλοι οι «SBCs» υποστηρίζουν το «SIP» .Όλοι επίσης συνήθως υποστηρίζουν και το «H.323». Για τα όρια μεταξύ των παρόχων ,είναι δυνατόν σε έναν «SBC» να παρέχεται δια λειτουργία [όπως μεταξύ της H.323 και του SIP, ή μεταξύ διαφοροποιήσεων της H.323]αν οι πάροχοι χρησιμοποιούν διαφορετικά πρωτόκολλα σηματοδοσίας. Επίσης οι «SBCs» συνήθως υποστηρίζουν το πρωτόκολλο «MGCP» ή και το «Megaco», αν και τυπικά δεν γίνεται καμιά διασυνεργασία που περιλαμβάνει αυτά τα δυο πρωτόκολλα.

5.1.9 Χρέωση κλήσης

Η συσκευή του «SBC-SIG» μπορεί να παρακολουθεί την πρόοδο κάθε κλήσης με σκοπό την χρέωση [αν και πάλι, τα περισσότερα τηλεφωνικά κέντρα «soft switches» θα εκτελούν μια ισοδύναμη λειτουργία].

• Μπορεί να δημιουργούν αναφορές λεπτομερειών κλήσεων «CDRs» [Call Detail Reports], που αναλύουν τις λεπτομέρειες κάθε κλήσης ,που

χρησιμοποιούνται για τη χρέωση και τον σχεδιασμό της χωρητικότητας [μερικοί προμηθευτές «SBC» προσφέρουν εργαλεία λογισμικού για εκ των υστέρων επεξεργασία της «CDRs» που παράγεται από τις μηχανές τους, για υπολογισμό και οπτικοποίηση του φορτίου του δικτύου].

• Μπορεί να τρέξει χρονομέτρη συνόδου, και αποσυνδέει τις κλήσεις που δεν τερματίστηκαν κανονικά

• Μπορεί να δώσει εντολή στο τείχος προστασίας να εμποδίσει κάθε κυκλοφορία «RTP» που δεν είναι συνδεδεμένη με μια ισχύουσα χρεωμένη συνεδρία από την είσοδο στο δίκτυο .Ειδικότερα, κλείνει τη ροή της κυκλοφορίας «RTP» σε μια συνεδρία μόλις σηματοδοτηθεί το τέλος της, για να εμποδίσει **κλοπή υπηρεσίας** [που συμβαίνει όταν οι καλούντες συνεχίζουν να στέλνουν πολυμέσα ακόμη και όταν σηματοδοτήθηκε το τέλος της κλήσης όπως είδαμε σε παραπάνω κεφάλαιο].

Η συσκευή του «SBC-MEDIA» επιβλέπει το εύρος ζώνης κάθε κλήσης στο δίκτυο πρόσβασης, ενώ προφυλάσσει από την κλοπή εύρους ζώνης [που συμβαίνει όταν για παράδειγμα οι καλούντες σιωπηλά αναβαθμίζουν τα «media» τους από, ας πούμε μόνο φωνή σε πλήρες βίντεο, και προσπαθούν να κάνουν βίντεο κλήση στην τιμή της κλήσης φωνής].

Ο σωστός τρόπος λειτουργίας του «SBC-MEDIA» δεν είναι να ακολουθεί την κυκλοφορία «RTP» εκτός εάν ρητά κατευθύνεται να κάνει αυτό από το «SBC-SIG», και τότε μόνο για να προωθήσει κυκλοφορία ειδικού τύπου[π.χ. εντός ορισμένων ορίων εύρους ζώνης ανά συνεδρία].Αυτή η αρχή σχεδιασμού εμποδίζει παράνομα «media» από το να πάρουν πρόσβαση στο δίκτυο του τηλεπικοινωνιακού φορέα.

5.1.10 Σύγκριση των μοντέλων μιας συσκευής «single-box» και δύο συσκευών «dual-box»

Η εσωτερική δομή ενός «SBC» , και των δύο μοντέλων[single-box,dual-box] είναι ισχύουσες αρχιτεκτονικές για τους «SBCs», με διαφορετικά πλεονεκτήματα και μειονεκτήματα για την κάθε μία. Αυτό το τμήμα συγκρίνει

τις δυο προσεγγίσεις ,και συζητά το πώς επιδρούν στη λειτουργία που προσφέρεται από τον «SBC».

5.1.10.1 Οριακοί ελεγκτές συνόδου μιας συσκευής «Single-box SBCs»

Οι περισσότεροι πωλητές σήμερα προσφέρουν τη λύση του «single-box» . Η πλειοψηφία αυτών των συσκευών είναι απλές συσκευές δύο θηρών, με την μια πόρτα αφιερωμένη στο εξωτερικό δίκτυο ,και μια άλλη στο εσωτερικό δίκτυο . Κάθε πόρτα χρησιμοποιείται και για σηματοδοσία και για πολυμέσα. Πάντως, χρησιμοποιώντας την ίδια πόρτα και για σηματοδοσία και για media δημιουργείται υψηλός κίνδυνος απόρριψης πακέτων σηματοδοσίας. Έτσι, ένας περισσότερο εξελιγμένος «SBC» θα προσφέρει πολλαπλές πόρτες, μια ή περισσότερες για σηματοδοσία, και πολλαπλές ξεχωριστές πόρτες για πολυμέσα. Οι πόρτες σηματοδοσίας και πολυμέσων θα ελέγχονται ιδανικά από ξεχωριστούς επεξεργαστές.

Το πλεονέκτημα που έχει η συσκευή «SBC single- box» έναντι της «SBC dual-box» είναι ότι είναι λιγότερο σύνθετες, ποιο εύκολες να κατασκευαστούν, ποιο εύκολες στον προγραμματισμό και την ανάπτυξή τους. Δεν υπάρχει ανάγκη να λειτουργεί πρωτόκολλο επικοινωνίας ή εφεδρείας μεταξύ των δυο διατάξεων ,έτσι αρκεί μια ιδιωτική προγραμματική «API», η οποία δεν απαιτεί έλεγχο δια λειτουργικότητας .

5.1.10.2 Οριακοί ελεγκτές συνόδου μιας συσκευής «Dual-box SBCs»

Κάποιοι πωλητές τώρα προσφέρουν τη λύση «dual-box».

Το μοντέλο αυτό επιτρέπει μεγαλύτερη επεκτασιμότητα. Μια απλή «SBC-SIG» συσκευή μπορεί να χειριστεί κλήση από διάφορα σημεία πρόσβασης, και ελέγχει μια συσκευή «SBC-MEDIA» σε κάθε σημείο πρόσβασης. Οι συσκευές

«SBC-MEDIA» είναι χαμηλότερου κόστους από τις «SBC-SIG» , έτσι αυτό προσβλέπει σε μια ποιο προσιτή λύση σε κάποιες τοπολογίες.

Πάντως, αυτή η προσέγγιση επίσης μειώνει την αποτελεσματικότητα με την οποία η «SBC-SIG» συσκευή μπορεί να αμυνθεί ενάντια στις επιθέσεις άρνησης λειτουργίας «DoS» και άλλες αιχμές στη δραστηριότητα του δικτύου, επειδή εκθέτει μια μονή «SBC-SIG» στην κυκλοφορία σηματοδοσίας από πολλαπλά σημεία πρόσβασης του δικτύου. Για να ικανοποιεί ένας «SBC» την βασική απαίτηση της προστασίας του πυρήνα του δικτύου από επιθέσεις «DoS» , κάθε συσκευή «SBC-SIG» πρέπει να εκτίθεται σε τμήμα μόνο του συνολικού φορτίου σηματοδοσίας του δικτύου, και έτσι η κάθε μια θα μπορεί να διαχειριστεί μόνο μικρό αριθμό «SBC-MEDIA» διατάξεων.

Το πλεονέκτημα αυτού του μοντέλου είναι ότι επιτρέπει ξεχωριστή ανάπτυξη των δια λειτουργικών διατάξεων .Επομένως, μια εταιρία μπορεί να ειδικεύεται στον ένα τύπο ή τον άλλο. Υπάρχουν πρότυπα που αναπτύσσονται που επιτρέπουν τη δια λειτουργικότητα μεταξύ των διατάξεων «dual-box» (κυρίως από τη Multiservice Switching Forum[MSF])

Ένα άλλο πλεονέκτημα είναι ότι, όπου διάφορες διατάξεις «SBC-MEDIA» υπηρετούν ένα δίκτυο μόνο, η συσκευή «SBC-SIG» μπορεί να φορτώσει εξισορροπημένες κλήσεις σε αυτές. Αυτό αυξάνει την επεκτασιμότητα των υπηρεσιών που μπορούν να προσφερθούν σε ξεχωριστούς πελάτες.

Τελικά, η αρχιτεκτονική της «dual-box SBC» προσφέρει την ευκαιρία της υπαγωγής της λειτουργίας «SBC-SIG» στα τηλεφωνικά κέντρα – «soft switches» των τηλεπικοινωνιακών παρόχων. Αυτό προσφέρει προφανή πλεονεκτήματα από την άποψη της μείωσης του αριθμού των συσκευών που απαιτούνται στο δίκτυο, μειώνοντας την πολυπλοκότητα και την δαπάνη λειτουργικότητας και συντήρησης. Πάντως, εντείνει τα μειονεκτήματα που περιγράφηκαν για την αρχιτεκτονική «dual-box». Το «soft switch» το ίδιο είναι τώρα υπεύθυνο για τον φόρτο εργασίας που αφορά στη διαχείριση των διατάξεων «SBC-MEDIA» [δεσμεύουν δυνητικά περισσότερο ακριβούς πόρους από ότι χρειάζεται] και εκτίθεται απευθείας σε πιθανή Άρνηση Υπηρεσίας (Denial of Service) ή περιστατικά υπερφόρτωσης.

5.1.11 Μοντέλα διαμόρφωσης

Οι υπάρχουσες διατάξεις «SBC» διαμορφώνονται – παραμετροποιούνται χρησιμοποιώντας διάφορες μεθόδους.

- Διεπαφή γραμμής εντολών «CLI [command line interface]»
- Διαχείριση «MIB» μέσω του πρωτοκόλλου «SNMPv3» [Οι SNMPv2 και v1 μπορεί να είναι επιθυμητές αλλά συνήθως θεωρούνται προαιρετικές]
- Διαμόρφωση διεπαφής χρήστη διαδικτιακής τεχνολογίας «Web based GUI» χρησιμοποιώντας «XML» και «SOAP».
- «COPS [common open policy service]».
- Διαμόρφωση μέσω διεπαφής «COBRA».

Από αυτές η ποιο κοινή είναι η παραμετροποίηση χρησιμοποιώντας τη γραμμή εντολών «CLI» μέσω telnet, ακολουθούμενη από τη SNMP.

5.2 Επεξεργασία DMZ

Η «DMZ demilitarized zone» είναι η αποστρατικοποιημένη ζώνη μεταξύ δύο δικτύων . Παρακάτω θα δούμε περισσότερες λεπτομέρειες για τον ρόλο του «SBC» στη «DMZ».

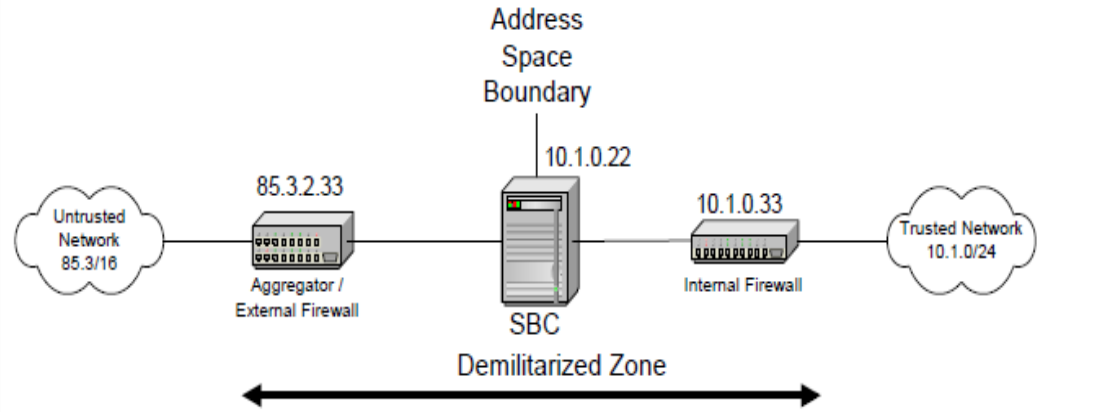
5.2.1 Διατάξεις στην DMZ

Όλοι οι «SBCs» εμπίπτουν σε μία από τις ακόλουθες δύο κατηγορίες.

- Αυτοί που δεν εφαρμόζουν επεξεργασία τείχους προστασίας στην «DMZ», αλλά αντί αυτού , επαναπαύονται σε ένα εξωτερικό και εσωτερικό τείχος προστασίας.

• Αυτοί που εφαρμόζουν επεξεργασία τείχους προστασίας [δηλ. που έχουν τείχος προστασίας].

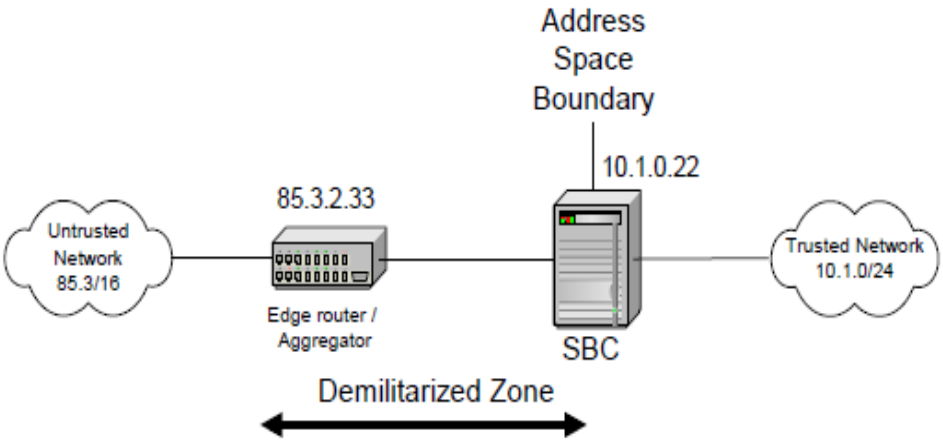
Εάν ένας «SBC» δεν εφαρμόζει επεξεργασία τείχους προστασίας, τότε η «DMZ» είναι έτσι [κοίτα και το σχήμα 31].



Σχήμα 31. Οι SBC και τα τείχη προστασίας είναι διακριτά

Αν ο «SBC» διασπάται στο μοντέλο «dual-box», τότε η συσκευή «SBC-MEDIA» βρίσκεται στη θέση που φαίνεται πιο πάνω, και η συσκευή «SBC-SIG» βρίσκεται στον πυρήνα του δικτύου. Σε αυτή την περίπτωση, η «SBC-SIG» ελέγχει το τείχος προστασίας ώστε να επιτρέπει τη σηματοδοσία των «VoIP» πολυμέσων να περνάνε .

Αν η SBC εκτελεί την λειτουργία του τείχους προστασίας, τότε η ίδια DMZ είναι έτσι [κοίτα επίσης και το σχήμα 32].



Σχήμα 32. Ο «SBC» κάνει τη λειτουργία του τείχους προστασίας

Αν ο «SBC» διασπάται στο μοντέλο «dual-box»,τότε ο «SBC-MEDIA» θέτει σε εφαρμογή ένα τείχος προστασίας που ξεκαθαρίζει την ανεπιθύμητη σηματοδοσία και πακέτα πολυμέσων.
Όλοι οι «SBCs» τυπικά συμπεριλαμβάνουν τη λειτουργία μετάφρασης δικτυακής διεύθυνσης «NAT [Network Address Translator]».

5.2.2 Το τείχος προστασίας

Τα τείχη προστασίας εμποδίζουν ανεπιθύμητη κυκλοφορία να εισέλθει ή να απέλθει από ένα δίκτυο με την εφαρμογή ενός βασικού φιλτραρίσματος πακέτων. Σημειώστε ότι τα τείχη προστασίας φιλτράρουν τα πακέτα εξετάζοντας τις επικεφαλίδες τους , και για να το κάνουν αυτό δεν αναλύουν ή κατανοούν το φορτίο «payload» των πακέτων. Έτσι, δεν φιλτράρουν όλους τους τύπους της ανεπιθύμητης κυκλοφορίας . Για παράδειγμα, τα τείχη προστασίας δεν εκτελούν τον έλεγχο «Call Admission Control» , τον κάνουν όμως οι «SBCs». Πάντως, τα τείχη προστασίας είναι χρήσιμα γιατί φιλτράρουν ικανοποιητικά μεγάλες κατηγορίες ανεπιθύμητης κυκλοφορίας, αφήνοντας τις διατάξεις εφαρμογής όπως οι «SBCs» να κάνουν λιγότερη εργασία.
Το εξωτερικό τείχος προστασίας στο Σχήμα 31 φιλτράρει πακέτα από το εξωτερικό δίκτυο, αλλά επιτρέπει σε όλα τα πακέτα από το εσωτερικό δίκτυο να περνάνε αφιλτράριστα .Το εσωτερικό τείχος προστασίας φιλτράρει πακέτα από το εσωτερικό δίκτυο, αλλά επιτρέπει όλα τα πακέτα από το εξωτερικό δίκτυο να περνούν αφιλτράριστα [αφού έχουν περάσει ήδη το εξωτερικό τείχος προστασίας].
Τα τείχη προστασίας κανονικά δεν δέχονται πακέτα από το δίκτυο, αλλά είναι σχεδιασμένα με κανόνες που τα επιτρέπουν να επιλέγουν και να δέχονται ορισμένα πακέτα. Έτσι, επιτρέπονται πακέτα προς [ή από] το δίκτυο βασισμένα σε αποκλειστικό σχεδιασμό και όχι προκαθορισμένο κανονικό σχεδιασμό.

5.2.3 Η NAT

Οι «SBCs» τυπικά συμπεριλαμβάνουν τη λειτουργία μετάφρασης διευθύνσεων δικτύου «NAT». Η λειτουργία της NAT διαχωρίζει ένα δίκτυο σε ξεχωριστές διευθύνσεις χώρων. Στο σχήμα 31 , η λειτουργία «NAT» του «SBC» διαχωρίζει το διάστημα της εσωτερικής διεύθυνσης του δικτύου 10.1.0/24 από το διάστημα της εξωτερικής διεύθυνσης δικτύου 85.3/16. Λίγες διευθύνσεις του δικτύου 85.3/16 χρησιμοποιούνται για να εκπροσωπήσουν όλες τις μηχανές μέσα στο δίκτυο 10.1.0/24.

Η «NAT» διατηρεί ένα πίνακα αντιστοιχίσεων από την πόρτα εξωτερικής διεύθυνσης στην πόρτα εσωτερικής διεύθυνσης και το ανάποδο. [αυτές οι αντιστοιχίσεις ονομάζονται και "pinholes"] Ο πίνακας είναι διπλού δείκτη, έτσι μία αντιστοίχιση μπορεί να θεωρηθεί είτε σαν εσωτερική είτε σαν εξωτερική πληροφορία διευθυνσιοδότησης . Η «NAT» χρησιμοποιεί αυτόν τον πίνακα για να ξαναγράψει τις επικεφαλίδες των πακέτων IP που προωθεί .

* Με την λήψη ενός πακέτου IP από το εξωτερικό δίκτυο, η «NAT» κοιτάει στους πίνακές της για την διεύθυνση προορισμού και την πόρτα του πακέτου [που θα είναι μια διεύθυνση από τον χώρο εξωτερικών διευθύνσεων].Αν βρεθεί μια αντιστοίχηση, τότε η επικεφαλίδα προορισμού στο πακέτο IP αλλάζει για να συμπεριλάβει την αντίστοιχη εσωτερική διεύθυνση και την πόρτα από τον πίνακα, και το πακέτο προωθείται στο εσωτερικό δίκτυο. Αν δεν βρεθεί αντιστοίχηση, το πακέτο απορρίπτεται.

* Με την λήψη ενός πακέτου IP από το εσωτερικό δίκτυο, η «NAT» κοιτάει στους πίνακές της για την διεύθυνση της πηγής και την πόρτα του πακέτου [η οποία θα είναι μια διεύθυνση από τον εξωτερικό χώρο διευθύνσεων].Εάν βρεθεί μια αντιστοίχηση, τότε αλλάζει η επικεφαλίδα της διεύθυνσης πηγής στο πακέτο IP για να συμπεριλάβει την αντιστοιχούσα εξωτερική διεύθυνση και την πόρτα από τον πίνακα, και το πακέτο προωθείται στο εξωτερικό δίκτυο. Αν δεν βρεθεί αντιστοίχηση, δημιουργείται μια

καινούρια , η «NAT» δυναμικά διαθέτει μια νέα εξωτερική διεύθυνση και πόρτα από τον εξωτερικό χώρο διευθύνσεων για το πακέτο [και όλα τα μελλοντικά πακέτα από αυτήν την πηγή διευθύνσεων και πλειάδας θυρών.] Αντιστοιχήσεις στον πίνακα δημιουργούνται με ένα ή δύο τρόπους.

- Από πακέτα που διασχίζουν τη «NAT» από το εσωτερικό δίκτυο προς το εξωτερικό, όπως περιγράφεται στη δεύτερη κουκκίδα παραπάνω.
- Με διαμόρφωση, ή από τον χειριστή του δικτύου μέσω μιας ανθρώπινης διεπαφής, ή μέσω προγραμματισμού από αξιόπιστο software μέσω ενός API.

5.3 Πως τα πακέτα σηματοδοσίας VoIP διασχίζουν την «DMZ»

Η λειτουργία «NAT» του «SBC» και τα τείχη προστασίας στη «DMZ» ρυθμίζονται ως εξής.

- Η «NAT» διαμορφώνεται με μια αντιστοίχιση μεταξύ της εσωτερικής διεύθυνσης του «SBC» [10.1.0.22 στο σχήμα 31]και της πόρτας που χρησιμοποιεί για σηματοδοσία, και κάποιας διεύθυνσης και πόρτας που παίρνει από τον χώρο διευθύνσεων του εξωτερικού δικτύου. Αυτή η εξωτερική διεύθυνση και πόρτα χρησιμοποιείται για την ταυτοποίηση του «SBC» στο δημόσιο δίκτυο. Πακέτα που αποστέλλονται από το εξωτερικό δίκτυο και προορίζονται για το «SBC» στέλνονται σε αυτή την διεύθυνση και πόρτα.
- Το εξωτερικό τείχος προστασίας διαμορφώνεται να επιτρέπει πακέτα IP των οποίων η επικεφαλίδα διεύθυνσης προορισμού περιέχει την διεύθυνση και την πόρτα που πιστοποιούν τον «SBC» στο εξωτερικό δίκτυο.
- Το εσωτερικό τείχος προστασίας διαμορφώνεται να επιτρέπει πακέτα IP των οποίων η επικεφαλίδα διεύθυνσης προορισμού περιέχει την εσωτερική διεύθυνση του «SBC» ,και την πόρτα που χρησιμοποιεί για σηματοδοσία.

Αυτή η διαμόρφωση επιτρέπει σε όλα τα πακέτα σηματοδοσίας που απευθύνονται προς τον «SBC» να διασχίζουν τις διατάξεις «DMZ» και να φτάνουν στον «SBC», δηλαδή τα πακέτα που προέρχονται από το εσωτερικό ή το εξωτερικό δίκτυο. Επιπροσθέτως, επιτρέπουν στον «SBC» να αποστέλλει μηνύματα σηματοδοσίας προς τα εσωτερικά ή τα εξωτερικά δίκτυα.

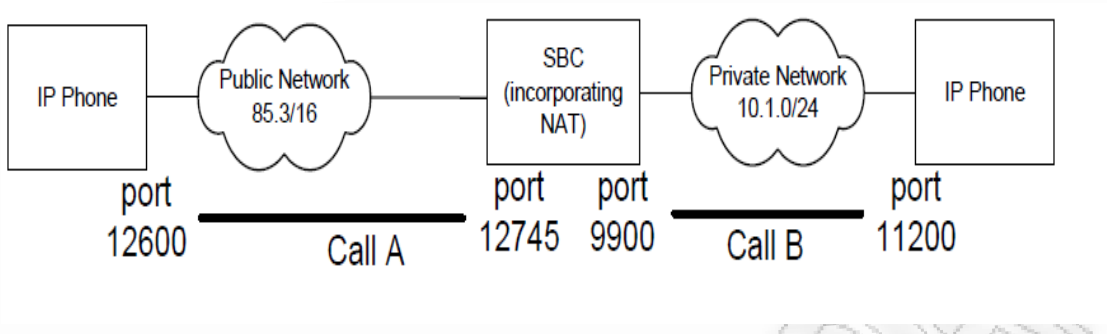
Αυτή η ιδέα έγκειται στο γεγονός ότι η εξωτερική διεύθυνση και η πόρτα που χρησιμοποιείται για να προσδιορίσει τον «SBC» στο δημόσιο δίκτυο για σηματοδοσία είναι καλά γνωστή στις διατάξεις «VoIP» στο δημόσιο δίκτυο. Τυπικά, αυτό επιτυγχάνεται με τη χρήση καταγραφών του «DNS» για τη σύνδεση αυτής της διεύθυνσης με τον «SBC» στο δημόσιο δίκτυο.

Αυτή η ιδέα επίσης έγκειται στο ότι ο «SBC» γνωρίζει την εξωτερική διεύθυνση IP και πόρτα για σηματοδοσία, επειδή πρέπει να τα χρησιμοποιεί στις επικεφαλίδες σηματοδοσίας VoIP που αποστέλλει μετά από αίτηση προς το εξωτερικό δίκτυο [καθώς αυτά τα πεδία συνήθως χρησιμοποιούνται για να δρομολογήσουν την απάντηση της σηματοδοσίας].Αυτό μπορεί να διαμορφωθεί στον «SBC».

5.4 Πως τα πακέτα VoIP media διασχίζουν την DMZ

Η κατάσταση με τα πακέτα «media» είναι λίγο πιο πολύπλοκη από την σηματοδοσία, επειδή τα πακέτα «media» σε δεδομένη κλήση από την οποία προέρχονται, και αποστέλλονται, χρησιμοποιούν διευθύνσεις και πόρτες που δυναμικά καθορίζονται από το πρωτόκολλο της RTP όταν δημιουργείται η κλήση.

Ο «SBC» τερματίζει τα «media» μιας κλήσης και στις δύο πλευρές εσωτερική και εξωτερική του δικτύου. Οι πόρτες που χρησιμοποιεί για να στείλει και να λάβει «media» σε κάθε πλευρά είναι δυναμικά τοποθετημένες όταν δημιουργείται η κλήση.



Σχήμα 33 : Πακέτα media VoIP που διασχίζουν την DMZ

Αυτό προκαλεί δύο προβλήματα.

• Το εσωτερικό τείχος προστασίας πρέπει να ρυθμιστεί ώστε να επιτρέπει την κυκλοφορία IP που αποστέλλεται στην πόρτα 9900 στον «SBC». Επειδή ο 9900 είναι ένας δυναμικά καθοριζόμενος αριθμός, αυτό πρέπει να γίνει αυτόματα κατά τη δημιουργία της κλήσης [δηλ. χωρίς ανθρώπινη παρέμβαση].

• Το εξωτερικό τείχος προστασίας πρέπει να ρυθμιστεί να επιτρέπει κυκλοφορία IP που αποστέλλεται στην εξωτερική διεύθυνση του «SBC» και την πόρτα 12745. Πάλι ,αυτό πρέπει να γίνει αυτόματα κατά την δημιουργία της κλήσης.

Αν το τείχος προστασίας και ο «SBC» βρίσκονται στην ίδια συσκευή, τότε αυτά τα προβλήματα εύκολα θα ξεπεραστούν με την εφαρμογή μιας προγραμματικής διεπαφής που επιτρέπει στον «SBC» να διαμορφώσει δυναμικά το λογισμικό του τείχους προστασίας.

Αν τα τείχη προστασίας είναι ξεχωριστά από την SBC, τότε έχουμε δύο επιλογές:

1. Ο SBC δυναμικά διαμορφώνει το τείχος προστασίας πάνω στο δίκτυο
2. Τα τείχη προστασίας πρέπει να διαμορφώνονται να επιτρέπουν όλη την κυκλοφορία να αποστέλλεται σε κάθε πόρτα του «SBC» [ή

τουλάχιστον, σε κάθε πόρτα στο φάσμα που χρησιμοποιείται από το πρωτόκολλο RTP .

5.5 Άλλες εφαρμογές των «SBCs»στην DMZ

Οι SBC εκτελούν επίσης και άλλες εφαρμογές σχετικές με τη DMZ, όπως περιγράφεται στα ακόλουθα τμήματα.

5.5.1 Απόκρυψη τοπολογίας

Τα μηνύματα σηματοδοσίας VoIP μεταφέρουν πληροφορία που μπορεί να επιτρέπει στον κάτοχό τους να ανακαλύψει την εσωτερική τοπολογία ενός δικτύου, και τον δρόμο που ακολουθεί μια κλήση κατά μήκος του δικτύου[και πιθανή έξοδο από το άλλο άκρο]. Για παράδειγμα, οι επικεφαλίδες Via στα μηνύματα σηματοδοσίας SIP μεταφέρουν αυτό το είδος της πληροφορίας.

Είναι συχνά ανεπιθύμητο να εκτίθεται αυτή η πληροφορία σε χρήστες εκτός δικτύου. Για παράδειγμα, αν είστε πάροχος υπηρεσίας που χρησιμοποιεί ένα δεύτερο πάροχο να ενεργεί σαν φορέας των κλήσεών σας, δεν θέλετε να εκθέσετε την ταυτότητα του φορέα αυτού στους πελάτες σας για να αποφευγχθει η περίπτωση να προσεγγίσουν κατευθείαν τον φορέα αυτόν για να επιτύχουν καλύτερη τιμή.
Για την επίλυση αυτού του προβλήματος, οι «SBCs» μπορούν να αφαιρούν ευαίσθητες πληροφορίες με την επανεγγραφή των επικεφαλίδων VoIP στα μηνύματα σηματοδοσίας που αποστέλλουν κατά μήκος των ορίων του δικτύου. Τερματίζουν την σηματοδοσία VoIP που δέχονται εντός του ιδιωτικού δικτύου, και σηματοδοτούν μια νέα κλήση προς το δημόσιο δίκτυο. Επειδή αυτή είναι μια νέα κλήση, δεν απαιτεί καμιά πληροφορία δρομολόγησης από την προηγούμενη κλήση [για παράδειγμα, καμία από τις επικεφαλίδες SIP Via δεν μεταφέρεται στο τμήμα του δημόσιου δικτύου].

5.5.2 Ανίχνευση κακόβουλων πρωτοκόλλων

Ο «SBC» διαχειρίζεται όλη τη σηματοδοσία και τα media που εισέρχονται και απέρχονται από το δίκτυο .Ως εκ τούτου μπορεί να διαχωρίζει -φιλτράρει το δίκτυο από κακόβουλα πρωτόκολλα στα πακέτα σηματοδοσίας ή πολυμέσων, απορρίπτοντας ή αποστέλλοντας αρνητικές απαντήσεις σε όχι ορθά σχηματισμένα πακέτα. Αυτό έχει δύο πλεονεκτήματα.

1. Μειώνει το φορτίο των εξυπηρετητών VoIP εντός του δικτύου, που μπορεί να είναι σημαντικό αν κάποιος προσπαθήσει να εξαπολύσει επίθεση «DoS» στο δίκτυο με την αποστολή κακόβουλων πακέτων.
2. Μειώνει την πιθανότητα τα κακόβουλα πακέτα να προκαλέσουν κατάρρευση σε κάποιο βασικό κομμάτι της υποδομής VoIP στο δίκτυο όπως το soft switch.

Ο έλεγχος που ένας «SBC» κάνει στα μηνύματα σηματοδοσίας πρέπει να είναι διαμορφώσιμος. Για παράδειγμα, θα μπορούσε να διαμορφωθεί να ελέγχει μόνο εκείνα τα πεδία που ο ίδιος ο «SBC» πρέπει να διεργασθεί στο μήνυμα ,ή θα μπορούσε να ελέγχει όλα τα πεδία στο μήνυμα, ή οπουδήποτε ενδιάμεσα.

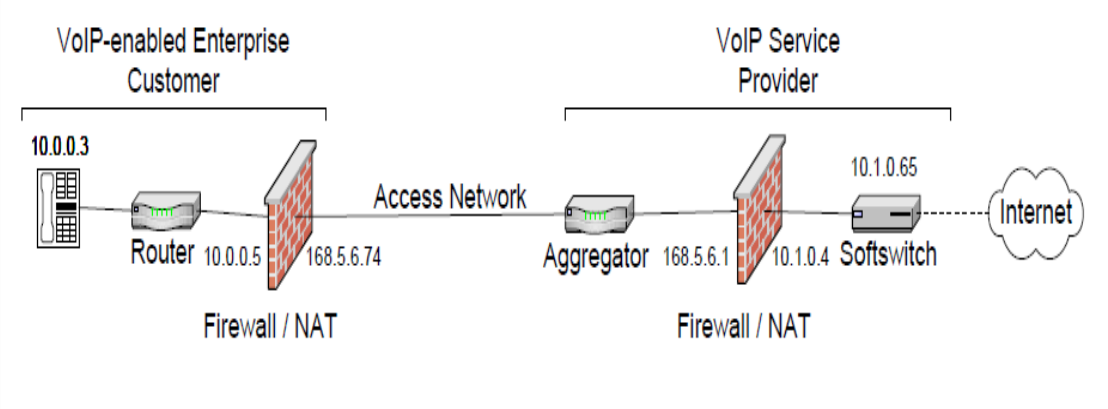
5.6 Διάβαση τείχους προστασίας και NAT

‘Οπως είδαμε παραπάνω οι «SBC» επιτρέπουν την σηματοδοσία και τα πολυμέσα του VoIP να ληφθούν και να διευθυνθούν προς μια συσκευή πίσω από ένα τείχος προστασίας /NAT στα όρια ενός γειτονικού δικτύου, χωρίς να απαιτείται αναβάθμιση της συσκευής ή του τείχους προστασίας. Παρακάτω

θα δούμε την αναγκαιότητα των «SBCs» για την επίλυση του προβλήματος του τείχου προστασίας και του «NAT» αλλά και τις μεθόδους που χρησιμοποιούν οι «SBCs» για να λύνουν αυτό το πρόβλημα

5.1 Το πρόβλημα του τείχους προστασίας VoIP / Διάβαση NAT

Ένα από τα πρώτα εμπόδια για την ανάπτυξη των VoIP είναι ότι τα πρωτόκολλα σηματοδοσίας και πολυμέσων δεν είχανε την δυνατότητα να διασχίσουν το «NAT» και τα τείχη προστασίας χωρίς σημαντική βοήθεια. Το παρά κάτω διάγραμμα είναι μια απλοποίηση ενός δικτύου παρόχου υπηρεσίας VoIP και του πελάτη του.



Σχήμα 34. τείχος προστασίας VoIP / διάβαση NAT

Το δίκτυο του πελάτη έχει τον ιδιωτικό του χώρο διευθύνσεων [10.0.0/24], και προστατεύεται από μία συσκευή τείχους προστασίας /NAT . Η ζεύξη πρόσβασης μεταξύ του πελάτη και του παρόχου είναι το υποδίκτυο 168.5.6/24. Το ίδιο το δίκτυο του παρόχου έχει ιδιωτικό χώρο διευθύνσεων 10.1.0/24, και προστατεύεται πάλι από συσκευή τείχους προστασίας /NAT.
Υπάρχουν δυο προβλήματα με την διευθέτηση αυτού του δικτύου ως προς το VoIP. Απεικονίζουμε αυτά τα προβλήματα χρησιμοποιώντας SIP, παρόμοια προβλήματα υπάρχουν για το H.323 και το MGCP / Megaco.

- Το τείχος προστασίας /NAT του πελάτη μπλοκάρει τη σηματοδοσία των εισερχομένων κλήσεων. Ο εξυπηρετητής «soft switch» στο πάροχο υπηρεσίας δεν μπορεί να στείλει αίτηση SIP INVITE στο IP τηλέφωνο, επειδή το τηλέφωνο δεν είναι διευθυνσιοδοτούμενο από τον πάροχο υπηρεσίας. Ακόμη και αν το τηλέφωνο είχε πάρει IP διεύθυνση από τον πάροχο [δηλ. το τείχος προστασίας του πελάτη δεν χρσιμοποιούσε επίσης NAT],το τείχος προστασίας του πελάτη θα μπλόκαρε ακόμη το μήνυμα INVITE.

Σημειώστε ότι αυτό το πρόβλημα δεν υπάρχει συνήθως στη σηματοδοσία εξερχομένων κλήσεων, επειδή το τηλεφωνικό κέντρο «soft switch» τυπικά θα έχει μια καλά γνωστή εξωτερική διεύθυνση IP, η οποία είναι στατικά απεικονισμένη από το NAT του παρόχου στην εσωτερική διεύθυνση IP [10.1.0.65 στο παραπάνω διάγραμμα]. Το τείχος προστασίας του παρόχου θα ρυθμιστεί να δέχεται αυτόκλητα πακέτα που λαμβάνονται στην εξωτερική διεύθυνση σε ορισμένες πόρτες σχεδιασμένες για κυκλοφορία σηματοδοσίας VoIP [π.χ. η πόρτα 5060 για SIP].

- Το τείχος προστασίας /NAT του πελάτη μπλοκάρει τα πολυμέσα εισερχόμενης κλήσης. Όταν το τηλέφωνο του πελάτη κάνει μια κλήση ,στέλνει μια SIP INVITE με ένα φορέα SDP που περιέχει την διεύθυνση IP .Όταν γίνεται η κλήση, ο καλούμενος στέλνει τα πολυμέσα του σε εκείνη τη διεύθυνση IP. Αυτό προκαλεί προβλήματα επειδή η διεύθυνση IP δεν δρομολογείται από το διαδύκτιο επειδη είναι ιδιωτική ,αλλά ακόμη και αν γινόταν αυτό, το τείχος προστασίας του πελάτη θα μπλοκάριζε πάλι την κυκλοφορία που θα στέλνονταν σε αυτό.

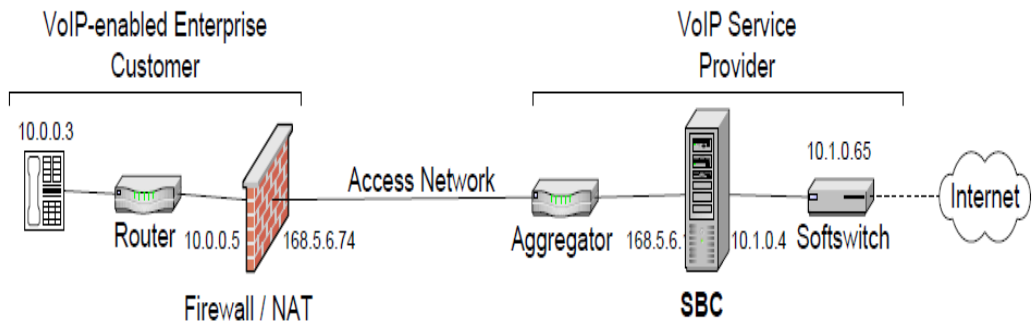
5.7 Λύση τρύπα – «pin hole» στον «SBC»

Το κλειδί της λύσης αυτού του προβλήματος είναι το γεγονός ότι η NAT του πελάτη πρέπει να ανοίξει μικρές τρύπες [pinholes] ώστε να καταστεί δυνατή η

αποστολή από το τηλέφωνο IP πακέτων σηματοδοσίας και «media» προς το δημόσιο δίκτυο, και το τείχος προστασίας του πελάτη πρέπει να επιτρέψει αυτά τα πακέτα να περάσουν. Εισερχόμενες κλήσεις και media από το δημόσιο δίκτυο μπορούν έτσι να διασχίζουν το τείχος προστασίας και το NAT του πελάτη διευθύνοντάς τες στη διεύθυνση της «pin hole» και της πόρτας στην πλευρά του δημόσιου δικτύου και στην πλευρά NAT του πελάτη. Τα «pin holes» για τη σηματοδοσία και τα «media» έχουν διαφορετική διάρκεια ζωής.

- Το «pin hole» σηματοδοσίας, όταν δημιουργηθεί , ξαναχρησιμοποιείται για όλες τις σηματοδοσίες κλήσεων
- Το «pin hole» των media δημιουργείται εκ νέου για κάθε ροή πολυμέσων, επειδή η πηγή και οι πόρτες προορισμού της ροής πολυμέσων δυναμικά διατίθενται ανά κλήση.

Το «pin hole» σηματοδοσίας δημιουργείται όταν το IP τηλέφωνο συνδεθεί στην γραμμή, και μετά κρατείται ανοικτό έως ότου κλείσει το τηλέφωνο . Τα pinhole πολυμέσων δημιουργούνται όταν το τηλέφωνο IP στείλει για πρώτη φορά ένα πακέτο πολυμέσων σε κάθε εγκατεστημένη συνεδρία πολυμέσων.
Για να λύσει το πρόβλημα του τείχους προστασίας VoIP / διάβασης της NAT, ο «SBC» αντικαθιστά το τείχος προστασίας /NAT του παρόχου , όπως φαίνεται πιο κάτω.



Σχήμα 35 : Λύση SBC στο πρόβλημα διάσχισης του τείχους προστασίας /NAT

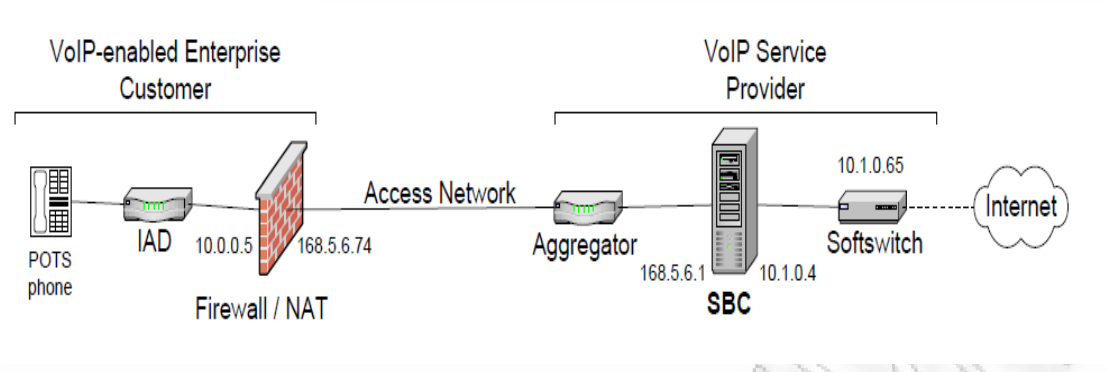
5.7.1 Το pin hole σηματοδοσίας

Στο σενάριο που είναι εικονογραφημένο στο σχήμα 35, το τηλέφωνο IP είναι παραμετροποιημένο με την δημόσια ταυτότητα IP του οριακού ελεγκτή συνόδου SBC ώς πύλη εξόδου για τον εξυπηρετητή SIP. Το IP τηλέφωνο έτσι στέλνει ένα μήνυμα SIP REGISTER στον «SBC» όταν κάνει κλήση το τηλέφωνο. Ο «SBC» τυπικά προωθεί το REGISTER στον εξυπηρετητή soft switch [υποθέτοντας ότι επιτρέπει στο REGISTER να αποκτήσει πρόσβαση στο δίκτυο]. Εσωτερικά επίσης αποθηκεύει μια αντιστοίχιση από το όνομα της συσκευής [π.χ. ipphone@enterprise.com] .Αυτό εξαρτάται από το πρωτόκολλο που χρησιμοποιείται για την μεταφορά της σηματοδοσίας.

- Για σηματοδοσία πάνω από το UDP, ο «SBC» καταγράφει το όνομα της συσκευής στην pinhole της δημόσιας διεύθυνσης και πόρτας, όπως την πληροφορήθηκε από την επικεφαλίδα IP του γραφήματος δεδομένων REGISTER.
- Για σηματοδοσία πάνω από τη TCP [περιλαμβανομένης της TLS], ο «SBC» καταγράφει το όνομα της συσκευής στη σύνδεση TCP που έχει εγκατασταθεί μεταξύ αυτής και του τηλεφώνου IP.

Στη συνέχεια, ο SBC χρησιμοποιεί την καταγραφή-αντιστοίχιση που έχει κάνει για να κατευθύνει εισερχόμενα μηνύματα κλήσεων ή πάνω στην εγκατεστημένη σύνδεση TCP, ή προς την δημόσια διεύθυνση και πόρτα της pinhole για το UPD.

Στο ακόλουθο διάγραμμα δικτύου, το τηλέφωνο IP αντικαταστάθηκε από τηλέφωνο παλιάς τηλεπικοινωνιακής τεχνολογίας και μιας συσκευής πρόσβασης που γεφυρώνει την παλιότερη τεχνολογία με το VoIP (POTS και μια IAD(Integrated Access Device)).



Σχήμα 36. : Λύση SBC με POTS και IAD

Σε αυτή την περίπτωση, δεν στέλνεται SIP REGISTER. Αντί αυτού ,η συσκευή πρόσβασης (IAD) επικοινωνεί με τον SBC χρησιμοποιώντας MGCP [ή Megaco]. στέλνει ένα μήνυμα RSIP στον SBC όταν κάνει εκκίνηση, ο οποίος ανοίγει την pinhole σηματοδοσίας ακριβώς με τον ίδιο τρόπο όπως και με το SIP REGISTER.

5.7.2 Κρατώντας ανοιχτή την pinhole της σηματοδοσίας

Αν ένα τείχος προστασίας δεν βλέπει κυκλοφορία σε μια pinhole για μια περίοδο χρόνου [τυπικά για λίγα λεπτά],θα την λήξει και θα την κλίσει, για να ελαχιστοποιήσει την έκθεση ασφάλειας. Πάντως, για τους σκοπούς του «SBC», όταν ανοίξει μια pinhole, πρέπει να κρατηθεί ανοιχτή το απαιτούμενο διάστημα. Πώς γίνεται αυτό εξαρτάται από το πρωτόκολλο σηματοδοσίας που χρησιμοποιείται.

- Αν το πρωτόκολλο σηματοδοσίας είναι SIP, τότε ο «SBC» περιοδικά στέλνει αιτήσεις OPTIONS στο τερματικό SIP. Κάθε φορά που το κάνει, το τείχος προστασίας του πελάτη επανεκκινεί το χρονομετρητή στην pinhole του, που την κρατάει ανοιχτή. Σημειώστε ότι το τερματικό SIP δεν χρειάζεται να ανταποκρίνεται θετικά στην αίτηση OPTIONS.

- Αν το πρωτόκολλο σηματοδοσίας είναι MGCP, τότε ο SBC περιοδικά στέλνει μηνύματα AUEP στο τελικό σημείο του MGCP ,που έχει το ίδιο αποτέλεσμα στη pinhole του τείχους προστασίας όπως το αίτημα OPTIONS στην περίπτωση του SIP. Ένας παρόμοιος μηχανισμός εφαρμόζεται για το Megaco.

Περαιτέρω ,αν η pinhole σηματοδοσίας κλείσει για οποιοδήποτε λόγο[π.χ. αν το τείχος προστασίας του πελάτη επανεκκινήσει],τότε θα πρέπει να ξανανοίξει χωρίς να απαιτείται να επανεκκινήσει το τερματικό . Αυτό απαιτεί κάποιο επίπεδο συνεργασίας από το τερματικό επειδή η pinhole μπορεί να ανοίξει μόνο μέσα από το δίκτυο των πελατών.

- Αν το SIP είναι σε χρήση, τότε το τηλέφωνο IP περιοδικά στέλνει μήνυμα REGISTER προς τον «SBC». Ο « SBC» περιορίζει αυτά τα μηνύματα REGISTER, και μόνο προωθεί μερικά από αυτά στον υπεύθυνο εξυπηρετητή. Αν το τηλέφωνο IP είναι ρυθμισμένο να κάνει αυτή τη λειτουργία περιορισμού των μηνυμάτων, τότε δεν χρειάζεται ο «SBC» να στέλνει περιοδικά OPTIONS στο τηλέφωνο. Τα περισσότερα [αν όχι όλα] τερματικά SIP μπορούν να ρυθμιστούν να επανεγγράφουν περιοδικά τον εαυτό τους. Για να σιγουρευτούμε ότι τα REGISTERs στέλνονται αρκετά συχνά, μπορούμε να τροποποιήσουμε κατάλληλα τον χρόνο λήξης κάθε REGISTER. Μια συχνότητα από ένα REGISTER για κάθε 30 δευτερόλεπτα απαιτείται τυπικά.

5.8 Τα pinhole των πολυμέσων

Τα πολυμέσα δεν ταξιδεύουν μέσα από τα pinhole σηματοδοσίας, ένα άλλο pinhole απαιτείται να ανοίξει για αυτά. Τα pinhole πρέπει να ανοίγονται μέσα από το δίκτυο του πελάτη Έτσι, το pinhole πολυμέσων ανοίγει όταν ο πελάτης στέλνει το πρώτο πακέτο RTP.

Όταν ο «SBC» λάβει αυτό το πακέτο πολυμέσων, το συσχετίζει με την υπάρχουσα κλήση. Αν αποτύχει να το κάνει αυτό, απορρίπτει το πακέτο[επειδή αυτό μπορεί να είναι προσπάθεια **κλοπής υπηρεσίας**]. Αν πετύχει αυτό, τότε δημιουργεί μια αντιστοίχηση μεταξύ της κλήσης και της εξωτερικής διεύθυνσης της pinhole και της πόρτας στο τείχος προστασίας μέσω της οποίας λήφθηκε το πακέτο RTP [το οποίο μαθαίνει από την επικεφαλίδα IP του πακέτου RTP]. Μετά επαναδιευθύνει κάθε εισερχόμενο πακέτο RTP που ανήκει σε αυτή την κλήση στην εξωτερική διεύθυνση και πόρτα της pinhole.

Η pinhole των πολυμέσων παραμένει ανοιχτή για όσο τρέχουν τα media στην κλήση, και μετά κλείνει στο τέλος της κλήσης. Δεν απαιτείται μηχανισμός διατήρησης, υπό την προυπόθεση ότι τα media εξακολουθούν να ρέουν.

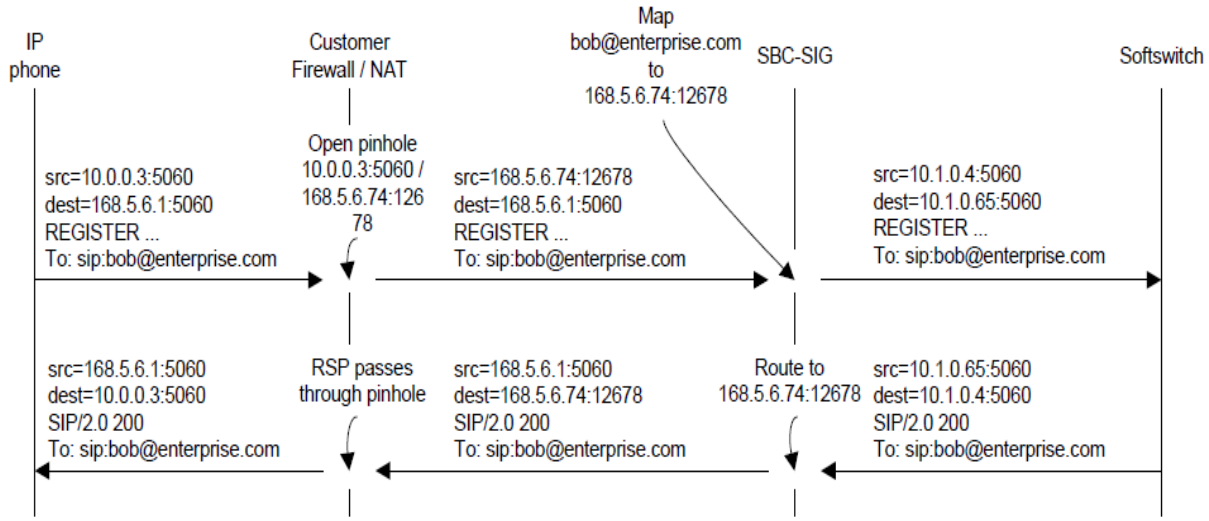
Ένας παράγοντας που μπορεί να περιπλέξει αυτό το σενάριο είναι ότι πολλές κλήσεις περιέχουν κάποιο στοιχείο μονοκατευθυντικής ροής media.

Για παράδειγμα, κλήσεις στο PSTN τυπικά έχουν σαν αποτέλεσμα την πρόωρη ροή media από την πύλη τους πίσω στον καλούντα, σαν τόνος κλήσης στο ακουστικό του καλούντος Η ροή των media είναι προς μια κατεύθυνση. Αν ο καλών είναι πίσω από τείχος προστασίας, τότε [επειδή δεν ρέουν media προς τα έξω από τον καλούντα κατά την πρώτη φάση της κλήσης] η pinhole πολυμέσων δεν θα ανοίξει, και τα πρώτα media δεν θα φτάσουν στον καλούντα.

Για να παρακάμψει αυτό το πρόβλημα, ο SBC ξαναγράφει την SDP που περιγράφει τα πρώιμα media να τα κάνει να φαίνονται στον καλούντα ότι η κλήση είναι αμφίδρομη [με την αλλαγή a=sendonly σε a=sendecv στην SDP]. Ο SBC τερματίζει τη ροή media από τον καλούντα, και διατηρεί μονοκατευθυντική ροή media με την πύλη των media.

5.9 Παράδειγμα ροής SIP

Αυτό το μήνυμα ροής απεικονίζει την Pinhole σηματοδοσία που ανοίχτηκε στο τείχος προστασίας του πελάτη, όταν το SIP είναι το πρωτόκολλο σηματοδοσίας που χρησιμοποιείται. Η διεύθυνση IP που χρησιμοποιείται στην ροή (και σε μεταγενέστερες ροές σε αυτό το τμήμα) ταιριάζει με το διάγραμμα δικτύου στο σχήμα 35.

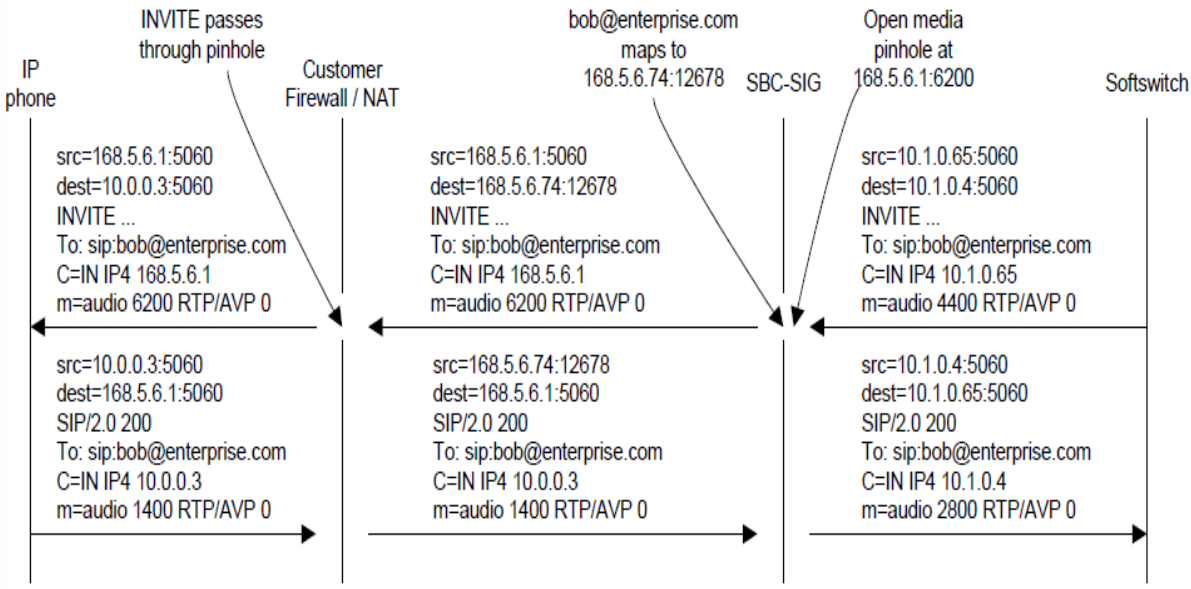


- Το τηλέφωνο του πελάτη στέλνει ένα SIP REGISTER. Το τείχους προστασίας του πελάτη ανοίγει μια pinhole για αυτό και αντιγράφει την επικεφαλίδα του IP καθώς προχωράει στο διάγραμμα.
- Το SBC επίσης συμπεριφέρεται σαν τείχος προστασίας και NAT. Το στοιχείο του τείχους προστασίας του SBC έχει ρυθμιστεί να επιτρέπει τη ροή μέσω συνεχόμενων πακέτων που στέλνονται στην δημόσια διεύθυνση του SBC που φτάνουν στην θύρα 5060.
- Ο SBC με το που λάβει το REGISTER, (i) αναγνωρίζει ότι η απάντηση πρέπει να σταλεί στην εξωτερική διεύθυνση του τείχους προστασίας (αντί για την διεύθυνση που βρίσκεται στην VIA επικεφαλίδα του REGISTER), και (ii) στέλνει ένα καινούριο REGISTER πάνω στον εξυπηρετητή soft switch, φροντίζοντας να ξαναγράψει τις επικεφαλίδες για να εξασφαλίσει ότι παραμένει στη ροή των πολυμέσων. Σημειώνουμε ότι στο βήμα (ii) η REGISTER θα αποκτήσει καινούριες Via και Contact επικεφαλίδες, για να σιγουρέψει ότι ο SBC

θα παραμένει στην διαδρομή του επόμενου μηνύματος σηματοδοσίας που θα σταλθεί στο τερματικό.

- Όταν ο SBC λάβει την απάντηση στο REGISTER, στέλνει μια απόκριση στον αρχικό REGISTER, διευθύνοντάς τη στην σωστή διεύθυνση και πόρτα στο τείχος προστασίας. Επειδή η pinhole στο τείχος προστασίας είναι ακόμη ανοιχτή, αυτό θα πρέπει να επιτρέπεται να φτάσει μέσω του τείχους προστασίας στο τηλέφωνο του πελάτη. Η επικεφαλίδα IP στην απάντηση ξαναγράφεται καθώς διασχίζει το τείχος προστασίας του πελάτη.

Όταν ανοίξει η pinhole , εισερχόμενες κλήσεις στο τηλέφωνο IP μπορούν να διευθυνθούν μέσω της pinhole, όπως φαίνεται πιο κάτω [η ACKδεν φαίνεται, αλλά διασχίζει τα τείχη προστασίας ομοίως με το INVITE].



Εισερχόμενες κλήσεις προς το τηλέφωνο IP που κατευθύνονται μέσω της pinhole

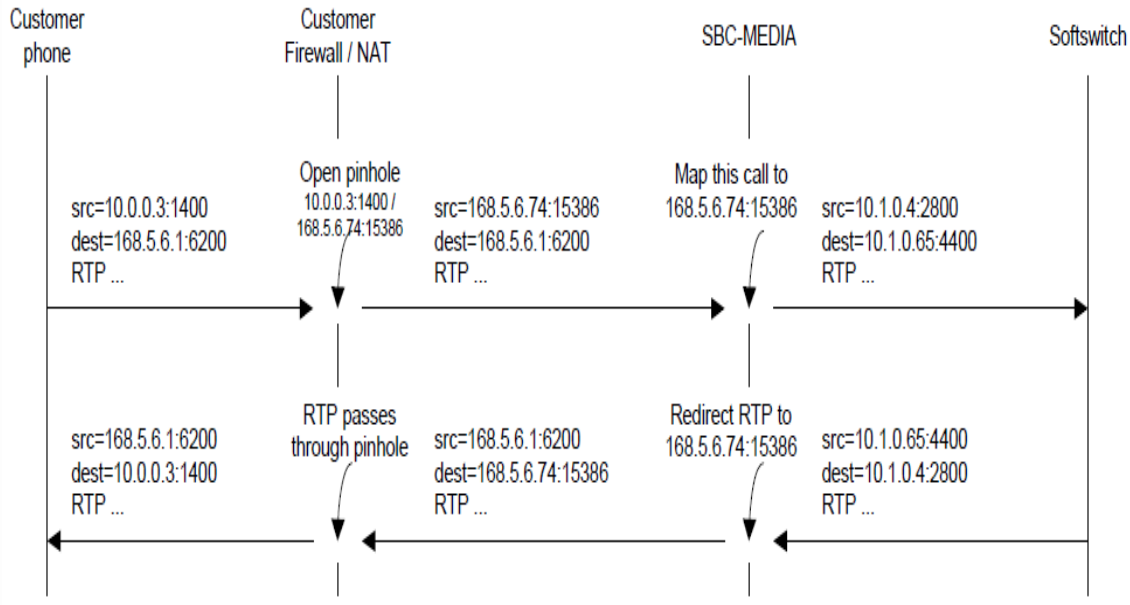
- Το soft switch δέχεται μια εισερχόμενη κλήση για bob@enterprise.com, και παράγει μια SIP INVITE, η οποία στέλνεται στην καταγραμμένη διεύθυνση επαφών του Bob [δηλ. τον SBC].

- Ο SBC αναγνωρίζει ότι η bob@enterprise.com αντιστοιχεί στο 168.5.6.74:12678 [που αναγνωρίστηκε νωρίτερα από την ανταλλαγή INVITE], και στέλνει ένα INVITE σε εκείνη τη διεύθυνση και την πόρτα.

- Η στοίβα RTP του SBC διαθέτει την πόρτα 6200 στην εξωτερική διεύθυνση IP του SBC για να λαμβάνει media επάνω στο τερματικό σημείο της SIP . Ο SBC ανοίγει μια pinhole στο τείχος προστασίας του [που συνήθως υπάρχουν στην ίδια τη συσκευή του SBC] για να επιτρέψουν τα media της κλήσης να ληφθούν σε αυτή την διεύθυνση και πόρτα.

- Το INVITE διασχίζει το τείχος προστασίας του πελάτη. Η απάντηση στο INVITE ταξιδεύει στην αντίθετη ροή μέσω του δικτύου. Η ACK [που δεν φαίνεται] ακολουθεί την ίδια ροή όπως το INVITE.

Όταν σηματοδοτηθεί η εισερχόμενη κλήση [όπως φάνηκε προηγούμενα],τα media αρχίζουν να ρέουν.



Ροή media μέσω pinhole

- Όταν το τηλέφωνο IP του πελάτη στέλνει το πρώτο πακέτο RTP, το τείχος προστασίας του ανοίγει μια pinhole για να επιτρέψει στο πακέτο να φύγει, και ξαναγράφει την διεύθυνση IP καθώς περνά. Αυτό το πακέτο RTP περνά επίσης από την τρύπα του τείχους προστασίας του παρόχου που άνοιξε ο SBC όταν σηματοδοτήθηκε η κλήση. Το πακέτο RTP που ελήφθη από τον SBC έχει πηγή διεύθυνσης και θύρας (επιτρέπεται δυναμικά από το τείχος προστασίας το άνοιγμα της pinhole) και διαφέρει από την διεύθυνση και την θύρα στο SDP. Όταν σταλούν πακέτα RTP πίσω στον πελάτη, ο SBC πρέπει να τα στείλει σε αυτή την διεύθυνση και θύρα, αντί να χρησιμοποιεί την διεύθυνση και την θύρα του SDP.
- Όταν τα πακέτα RTP ρέουν από το soft switch, ο SBC τα κατευθύνει σε μία εξωτερική IP διεύθυνση και πόρτα της media pinhole στο τείχος προστασίας του πελάτη, που μαθεύτηκε σε προηγούμενο βήμα.

Οικονομικά στοιχεία

Σύμφωνα με έρευνα της Infonetics Research η εταιρική αγορά για τους Οριακούς Ελεγχτες Συνόδου SBC's θα αυξηθεί 44% από το έτος 2009 στο 2014. Επίσης, αυξήθηκε 53% η αγορά το 2009 σε σχέση με το 2008

Σύμφωνα με την ερευνητική εταιρία Dell'Oro Group οι πωλήσεις των SBC's το 2009, μια χρονιά παγκόσμια ύφεσης και αρνητικού κλίματος για επενδύσεις, ήταν 197 εκ. Δολάρια

Τα στοιχεία αυτά δείχνουν ,εκτός του γεγονότος ότι η διαδικτυακή τηλεφωνία αναπτύσεται ραγδαία , ότι ο ρόλος των SBC στα εταιρικά δίκτυα VoIP είναι ,αν όχι απαραίτητος, αρκετά σημαντικός. Επιλύοντας σημαντικά προβλήματα στο τομέα της ασφάλειας , της λειτουργικότητας και ανάπτυξης των SIP και γενικότερα VoIP δικτύων.

Συμπεράσματα

'Οπως είδαμε υπάρχουνε διάφορα ασύρματα και ενσύρματα δίκτυα διαθέσιμα. Η τάση της τεχνολογίας είναι η σύγκλιση των διαφορετικών δικτύων αυτών. Στον τομέα της σηματοδοσίας το SIP πρωτόκολλο συμβάλλει στη συγκλιση αυτή. 'Εχοντας αποδεχτεί ως 3GPP πρωτόκολλο σηματοδοσίας και ως βασικό στοιχείο του (IMS) έχει προβάδισμα στην καθιέρωση του ως κυρίαρχο πρωτόκολλο σηματοδοσίας στα τηλεπικοινωνιακά συστήματα επόμενης γενιάς .

Στο κεφάλαιο 2 αναλύσαμε σε ένα βαθμό τη λειτουργία του SIP, είδαμε τις οντότητές του , την αρχιτεκτονική του , τα μηνύματά του (αιτήσεις/αποκρίσεις) και το περιεχόμενό τους επίσης παράδειγματα κλήσης, καθώς και την σημαντική λειτουργία της εγγραφής .

Η λειτουργία του SIP βασίζεται σε τεχνολογίες διαδικτύου IP έτσι αντιμετωπίζει και παρόμοια προβλήματα ασφάλειας στη λειτουργία του.

Από τις επιθέσεις σε SIP συστήματα που είδαμε στο κεφάλαιο 3 καταλαβαίνουμε ότι υπάρχουν αρκετές αδυναμίες .

Εχουμε επιθέσεις υποκλοπής , επιθέσεις σε SIP εξυπηρετητές με συμβατά αλλά και μη συμβατά μηνύματα, επιθέσεις πλημμύρας σε διάφορες SIP οντότητες, επιθέσεις ενδιαμεσου κακόβουλου χρήστη σε διαφορες φάσεις, επιθέσεις στη SIP αυθεντικοποίηση αλλά και επιθέσεις κοινωνικής μηχανικής και παρενόχλησης .

Οι μηχανισμοί ασφαλείας που υπάρχουν στο πρωτόκολλο έχουνε κάποιους περιορισμούς όπως για παράδειγμα σε κάποιες περιπτώσεις προαπαιτούν σχέσεις εμπιστοσύνης μεταξύ των κόμβων που επικοινωνούν (IPSec , Http digest), επίσης σε άλλες είναι απαραίτητο οι τερματικές συσκευές να υποστηρίζουν συγκεκριμένα πρωτόκολλα και μηχανισμούς ασφαλείας (TLS, S/MIME) και επιπλέον σε άλλες απαιτούνται υποδομές δημοσίου κλειδιού για τελικούς χρήστες (S/MIME).

Η λύση των Οριακών Ελεγκτών Συνόδου «SBC» ενισχύει σε σημαντικό βαθμό την ασφάλεια στα SIP συστήματα προστατευόντάς τα όπως είδαμε από αρκετές απειλές. Κάποιες από τις λειτουργίες των «SBC» είναι η ανάπτυξη της αποστρατικοποιημένης ζώνης , η διάβαση του τείχους προστασίας , η αποδοχή ελέγχου κλήσης, η εγγύηση της ποιότητας υπηρεσίας, η γεφύρωση των πολυμέσων , η ανοχή σφάλματος, η πολιτική δρομολόγησης των κλήσεων, η δια λειτουργικότητα διαφορετικών πρωτοκόλλων σηματοδοσίας και η χρέωση κλήσης.

Ακόμη είδαμε και άλλες εφαρμογές των «SBC» που ενισχύουν την ασφάλεια όπως η απόκρυψη τοπολογίας και η ανίχνευση κακόβουλων πρωτοκόλλων.

Επιπλέον, είδαμε ότι ο «SBC» λειτουργεί ως τείχος προστασίας και NAT δίνοντας έτσι και λύση στο πρόβλημα της προσπέλασης των μηνυμάτων σηματοδοσίας απο το τείχος προστασίας και το NAT με κατάλληλο μηχανισμό που χρησιμοποιεί(pin hole). Τέλος, τα οικονομικά στοιχεία δείχνουν ότι οι πωλήσεις των SBC’s θα έχουν αρκετά μεγάλη αύξηση τα επόμενα χρόνια γεγονός που φανερώνει τη πολύτιμη σημασία τους στο σύγχρονο τηλεπικοινωνιακό περιβάλλον

Βιβλιογραφία

Κύριες Πηγές:

1. SIP RFC 3261 http://www.ietf.org/rfc/rfc3261.txt

2. «Πλαίσιο Ανίχνευσης και Αντιμετώπισης Περιστατικών Ασφαλείας σε Συστήματα Διαδικτυακής Τηλεφωνίας» , Διδακτορική Διατριβή του Γενειατάκη Δημήτρη

3. «Session Border Controllers-Enabling the VoIP Revolution», Metaswitch Networks

4. «Internet Communications Using SIP», Henry Sinnreich, Alan B. Johnston

5. «Securing VoIP Networks –Threats, Vulnerabilities and Countermeasures», Peter Thermos, Ari Takanen

http://en.wikipedia.org

Επι μέρους πηγές:

[1] Geneiatakis D., Dagiouklas A., Kambourakis G., Lambrinoudakis C., Gritzalis S., Ehlert S.,
Sisalem D., "Survey of Security Vulnerabilities in Session Initiation Protocol", *IEEECommunications Surveys and Tutorials*, Vo. 8, No. 3, pp. 68-81, IEEE Press, 2006.

[2] Geneiatakis D., Kambourakis G., Dagiouklas A., Lambrinoudakis C., Gritzalis S., "Session Initiation Protocol Security Mechanisms: A state-of-the-art review", *in the proceedings of Fifth International Network Conference*, S. Furnell, S. K. Katsikas (Eds.), pp. 147-156, , Samos, Greece, Ziti Pubs, July 2005.

[3] Wieser., C., Laakso, M., Schulzrinne, H., "Security Testing of SIP Implementations", Available
on line:
http://compose.labri.fr/documentation/sip/Documentation/Papers/Security/Papers/462.pdf

[4] Sisalem, D., Kuthan, J., Ehlert, S., "Denial of service attacks targeting a SIP VoIP infrastructure:
attack scenarios and prevention mechanisms," *Network, IEEE* , vol.20, no.5pp. 26- 31, 2006. http://www.iptel.org/~dor/papers/Sisa0610_Denial.pdf

[5](http://www.juniper.net/security/auto/vulnerabilities/vuln25299.html

[6] Wagner D., Foster J. S., Brewer E. A., Aiken A., "A First Step towards Automated Detection of
Buffer Overrun Vulnerabilities", *in the Proceedings of the ISOC Symposium on Network and Distributed System Security (SNDSS)*, February 2000.

[7] CERT Advisory CA-2000-02, "Malicious HTML Tags Embedded in Client Web Requests",available online http://www.cert.org/advisories/CA-2000-02.html
[8] CERT Vulnerability Note, "VU#282403", available online
http://www.kb.cert.org/vuls/id/282403

[9] CERT Vulnerability, "Note VU#496064", available online
http://www.kb.cert.org/vuls/id/496064

[10] Anley, C., "Advanced SQL Injection In SQL Server Applications", An NGSSoftware Insight Security Research (NISR) Publication, 2002.

[11] "SIP Express Router", http://www.iptel.org/ser

[12] http://vovida.org

[13]SIP Message Tampering THE SQL code INJECTION attack, Dimitris Geneiatakis, Georgios Kambourakis, Costas Lambrinoudakis, Tasos Dagiuklas and Stefanos Gritzalis

[14] (http://www.securityfocus.com/tools/3528)

[15] http://xforce.iss.net/xforce/xfdb/41733

[16] CERT, Advisory CA-1996-21, "TCP SYN Flooding and IP Spoofing Attacks", available online
http://www.cert.org/advisories/CA-1996-21.html, September 1996

[17] Eddy, W., "TCP SYN Flooding Attacks and Common Mitigations", *RFC 4987*, August 2007.

[18] Gibson, S., "DRDoS Distributed Reflection Denial of Service", available online http://grc.com/dos/drdos.htm, 2002.

[19] HTTP Digest http://tools.ietf.org/html/rfc3310

[20] Sisalem, D., Kuthan, J., Ehlert, S., "Denial of service attacks targeting a SIP VoIP infrastructure:
attack scenarios and prevention mechanisms," *Network, IEEE* , vol.20, no.5pp. 26- 31, 2006.

[21] Zhang, G., Ehlert S., Magedanz, T., Sisalem D., "Denial of Service Attack and Prevention on SIP VoIP Infrastructures Using DNS Flooding", in the proceeding of *Principles, Systems and Applications of IP Telecommunications (IPTComm2007) Conference,* July 2007.

[22] (http://en.wikipedia.org/wiki/Dictionary_attack)

[23] http://en.wikipedia.org/wiki/Rainbow_table