ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Αξιοποίηση και λειτουργία της VoIP τεχνολογίας στην OFF net και ON net τηλεφωνία-Θέματα ασφάλειας που προκύπτουν από τη χρήση της.

ΔΕΣΠΟΙΝΑ ΚΥΡΙΑΚΑΚΗ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων

ΓΕΩΡΓΙΟΣ ΣΤΑΜΟΥΛΗΣ

Λαμία, 2018

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Αξιοποίηση και λειτουργία της VoIP τεχνολογίας στην OFF net και ON net τηλεφωνία-Θέματα ασφάλειας που προκύπτουν από τη χρήση της.» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Η ΔΗΛΟΥΣΑ

03/09/2018

Αξιοποίηση και λειτουργία της VoIP τεχνολογίας στην OFF net και ON net τηλεφωνία-Θέματα ασφάλειας που προκύπτουν από τη χρήση της.

ΔΕΣΠΟΙΝΑ ΚΥΡΙΑΚΑΚΗ

Τριμελής Επιτροπή:

ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

ΒΑΒΟΥΓΥΪΟΣ ΔΗΜΗΤΡΙΟΣ

ΔΗΜΗΤΡΙΟΥ ΓΕΩΡΓΙΟΣ

Επιστημονικός Σύμβουλος:

ΣΤΑΜΟΥΛΗΣ ΓΕΩΡΓΙΟΣ

Περιεχόμενα

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΕΙΣΑΓΩΓΗ

Οι υπηρεσίες φωνής μέσω πρωτοκόλλου του Διαδικτύου, ευρύτερα γνωστές ως υπηρεσίες VoIP (Voice over Internet Protocol) ή IP Telephony ή Internet Telephony, περιλαμβάνουν τις απαραίτητες ενέργειες για να πραγματοποιούνται συνομιλίες χρησιμοποιώντας δίκτυα δεδομένων IP. Στο παρελθόν έχουν δοθεί διαφορετικές ερμηνείες για αυτούς τους όρους, ανάλογα με το είδος των υπηρεσιών που προσφέρονται ή την προοριζόμενη χρήση του δικτύου, ωστόσο έχει επικρατήσει να θεωρούνται ταυτόσημοι. Διατηρώντας αυτή την προσέγγιση, οι όροι αυτοί θα χρησιμοποιούνται εναλλακτικά στην παρούσα εργασία.

Μέχρι τα τέλη της δεκαετίας του 1900 ο όρος VoIP χρησιμοποιούταν για να περιγράφει υπηρεσίες φωνής, υποκατάστατες της παραδοσιακής σταθερής τηλεφωνίας. Σταδιακά όμως έγινε αντιληπτό ότι μπορεί να προσφέρουν εξελιγμένες υπηρεσίες, οι οποίες λαμβάνουν υπόψη για παράδειγμα τις ιδιαιτερότητες της συσκευής και τη διαθεσιμότητα του χρήστη. Τον ίδιο καιρό η απελευθέρωση της αγοράς τηλεπικοινωνιών οδήγησε στην ανάπτυξη ανταγωνισμού. Αυτό είχε σαν αποτέλεσμα το σύνολο των χρηστών να μην ανήκει πλέον σε έναν μόνο πάροχο και επομένους δημιούργησε την ανάγκη οι τελευταίοι να συνεργαστούν προκειμένου να προσφέρει μία υπηρεσία.

Πρόσφατα, η ανάπτυξη νέων τεχνολογιών και σταδιακή υιοθέτηση τους από παρόχους επιτρέπει σύγκλιση των υπηρεσιών, και επομένως ακόμη μεγαλύτερη ευελιξία στην παροχή μιας υπηρεσίας. Με τα Δίκτυα Νέας Γενιάς για παράδειγμα, οι χρήστες μπορούν να λαμβάνουν τις υπηρεσίες που επιθυμούν ανεξάρτητα από την τεχνολογία δικτύου πρόσβασης που χρησιμοποιούν τη δεδομένη στιγμή. Αυτό σημαίνει ότι ενδέχεται να υπάρχουν εναλλακτικοί τρόποι για να προσφερθεί μία υπηρεσία, ο καθένας από τους οποίους έχει διαφορετικές ιδιότητες. Η επιλογή της καταλληλότερης μεθόδου για την εξυπηρέτηση ενός αιτήματος αποτελεί καθοριστικό παράγοντα για την ικανοποίηση των επιδιώξεων χρηστών και παροχών και επομένως απαιτεί σχεδιασμό εξελιγμένων διαδικασιών. Στην περίπτωση των

τηλεφωνικών υπηρεσιών, οι διαδικασίες αυτές ονομάζονται στρατηγικές δρομολόγησης (Hardy, 2003).

ΚΕΦΑΛΑΙΟ 1- Εισαγωγή στο VoIP

Σε όλο τον κόσμο η τηλεφωνία μέσω Internet αναπτύσσεται με ταχύτατους ρυθμούς, συνήθως στα πλαίσια του double-play, δηλαδή της παροχής ευρυζωνικής πρόσβασης και τηλεφωνίας μαζί. Καθώς με τη VoIP επιτυγχάνεται η ενοποίηση δικτύων (δηλαδή η πρόσβαση στο Internet και η τηλεφωνία πάνω από ένα δίκτυο), το αποτέλεσμα είναι -ιδιαίτερα στα υπεραστικά τηλεφωνήματα- οι χρεώσεις μέσω διαδικτύου να είναι εξαιρετικά χαμηλές και συχνά να βρίσκονται κάτω από αυτές των αστικών κλήσεων. Αντιλαμβάνεται κανείς πόσο σημαντικά είναι τα πλεονεκτήματα για τα ΜΜΕ, τα οποία προσπαθούν να μειώσουν τα κόστη τους στο έντονα ανταγωνιστικό περιβάλλον, και ιδίως για τις επιχειρήσεις που συναλλάσσονται με το εξωτερικό. Ήδη στη Βρετανία τα VoIP τηλέφωνα έχουν λάβει δικό τους κωδικό περιοχής, ενώ πρόγραμμα που προσφέρει δωρεάν τηλεφωνία ανάμεσα σε χρήστες του Internet ήδη έχει περάσει τα 50 εκατομμύρια χρήστες (Dunte & Ruland, 2007).

Συχνά επικρατεί η εσφαλμένη αντίληψη ότι Voice over IP σημαίνει αποκλειστικά χαμηλές χρεώσεις. Στην πραγματικότητα, η τηλεφωνία μέσω Internet έρχεται να "παντρέψει" τις υπηρεσίες φωνής με τον κόσμο του IP, το διαδίκτυο. Οι δυνατότητες που παρέχει στις επιχειρήσεις και τους επαγγελματίες είναι πραγματικά απεριόριστες.

Οι προϋποθέσεις για την δημιουργία του VoIP τέθηκαν το 1991, όταν ο αμερικάνικος οργανισμός NSK διέκοψε τη χρηματοδότηση του δικτύου κορμού του Διαδικτύου, δίνοντας το έναυσμα για την εμπορική χρήση του. Στη συνέχεια, η υπάρχουσα υποδομή, οι τεχνολογικές εξελίξεις και το ευνοϊκό ρυθμιστικό πλαίσιο συνέβαλαν ώστε να προσφερθεί ως υπηρεσία στους τελικούς χρήστες. Αρχικά, για να επικοινωνήσουν δύο μέρη έπρεπε να χρησιμοποιούν υπολογιστή με ειδικό λογισμικό και περιφερειακό εξοπλισμό. Οι χρήστες αυτής της

υπηρεσίας ήταν κυρίως άτομα με μεγάλη ευχέρεια στη χρήση υπολογιστή που έψαχναν ένα τρόπο να συνομιλούν «δωρεάν». Η πρώτη υπηρεσία VoIP προς το κοινό χρονολογείται στο 1990 και προσφέρθηκε απ' τη Net2Phone. Συνάπτοντας συμφωνίες με Internet Service Providers (ISPs) σε διάφορες χώρες, τοποθετούσε ειδικές συσκευές (πύλες τηλεφωνίας) για να μπορεί να τερματίζει διεθνείς κλήσεις προς το Δημόσιο Τηλεφωνικό Δίκτυο Μεταγωγής (PSTN) χρησιμοποιώντας ως υποδομή το Διαδίκτυο επειδή οι υπηρεσίες αυτές θεωρούνταν ημιπαράνομες.

Η επιχειρηματική δραστηριότητα που άνηκε σ' αυτή την κατηγορία ονομάστηκε «γκρίζα αγορά» (grey market). Οι χρήστες σ' αυτή την περίπτωση ανήκαν κυρίως στη χαμηλή εισοδηματική τάξη. Ωστόσο, και στις δύο παραπάνω περιπτώσεις το μοναδικό ελκυστικό χαρακτηριστικό ήταν η μηδενική ή πολύ μικρή χρέωση. Όπως αναφέρει στο άρθρο του Chang (2004), η ποιότητα της φωνής ήταν κακή, ο χρόνος εγκατάστασης κλήσης μεγάλος και το ποσοστό απορριφθέντων κλήσεων (call blocking probability) σχεδόν 90%. Η κατάσταση άρχισε να αλλάζει όταν η τηλεφωνία IP απασχόλησε μεγάλες εταιρείες παραγωγής δικτυακού εξοπλισμού, όπως τη CISCO και τη Nortel Networks. Άλλοι σημαντικοί παράγοντες ήταν ο σχεδιασμός και υιοθέτηση προτύπων για τα πρωτόκολλα διαδικτύου και η ύπαρξη αχρησιμοποίητου εύρους ζώνης στο δίκτυο κορμού (Internet backbone) καθώς και στα δίκτυα των εταιρειών (LAN).

Όλο και περισσότερες εταιρείες άρχισαν τότε να προσφέρουν χονδρικές υπηρεσίες VoIP για υπεραστικές και διεθνείς κλήσεις, παρακάμπτοντας τους παραδοσιακούς παρόχους τηλεφωνίας (Long distance loll bypass). Προκειμένου να πλησιάζουν τα επίπεδα ποιότητας της παραδοσιακής τηλεφωνίας, ανέπτυξαν ειδικά συστήματα δρομολόγησης κλήσεων ενώ χρησιμοποιούν ως εναλλακτική το ίδιο το PSTN. Εξάλλου, μεγάλες εταιρείες με πολλά υποκαταστήματα και πανεπιστήμια ενοποίησαν το δίκτυο δεδομένων με το τηλεφωνικό τους δίκτυο, αντικαθιστώντας τα PBX (Private Branch Exchange) με τα νεότερα IP-PBX (Sisalem, 2006).

Η ενοποίηση φωνής, βίντεο και δεδομένων σ’ ένα δίκτυο επιτρέπει την παροχή εξειδικευμένων υπηρεσιών και θεωρείται η νέα γενιά υπηρεσιών VoIP. Καθώς ο έντονος

ανταγωνισμός στον κλάδο των τηλεπικοινωνιών μικραίνει τη διαφορά τιμών, οι πάροχοι πλέον πρέπει να διατηρήσουν τους πελάτες τους και να προσελκύσουν νέους με καινοτόμες υπηρεσίες.

1.1. Κλήσεις VoIP

Υπάρχουν οι ακόλουθοι τύποι υπηρεσιών για τους τελικούς πελάτες: Συνδιάλεξη υπολογιστή με υπολογιστή (PC-to-PC), τηλέφωνο με τηλέφωνο (Phone-to-Phone) και υπολογιστή με τηλέφωνο (PC-2-Phone ή το αντίστροφο). Ανεξάρτητα όμως από τον τύπο της συσκευής που ξεκινά τη συνομιλία, τα βασικά στάδια για την πραγματοποίησή της είναι δύο: η εγκατάσταση της κλήσης (call setup) και η μετάδοση της φωνής (telephone conversation). Ενδεικτικά, για μια συνδιάλεξη από υπολογιστή σε τηλέφωνο (Dunte, 2007):

• η φάση εγκατάστασης κλήσης περιλαμβάνει τη λήψη σήματος διαθεσιμότητας γραμμής, την πληκτρολόγηση του αριθμού προορισμού, τη δρομολόγηση της κλήσης, τη δέσμευση πόρων ή την τήρηση πληροφοριών για τη σύνοδο, και τη λήψη σήματος εξέλιξης, αναμονής, ή δεσμευμένης γραμμής.

• η φάση της μετάδοσης φωνής ξεκινά όταν ο καλούμενος απαντήσει στην κλήση και περιλαμβάνει τη δειγματοληψία, ψηφιοποίηση και συμπίεση της φωνής, την ενσωμάτωση σε πακέτα IP, τη δρομολόγηση των πακέτων, την ταξινόμηση και αποσυμπίεσή τους όταν φτάσουν στην πύλη τηλεφωνίας, τη μετατροπή τους σε ψηφιακά σήματα και τελικά σε αναλογικά σήματα. Κατά τη φάση εγκατάστασης κλήσης το πλέον σημαντικό βήμα είναι η δρομολόγηση της κλήσης, που προϋποθέτει ότι έχει αναγνωριστεί ο καλούμενος και έχει εντοπιστεί.

1.2. Αρχή λειτουργίας VoIP

Η αρχή πάνω στην οποία στηρίζεται η λειτουργία της μετάδοσης φωνής μέσω IP είναι ότι ο πελάτης πληρώνει ένα ορισμένο ποσό για να συνδεθεί στο δίκτυο και στη συνέχεια πληρώνει ανάλογα με το χρόνο χρήσης και τις χρησιμοποιούμενες εγκαταστάσεις (βάσει της απόστασης).

Η συχνότητα που απαιτεί η τεχνολογία IP για τη μετάδοση των δεδομένων είναι τουλάχιστον έξι φορές μικρότερη από την αντίστοιχη των παραδοσιακών τηλεπικοινωνιακών δικτύων που χρησιμοποιούν σήμερα οι περισσότεροι συνδρομητές σε όλο τον κόσμο. Η σημαντική αυτή διαφορά καθιστά τις κλήσεις μέσω του VoIP σαφέστατα πιο οικονομικές, και σε αρκετές περιπτώσεις το τηλεφώνημα μέσω διαδικτύου μπορεί να στοιχίσει έως και 90% φθηνότερα απ' ό,τι μέσω του παραδοσιακού τηλεπικοινωνιακού δικτύου (Frederique & Zakhama, 2008).

Εικόνα 1

Διαφορά με τα κλασσικά τηλεφωνικά δίκτυα

Σε αντίθεση με τα δίκτυα μεταγωγής πακέτων, όπως αυτά που βασίζονται στο πρωτόκολλο IP, στα κλασικά τηλεφωνικά εφαρμόζεται η λογική της απευθείας σύνδεσης μεταξύ των δύο συνομιλητών μέσω γραμμής που δεσμεύεται αποκλειστικά για κάθε επικοινωνία. Στα δίκτυα μεταγωγής πακέτων, όμως, από την ίδια γραμμή περνούν ταυτόχρονα διαφορετικά πακέτα δεδομένων. Έτσι, ταυτόχρονα με τα πακέτα φωνής μιας ή περισσότερων συνομιλιών, μπορούν να περνούν στην ίδια γραμμή πακέτα με άλλα δεδομένα, έγγραφα κ.ο.κ. Αυτή είναι και η βασική διαφορά μεταξύ της κλασικής τηλεφωνίας που εφαρμόζεται στο δημόσιο τηλεφωνικό δίκτυο και της υλοποίησης τηλεφωνίας πάνω σε δίκτυα IP ή, γενικότερα, σε δίκτυα μεταγωγής πακέτων (Frederique & Zakhama, 2008).

1.3. Κωδικοποίηση φωνής και Πραγματοποίηση κλήσεων

Η πραγματοποίηση μιας κλήσης, ανεξάρτητα από την τεχνολογία που χρησιμοποιεί, διακρίνεται σε δύο βήματα: α) την εγκατάσταση της κλήσης και β) τη μετάδοση φωνής. Η εγκατάσταση της κλήσης αποτελεί προϋπόθεση για τη μετάδοση της φωνής και για αυτό παίζει καθοριστικό ρόλο στην αξιολόγηση των παρόχων. Κατά τη διάρκεια της εγκαθίδρυσης η κρισιμότερη απόφαση που έχει να πάρει ο πάροχος αφορά τον τρόπο με τον οποίο θα γίνει η δρομολόγηση, δηλαδή την προώθηση της κλήσης προς τον προορισμό. Ενδέχεται να συμμετέχουν περισσότεροι από ένας πάροχοι σε αυτή τη διαδικασία, ειδικά όταν οι συμμετέχοντες δεν είναι συνδρομητές του ίδιου παρόχου. Η απόφαση δρομολόγησης που παίρνει κάθε πάροχος συντελεί στον καθορισμό ενός μονοπατιού από τον καλούντα στον καλούμενο. Οι συσκευές των παρόχων που συμμετέχουν σε αυτό το μονοπάτι αποκαλούνται εξυπηρετητές σηματοδοσίας (signalling servers), επειδή δέχονται και επεξεργάζονται αιτήσεις

κλήσεων με τη μορφή κωδικοποιημένων σημάτων.

Στο σημείο αυτό πρέπει να αναφέρουμε ότι η πραγματοποίηση κλήσεων μεταξύ χρηστών που χρησιμοποιούν διαφορετικές τεχνολογίες απαιτεί τη συμμετοχή ειδικών συσκευών, που ονομάζονται πύλες τηλεφωνίας (ή Gateways). Οι συσκευές αυτές αναλαμβάνουν να κάνουν τις απαραίτητες μετατροπές στα μηνύματα σηματοδοσίας για την εγκατάσταση και διαχείριση της κλήσης και στη φωνή που μεταδίδεται, προκειμένου να αποφευχθούν προβλήματα ασυμβατότητας. Η χρήση των gateways είναι πολύ διαδεδομένη, για παράδειγμα, σε περιπτώσεις κλήσεων VoIP προς τηλεφωνικούς αριθμούς του δικτύου σταθερής τηλεφωνίας (PSTN).

Στην παρούσα εργασία θα χρησιμοποιούμε τους όρους ‘πύλη τηλεφωνίας' και 'Gateway' εναλλάξ. Επιπλέον, θα συμπεριλάβουμε τα Gateways στους εξυπηρετητές σηματοδοσίας, δεδομένου ότι και αυτά συμμετέχουν στη φάση εγκατάστασης μιας κλήσης.

Πριν την απελευθέρωση των αγορών τηλεπικοινωνιών, η διαδικασία της δρομολόγησης ήταν σχετικά απλή γιατί δεν υπήρχαν εναλλακτικές επιλογές. Σήμερα, με την πρόοδο της τεχνολογίας και την ανάπτυξη ανταγωνισμού, ενδέχεται να υπάρχουν εναλλακτικοί τρόποι για την εγκατάσταση της κλήσης οι οποίοι πρέπει να αναζητηθούν και να αξιολογηθούν εκείνη τη στιγμή. Αυτό το χαρακτηριστικό είναι πολύ σημαντικό γιατί αυξάνει την πολυπλοκότητα του προβλήματος δεδομένου ότι οι χρήστες ανησυχούν για την εξέλιξη της κλήσης τους όταν περνάει μεγάλος χρόνος μέχρι να ακούσουν τον ήχο κλήσης (ring tone).

Παραδοσιακά, όταν ένας πάροχος δέχεται μία εισερχόμενη κλήση, η δρομολόγησή της γίνεται με βάση το αναγνωριστικό (ID) του καλούμενου (π.χ. τον τηλεφωνικό αριθμό του). Με βάση αυτό το αναγνωριστικό ο πάροχος αναζητά τους υποψήφιους εξυπηρετητές σηματοδοσίας στο σύστημά του και επιλέγει αυτόν που πληροί κάποιες προϋποθέσεις. Με τη σύγκλιση των υπηρεσιών ένας πάροχος μπορεί να έχει πρόσβαση σε ακόμη περισσότερες επιλογές. Αυτό γίνεται αναζητώντας εναλλακτικά αναγνωριστικά του ίδιου χρήστη σε κατάλληλα συστήματα, και στη συνέχεια βρίσκοντας υποψήφιους εξυπηρετητές σηματοδοσίας για όλα τα διαθέσιμα αναγνωριστικά χρήστη.

Ένα συνηθισμένο παράδειγμα εύρεσης εναλλακτικών αναγνωριστικών αφορά ένα προορισμό που είναι συνδρομητής σταθερής και κινητής τηλεφωνίας, δηλαδή διαθέτει δύο τηλεφωνικούς αριθμούς (αναγνωριστικά). Μία εισερχόμενη κλήση προς το σταθερό τηλέφωνο θα μπορούσε να εκτραπεί προς το κινητό τηλέφωνο του χρήστη, αν ο πάροχος γνώριζε ότι αντιστοιχούν στον ίδιο χρήστη. Κάτι τέτοιο θα ήταν προς όφελος του παρόχου αν, για παράδειγμα, τύχαινε να είναι συνδρομητής του. Παρόλο που δεν είναι δεδομένο ότι όλοι οι τηλεφωνικοί αριθμοί ενός χρήστη είναι ισοδύναμοι, σε πολλές περιπτώσεις (για παράδειγμα στο Δημόσιο) ο χρήστης έχει δώσει τη συγκατάθεσή του αυτά να χρησιμοποιούνται εναλλακτικά.

Αυτές οι εναλλακτικές επιλογές αναμένεται να διαφέρουν σε χαρακτηριστικά όπως το κόστος και η διαθεσιμότητα των απαιτούμενων πόρων τη δεδομένη χρονική στιγμή κ.ά. Το γεγονός μάλιστα ότι υπάρχει αβεβαιότητα για τη διαθεσιμότητα ή μη ενός εξυπηρετητή καθιστά αυτή την απόφαση ένα ενδιαφέρον ερευνητικό και πρακτικό πρόβλημα. Για αυτό το λόγο, προτείνουμε και αξιολογούμε πολιτικές των παρόχων VoIP που μπορούν να πετύχουν *βέλτιστη* δρομολόγηση κλήσεων, λαμβάνοντας υπόψη τα αναμενόμενα κέρδη από κάθε κλήση που εγκαθίσταται επιτυχώς. Γενικά, αυτές οι πολιτικές δρομολόγησης είναι :

- η μονή προσπάθεια (single attempt), κατά την οποία χρησιμοποιείται ο επιλεγμένος εξυπηρετητής και αν αυτός δεν είναι διαθέσιμος τότε ενημερώνεται ο καλών ότι συνέβη κάποιο σφάλμα. Στην περίπτωση αυτή ο πάροχος περιμένει ο καλών να ξανακαλέσει, εφόσον το κρίνει απαραίτητο.

- η σειριακή προσπάθεια (sequential attempt), κατά την οποία οι επιλεγμένοι εξυπηρετητές χρησιμοποιούνται διαδοχικά, όταν οι προηγούμενοι στη σειρά δε βρίσκονται διαθέσιμοι.

- η παράλληλη προσπάθεια (forked attempt), κατά την οποία οι επιλεγμένοι εξυπηρετητές χρησιμοποιούνται ταυτόχρονα, αλλά μόνο ένας προλαβαίνει τον προορισμό διαθέσιμο. Μία τέτοια πολιτική είναι εφικτή με όλα τα διαδεδομένα πρωτόκολλα σηματοδοσίας (π.χ. SIP) και είναι γνωστή ως *Διακλάδωση* (Forking).

1.4. Τα Συστήματα Επικοινωνιών VoIP

Τα τελευταία χρόνια έχουν αναπτυχθεί πολλά συστήματα - εφαρμογές για επικοινωνία των χρηστών μέσω VoIP. Ιδιαίτερα διαδεδομένες είναι για παράδειγμα οι εφαρμογές Skype, Google Talk, Windows Messenger, Yahoo Messenger, οι οποίες επιτρέπουν στους χρήστες τους να χρησιμοποιούν το Διαδίκτυο για δωρεάν κλήσεις και για ανταλλαγή σύντομων μηνυμάτων. Επιπλέον, κάποιες από αυτές υποστηρίζουν κλήσεις από και προς παραδοσιακούς αριθμούς (π.χ. Skype). Με εξαίρεση το Google Talk που χρησιμοποιεί το πρωτόκολλο XMPP (Extensible Messaging and Presence Protocol), οι υπόλοιπες εφαρμογές χρησιμοποιούν μη προτυποποιημένα πρωτόκολλα. Αυτό το χαρακτηριστικό τους καθιστά δύσκολη την επικοινωνία χρηστών μεταξύ διαφορετικών εφαρμογών. Ένα σύστημα επικοινωνιών VoIP που παρουσιάζει ιδιαίτερο ενδιαφέρον είναι το fwdOUT, που είναι μία κοινότητα χρηστών όπου ο καθένας (Victor et Al, 2015):

- διαθέτει ειδικό εξοπλισμό που λειτουργεί σαν προσωπικό Gateway (είναι γνωστό ως Analog Telephone Adaptor-ATA),
- είναι συνδρομητής υπηρεσιών τηλεφωνίας,
- διαθέτει ευρυζωνική πρόσβαση στο Διαδίκτυο (π.χ. xDSL),
- έχει εγκατεστημένο παρεχόμενο λογισμικό για πραγματοποίηση κλήσεων. Κάθε μέλος της κοινότητας ενημερώνει τον κεντρικό εξυπηρετητή του συστήματος για τους τηλεφωνικούς αριθμούς για τους οποίους είναι διατεθειμένο να δεχτεί κλήσεις προκειμένου να τις προωθήσει στον τελικό προορισμό τους.

Ο χρήστης επίσης εισάγει κανόνες που πρέπει να πληρούνται ώστε να γίνει δεκτή η κλήση (π.χ. επιτρεπτές ώρες), καθώς και το μέγιστο πλήθος ταυτόχρονων κλήσεων που μπορεί να υποστηρίξει. Ένας χρήστης που θέλει να καλέσει κάποιο προορισμό θα κατευθύνει το αίτημά του στον κεντρικό εξυπηρετητή και αυτός στη συνέχεια θα διαλέξει έναν άλλο χρήστη, εφόσον ικανοποιούνται οι προϋποθέσεις που ο τελευταίος είχε θέσει. Εάν ο ενδιάμεσος

χρήστης του συστήματος έχει διαθέσιμους πόρους τότε η κλήση θα ολοκληρωθεί. Το σκεπτικό είναι να πραγματοποιούνται κλήσεις μέσω κάποιου άλλου χρήστη που έχει φθηνότερη χρέωση από τον καλούντα. Για παράδειγμα, μία διεθνής ή υπεραστική κλήση για τον καλούντα θα μπορούσε να πραγματοποιηθεί σε δύο βήματα. Στο πρώτο βήμα, η κλήση θα είναι VoIP προς έναν ομότιμο χρήστη, ο οποίος έχει για παράδειγμα αστική χρέωση και στο δεύτερο βήμα μέσω του PSTN. Στην περίπτωση αυτή, το Gateway που χρησιμοποιείται είναι ο εξοπλισμός του ομότιμου χρήστη. Να σημειωθεί ότι το σύστημα αυτό είναι ανταποδοτικό, δηλαδή ο καλών δεν πληρώνει άμεσα τον ομότιμο χρήστη αλλά έμμεσα, κάνοντας χρήση ενός κεντρικού μηχανισμού φήμης (State et al, 2009).

Όποτε πραγματοποιείται μία κλήση, ο κεντρικός εξυπηρετητής ενημερώνει το ιστορικό του κάθε χρήστη για κάθε συναλλαγή. Εάν ένας χρήστης έχει αρνητικό ισοζύγιο κλήσεων (δηλαδή οι εξερχόμενες κλήσεις είναι περισσότερες από τις εισερχόμενες) τότε δεν έχει δικαίωμα να ξεκινήσει νέα κλήση μέσω του συστήματος. Η σημαντικότερη διαφορά του προτεινόμενου συστήματος σε σχέση με το fwdOUT είναι η απουσία κάποιας κεντρικής οντότητας που συμμετέχει σε όλες τις προσπάθειες εγκατάστασης κλήσεων. Επομένως, δεν υπάρχει κίνδυνος για διακοπή λειτουργίας του συστήματος αν ο κεντρικός εξυπηρετητής παρουσιάσει πρόβλημα, αλλά με αντάλλαγμα στον έλεγχο και επιβολή (Keromytis, 2010).

1.5. Πολιτικές Δρομολόγησης Κλήσεων VoIP

Αν και η εγκατάσταση της κλήσης αποτελεί προϋπόθεση για την πραγματοποίησή της, οι περισσότεροι ερευνητές του VoIP έχουν επικεντρωθεί στη βελτίωση της ποιότητας για τη φάση της συνομιλίας. Το ενδιαφέρον αυτό αποδίδεται στα προβλήματα που αντιμετώπιζαν οι πρώτοι χρήστες υπηρεσιών VoIP και συγκεκριμένα τη συχνή καθυστέρηση μετάδοσης της φωνής από το ένα άκρο στο άλλο (delay) και την απόρριψη πακέτων εξαιτίας συμφόρησης (packet-loss) (Courcoubetis et al, 2009).

Τα προβλήματα αυτά οφείλονται στο γεγονός ότι το Διαδίκτυο έχει υιοθετήσει το παράδειγμα (paradigm) της μεταγωγής πακέτου, χωρίς εγγύηση ποιότητας (best-effort). Η επίδοση των παρόχων σε αυτόν τον τομέα εξακολουθεί να είναι το βασικό κριτήριο αξιολόγησης της υπηρεσίας από τους τελικούς χρήστες, αλλά τα τελευταία χρόνια τα προβλήματα αυτά έχουν ελαττωθεί. Σημαντικό ρόλο στη μείωση αυτών των προβλημάτων έπαιξε εκτός από την αύξηση της χωρητικότητας των δικτύων, η ανάπτυξη και σταδιακή υιοθέτηση πρωτοκόλλων που επιτρέπουν σε δίκτυα μεταγωγής πακέτου να αποκτούν χαρακτηριστικά των δικτύων μεταγωγής κυκλώματος (Burke et al, 2007).

Για τον λόγο αυτό, η ερευνητική δραστηριότητα για την ποιότητα επικοινωνίας έχει μετατοπιστεί στις ασύρματες τεχνολογίες δικτύων πρόσβασης.

Ωστόσο, οι προσεγγίσεις αυτές βασίζονται σε πληροφορίες οι οποίες μπορούν να θεωρηθούν αξιόπιστες μόνο όταν οι εξυπηρετητές ανήκουν στον ίδιο τον πάροχο που παίρνει την απόφαση δρομολόγησης ή σε κάποιο έμπιστο συνεργάτη του. Τέλος, παρόμοιες πολιτικές δρομολόγησης προτείνονται από τον (State et al, 2009), με τη διαφορά ότι η αξιολόγηση βασίζεται στο πλήθος των μηνυμάτων που πρέπει να επεξεργάζεται ο πάροχος προκειμένου να ολοκληρώσει μία κλήση προς ένα προορισμό που βρίσκεται σε μία μόνο συσκευή από τις πολλές που πιθανόν έχει ενεργοποιήσει (χρήστης με κινητικότητα μεταξύ σταθερών συσκευών).

Τα άρθρα των Kushal και Sahoo (2007), βασίζονται σε περιοδική πληροφόρηση για την κατάσταση των εξυπηρετητών (Gateways), η οποία επιτυγχάνεται μέσω του πρωτοκόλλου TGREP (Telephony Gateway REgistralion Protocol) ή του I-TRIP (Internal-Telephony Routing over IP). Αυτό συνεπάγεται όμως ότι οι προτεινόμενες πολιτικές περιορίζονται σε ελεγχόμενες αγορές, για παράδειγμα όταν ένας πάροχος διαθέτει δικούς του εξυπηρετητές και επιθυμεί να επιλέξει αυτόν που ικανοποιεί τα κριτήρια που έχει θέσει. Οι λόγοι είναι ότι αυτές οι πληροφορίες α) ενδέχεται να μην είναι αξιόπιστες και β) δεν υπάρχει προτυποποιημένο πρωτόκολλο που να τις διακινεί [Kushal και Sahoo (2007)].

Για παράδειγμα, το πρωτόκολλο δρομολόγησης E-TRIP (E-Telephony Routing over IP) δε διακινεί τέτοιες δυναμικές πληροφορίες μεταξύ των παρόχων για να αποφευχθεί η αποστολή μεγάλου αριθμού μηνυμάτων. Δηλαδή τα δεδομένα ενσωματώνονται σε αυτόνομα πακέτα τα οποία μπορεί να ακολουθήσουν διαφορετικό μονοπάτι για να φτάσουν στον προορισμό τους.

Οι συγγραφείς συμπεραίνουν ότι ολοκληρώνονται περισσότερες διαδοχικές κλήσεις όταν δρομολογούνται προς τις πύλες τηλεφωνίας με το μεγαλύτερο ποσοστό διαθέσιμων πόρων, παρά με τους περισσότερους διαθέσιμους πόρους κατά απόλυτη τιμή. Ο λόγος είναι ότι στη δεύτερη περίπτωση, το επιλεγμένο Gateway ενδέχεται να κορεστεί γρήγορα με αποτέλεσμα ο εξυπηρετητής του παρόχου να συνεχίσει να το χρησιμοποιεί μέχρι να λάβει νέο μήνυμα. Με άλλα λόγια, η επιλογή ενός Gateway κατά αναλογία των πόρων του αποδίδει καλύτερα επειδή εξισορροπεί καλύτερα το φόρτο κατά μέσο όρο. Οι Schlesener και Frost (2013), σε άρθρο τους, εξετάζουν την επίδραση που μπορεί να έχει το πρωτόκολλο I-TRIF στην εφαρμογή της βέλτιστης επιλογής Gateway.

Το σενάριο που εξετάζουν αφορά δύο παρόχους υπηρεσιών VoIP στο οποίο ο καθένας λειτουργεί μία πύλη τηλεφωνίας και επιλέγει την πύλη του άλλου μόνο όταν η ιδιόκτητη πύλη δε διαθέτει πόρους. Δηλαδή και σε αυτή την περίπτωση, οι πάροχοι ακολουθούν τη στρατηγική δρομολόγησης μονής προσπάθειας. Πραγματοποιώντας προσομοιώσεις διαπίστωσαν ότι όταν η καθυστέρηση διάδοσης των μηνυμάτων αυξάνεται (π.χ. > 125ms) τότε η πιθανότητα επιλογής ενός μπλοκαρισμένου εξυπηρετητή ενδέχεται να αυξηθεί σημαντικά. Ο λόγος είναι ότι η πληροφορία της κατάστασής του μπορεί να είναι ξεπερασμένη

όταν φτάσει στον προορισμό και επομένως δε θα επιλεχθεί ο εξυπηρετητής του άλλου παρόχου. Όπως αναμένεται, η επίδραση αυτού του παράγοντα μεγαλώνει καθώς αυξάνει η χρησιμοποίηση των Gateways. Επίσης, οι Chapman et al (2012) προτείνουν μία γενικότερη πολιτική διαχείρισης κλήσεων στοχεύοντας να πετύχει ισορροπία μεταξύ των εξής στοιχείων:

• αποδοτικότητα δικτύου (εκφρασμένη ως μειωμένη πιθανότητα αποτυχίας μιας κλήσης και ικανοποιητική ποιότητα υπηρεσίας στη μετάδοση των δεδομένων φωνής),

• μεγιστοποίηση χρησιμότητας χρηστών (έτσι ώστε να έχουν προτεραιότητα οι χρήστες που είναι διατεθειμένοι να πληρώσουν περισσότερο για την ίδια υπηρεσία), και

• μεγιστοποίηση των κερδών των παροχών (ώστε να έχουν κίνητρο να εφαρμόσουν την προτεινόμενη πολιτική). Οι ανωτέρω στόχοι επιτυγχάνονται συνδυάζοντας τους μηχανισμούς: Ο πρώτος αφορά στον έλεγχο αποδοχής κλήσεων (call admission control) εφαρμόζοντας χρέωση συμφόρησης (congestion pricing) όταν το επιλεγμένο Gateway πλησιάζει στο μέγιστο των δυνατοτήτων του και ο δεύτερος αφορά στην πολιτική δρομολόγησης του παρόχου.

Συγκεκριμένα, η προτεινόμενη πολιτική δρομολόγησης υποδεικνύει ότι ο πάροχος θα πρέπει να εφαρμόσει τη στρατηγική μονής προσπάθειας λαμβάνοντας υπόψη τους διαθέσιμους πόρους των πυλών τηλεφωνίας καθώς και τα χαρακτηριστικά του δικτύου προς αυτά. Η Bozinovski (2010) περιγράφει και αξιολογεί πολιτικές επιλογής εναλλακτικών εξυπηρετητών του ίδιου παρόχου (pooled servers) ώστε σε κάθε απόπειρα να μεγιστοποιείται η πιθανότητα να εγκατασταθεί η σύνοδος. Μετά από μία αποτυχημένη προσπάθεια, επιλέγεται ο επόμενος στη σειρά προτίμησης με βάση πληροφορίες που έχουν συλλεχθεί από τις τελευταίες χρονικές στιγμές που βρέθηκε κάθε εξυπηρετητής α) διαθέσιμος και β) πλήρης. Η γνώση για τους υπάρχοντες εξυπηρετητές και εν μέρει η διαθεσιμότητά τους βασίζεται στην ύπαρξη του πρωτοκόλλου RSerPool δηλαδή δεν απαιτείται η περιοδική δοκιμή εξυπηρετητών για να διαπιστωθεί η τρέχουσα κατάστασή τους. Ωστόσο, η αξιοπιστία των πληροφοριών που διακινούνται με αυτό το πρωτόκολλο μπορεί να είναι αμφισβητήσιμη σε ένα ανταγωνιστικό περιβάλλον όπου υπάρχουν εξυπηρετητές πολλών παρόχων.

Αντίθετα, η συλλογή ιστορικών δεδομένων για την εξαγωγή συμπερασμάτων σχετικά με τη

στατιστική συμπεριφορά των εναλλακτικών Gateways μπορεί να οδηγεί στη δοκιμαστική δρομολόγηση κλήσεων προς κάποια από αυτά, παρόλο που μπορεί να μην επιλέγονταν διαφορετικά, αλλά προσφέρει μεγαλύτερη αξιοπιστία. Επίσης, εξετάζονται πολιτικές δρομολόγησης για εισερχόμενες συνόδους προς χρήστες στο IP (π.χ. κλήσεις VoIP), οι οποίοι ενδέχεται να έχουν κάνει καταχώρηση σε πολλές συσκευές (κινητικότητα χρηστών). Στην περίπτωση αυτή αποτυχία μιας προσπάθειας έχουμε όταν η συσκευή που δοκιμάζεται δεν είναι αυτή στην οποία βρίσκεται ο χρήστης τη δεδομένη στιγμή ή εξαντλήθηκε η υπομονή του καλώντος (αν και δε λαμβάνεται υπόψη κατά την αξιολόγηση).

Προτείνουν την πολιτική «pipelined» η οποία συνδυάζει χαρακτηριστικά της ακολουθιακής και της παράλληλης πολιτικής. Προσπάθειες έναρξης συνόδου προς εναλλακτικές δικτυακές διευθύνσεις του χρήστη γίνονται εισάγοντας μια τεχνητή καθυστέρηση, έστω d, με βάση κάποιο κριτήριο. Διευθύνσεις που έχουν παρόμοια τιμή κριτηρίου ομαδοποιούνται και χρησιμοποιούνται παράλληλα. Σκοπός τους είναι η αντιστάθμιση μεταξύ καθυστέρησης στην εγκατάσταση συνόδου (περίπτωση ακολουθιακής πολιτικής ή sequential) και αυξημένης χρήσης πόρων (περίπτωση παράλληλης πολιτικής ή forking). Συγκρίνουν το κόστος εγκατάστασης της κλήσης (πλήθος μηνυμάτων) και την καθυστέρηση εγκατάστασης της κλήσης για τις πολιτικές forking και pipelined για δύο περιπτώσεις κατανομών της τρέχουσας θέσης του χρήστη- την ομοιόμορφη και αυτή στην οποία ο χρήστης έχει ορισμένες δημοφιλείς θέσεις. Δείχνουν ότι η πολιτική pipelined πετυχαίνει καλύτερα αποτελέσματα σε σχέση με την πολιτική forking, ιδιαίτερα για τη δεύτερη μορφή κινητικότητας χρηστών. Η πληροφορία για την πίεση του χρήστη θα μπορούσε να χρησιμοποιηθεί ώστε να αυξηθεί η πιθανότητα μια προσπάθεια να είναι επιτυχημένη και ταυτόχρονα να μη δεσμεύονται πόροι υπερβολικά.

Αξίζει να σημειωθεί ότι η πολιτική pipelined έχει πολλές ομοιότητες με την πολιτική που προτείνουμε (π.χ. όταν υπάρχει χρόνος για περισσότερες από μία προσπάθειες). Αν και περιγράφεται η πολιτική αυτή, δεν προτείνεται ένας τρόπος για βέλτιστη χρήση της. Για παράδειγμα, το πλήθος των θέσεων που θα δοκιμαστούν κάθε φορά δεν προκύπτει από κάποιο αναλυτικό μοντέλο που θα μπορούσε να χρησιμοποιηθεί ως αλγόριθμος εύρεσης

βέλτιστης στρατηγικής. Αντίθετα, η αξιολόγηση των πολιτικών ως προς την καθυστέρηση εγκατάστασης της κλήσης γίνεται με χρήση προσομοιώσεων, υπάρχει, όμως, θεωρητική ανάλυση σε ό,τι αφορά την αξιολόγηση των πολιτικών ως προς το πλήθος των μηνυμάτων σηματοδοσίας.

Αντίθετα, εμείς θεωρούμε ότι οι εξυπηρετητές σηματοδοσίας μπορούν να διαχειριστούν μεγάλο αριθμό μηνυμάτων και δε λαμβάνουμε υπόψη αυτό το κόστος στην ανάλυσή μας. Τέλος, τα πρωτόκολλα MPLS μπορούν να χρησιμοποιηθούν και για την γρηγορότερη εγκατάσταση των κλήσεων. Για παράδειγμα, το άρθρο των Kim et al (2014) προτείνει μία επέκταση στο SIP η οποία μπορεί να λαμβάνεται υπόψη από τους δρομολογητές που υποστηρίζουν MPLS ώστε να εκχωρούν μεγαλύτερη προτεραιότητα στα πακέτα αυτά.

ΚΕΦΑΛΑΙΟ 2- Πρωτόκολλα που χρησιμοποιούνται στο VOIP

2.1. Πρωτόκολλο TRIP (Telephony Routing over IP)

Το TRIP είναι ένα πρωτόκολλο που στοχεύει στην ανταλλαγή πληροφοριών δρομολόγησης μεταξύ παρόχων που διαθέτουν πύλες τηλεφωνίας (Gateways). Πιο συγκεκριμένα, χρησιμοποιείται ώστε ένας πάροχος να ενημερώσει τους γείτονές του για τις ιδιότητες των Gateways που διαθέτει ο ίδιος ή έμαθε από άλλους γείτονές του. Οι ιδιότητες αυτές περιλαμβάνουν τους τηλεφωνικούς προορισμούς που εξυπηρετούν, τη δικτυακή διεύθυνση IP του Gateway καθώς και άλλες ιδιότητές τους, όπως το μέγιστο πλήθος ταυτόχρονων κλήσεων που μπορούν να εξυπηρετήσουν. Το TRIP όντας ένα πρωτόκολλο επιλογής προτιμητέου γείτονα χρησιμοποιείται για να διαδώσει ένα μόνο Gateway για κάθε τηλεφωνικό προορισμό. Ωστόσο, οι πάροχοι μπορούν να μάθουν εναλλακτικούς τρόπους ολοκλήρωσης κλήσεων προς τηλεφωνικούς αριθμούς συλλέγοντας πληροφορίες από πολλούς γείτονες. Με αυτό τον τρόπο δημιουργούν τον πίνακα δρομολόγησης, στον οποίο αναζητείται ο επόμενος κόμβος στο μονοπάτι της σηματοδοσίας όταν χρειαστεί να πραγματοποιηθεί μία κλήση. Να σημειωθεί ότι εξ' ορισμού οι πίνακες δρομολόγησης περιλαμβάνουν ένα μόνο προεπιλεγμένο Gateway για κάθε τηλεφωνικό προορισμό, ωστόσο μπορούν να τροποποιηθούν για να περιλαμβάνουν περισσότερα (Collier, 2005).

2.2. Πρωτόκολλο H.501

Το πρωτόκολλο H.501, όπως και το TRIP, είναι ένα πρωτόκολλο δρομολόγησης το οποίο ανήκει στη σουίτα πρωτοκόλλων του H.323. Μάλιστα έχουν την ίδια ακριβώς φιλοσοφία και τρόπο λειτουργίας. Η μόνη ουσιαστική διαφορά τους είναι ότι το H.501 επιτρέπει την ανταλλαγή περισσότερων πληροφοριών, όπως για παράδειγμα τη χρέωση ενός Gateway

(Geneiatakis et al, 2005).

2.3. Πρωτόκολλο DUND (Distributed Universal Number Discovery)

Σε αντίθεση με τα πρωτόκολλα TRIP και H.501, το DUND είναι ένα πρωτόκολλο που βασίζεται στην τεχνική της «πλημμύρας». Όταν ένας πάροχος δεχτεί μία εισερχόμενη κλήση τότε θα κοιτάξει στην τοπική βάση δεδομένων του (dialplan) αν περιέχει τον προορισμό. Εάν βρεθεί, τότε ο προορισμός είναι πελάτης του κι επομένως ξέρει ποια είναι η δικτυακή του διεύθυνση. Εάν όμως δεν είναι πελάτης του, τότε θα ρωτήσει τους παρόχους με τους οποίους συνεργάζεται μήπως γνωρίζουν εκείνοι ποια είναι η τρέχουσα δικτυακή διεύθυνση του προορισμού, ή μπορούν να τη μάθουν προωθώντας το ερώτημα στους δικούς τους γείτονες (Dunde, 2007).

Στη δεύτερη περίπτωση, ο πάροχος θα περιμένει μέχρι να λάβει μία τουλάχιστον διεύθυνση IP του προορισμού, ή να περάσει κάποιο χρονικό διάστημα. Εάν βρεθεί ο πάροχος του προορισμού τότε απαντά περιλαμβάνοντας τη διεύθυνση IP του εξυπηρετητή που θα δεχτεί την αίτηση εγκατάστασης κλήσης. Η απάντηση αυτή ακολουθεί το αντίθετο μονοπάτι και φτάνει στον τελικό αποδέκτη. Δηλαδή στην περίπτωση του DUND ο πάροχος δε διατηρεί πίνακα δρομολόγησης, αλλά ψάχνει να βρει τον πάροχο του προορισμού σε καθεστώς ζήτησης (on-demand). Αυτό όμως έχει αντίκτυπο στο χρόνο εγκατάστασης της κλήσης.

Το αναγνωριστικό με το οποίο γίνεται αναζήτηση μπορεί να είναι ένας τηλεφωνικός αριθμός, μία διεύθυνση IP, μία διεύθυνση SIP ή μία διεύθυνση H.323, και εξαρτάται από το πρωτόκολλο σηματοδοσίας που χρησιμοποίησε ο καλών. Να σημειωθεί, ότι το DUND εκτελείται μεταξύ των εξυπηρετητών Asterisk και προϋποθέτει ότι οι δύο πάροχοι έχουν συμφωνήσει με τους όρους “καλής γειτονίας” για λόγους ασφάλειας (π.χ. αποφυγή ανεπιθύμητων κλήσεων) (Dunde, 2007).

2.4. Διαχείριση πολυμεσικών συνόδων

Η διαχείριση των συνόδων γίνεται με χρήση πρωτοκόλλων σηματοδοσίας. Τα σημαντικότερα πρωτόκολλα, και τα οποία θα περιγράφουμε στη συνέχεια, είναι το SIP και το H.323.

2.4.1. Πρωτόκολλο SIP (Session Initiation Protocol)

Το SIP είναι ένα πρωτόκολλο σηματοδοσίας που ορίζει ότι χρειάζεται για να επικοινωνήσουν τα ενδιαφερόμενα μέρη. Συγκεκριμένα, προσδιορίζει τη μορφή των διευθύνσεων SIP αλλά και τη δομή και ακολουθία μηνυμάτων για τη διαχείριση των συνόδων (π.χ. έναρξη, τροποποίηση και ολοκλήρωση κλήσεων). Μπορεί να χρησιμοποιηθεί ακόμη και χωρίς το TTL (Time-To-Live), είναι ένας μετρητής που έχει προκαθορισμένη τιμή το 32 και μειώνεται κατά ένα κάθε φορά που η επερώτηση φτάνει σε ένα κόμβο. Δηλαδή μέχρι 32 διαδοχικοί γείτονες μπορεί να ρωτηθούν, αν και οι διαχειριστές μπορούν να ορίσουν και μικρότερη τιμή.

Ωστόσο, η ανάγκη για εύρεση της τρέχουσας δικτυακής διεύθυνσης του προορισμού αποτελεί σημαντικό λόγο για τη συμμετοχή των παρόχων στη φάση εγκατάστασης της κλήσης. Μάλιστα, στην τυπική περίπτωση που δεν ανήκουν στον ίδιο πάροχο τότε θα συμμετέχουν τουλάχιστον δύο εξυπηρετητές.

Να σημειωθεί ότι το SIP δεν περιορίζεται στο VoIP. Αντιθέτως, αποτελεί ένα μέσο για να μεταφέρει την περιγραφή μιας συνόδου στον προορισμό και μετά χρησιμοποιείται όποτε χρειάζεται να αλλάξει η κατάσταση αυτής της συνόδου. Για αυτόν ακριβώς το λόγο, οι εξυπηρετητές σηματοδοσίας δε συμμετέχουν στη μετάδοση των πακέτων φωνής αφού εγκατασταθεί μία τηλεφωνική κλήση. Αυτό έχει σαν αποτέλεσμα οι εξυπηρετητές να καταφεύγουν σε τεχνάσματα προκειμένου να πετύχουν εφάμιλλη ποιότητα υπηρεσίας με αυτή του PSTN.

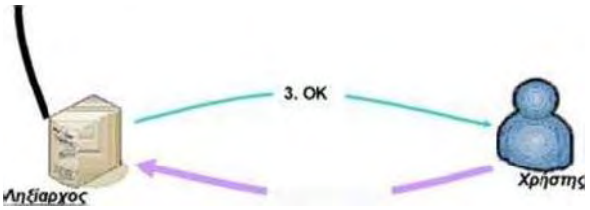
Υπάρχουν δύο ειδών οντότητες στο SIP οι τερματικές συσκευές και οι εξυπηρετητές. Ένα τερματικό μπορεί είτε να ξεκινά μία σύνοδο ή να αποτελεί τον τελικό αποδέκτη μιας αίτησης.

Παραδείγματα τερματικών συσκευών που έχουν υιοθετήσει το SIP είναι σταθερές τηλεφωνικές συσκευές με μία διεπαφή δικτύου (π.χ. Ethernet) και κινητά τηλέφωνα με δύο ή περισσότερες διεπαφές δικτύου dual-mode (π.χ. UMTS, Wi-Fi). Πρέπει να σημειωθεί ότι η σύγκλιση των επικοινωνιών που περιγράψαμε, δε θα ήταν ελκυστική για τους χρήστες αν δεν υπήρχαν συσκευές που να δέχονται αιτήσεις από οποιαδήποτε διεπαφή όσο είναι σε κατάσταση αναμονής.

Ο βασικός τύπος εξυπηρετητών στο SIP ονομάζονται Proxies και είναι αυτοί που δέχονται αιτήματα για έναρξη συνόδων και τα κατευθύνουν προς τον προορισμό εφαρμόζοντας την πολιτική του παρόχου. Υπάρχουν τρεις τύποι Proxies, ανάλογα με το βαθμό των πληροφοριών που διατηρούν κατά την εξυπηρέτηση των μηνυμάτων:

- Stateless Proxies, οι οποίοι προωθούν τα μηνύματα χωρίς να κρατούν πληροφορίες για την κατάσταση της συνόδου. Παράδειγμα τέτοιων εξυπηρετητών είναι οι Redirect Proxies που αντί να προωθήσουν το μήνυμα προς τον προορισμό του, ανακατευθύνουν την πηγή του μηνύματος σε κάποιο άλλο αρμόδιο Proxy. Εάν αυτός ο νέος Proxy δεν ανήκει στον ίδιο πάροχο τότε αυτός χάνει πλέον τον έλεγχο της κλήσης.

- Transaction-stateful Proxies, οι οποίοι διατηρούν όσες πληροφορίες χρειάζεται προκειμένου να διαχειριστούν μια σύνοδο. Μία ομάδα μηνυμάτων που πρέπει να αποσταλεί επιτυχώς προκειμένου να πραγματοποιηθεί η σύνοδος ονομάζεται συναλλαγή (transaction).



Εικόνα 2- : Η διαδικασία καταχώρησης της τρέχουσας δικτυακής διεύθυνσης ενός χρήστη στο SIP

Για παράδειγμα, κατά την έναρξη μιας κλήσης οι εξυπηρετητές αυτοί διατηρούν πληροφορίες μέχρι τα ενδιαφερόμενα μέρη να αρχίσουν να επικοινωνούν. Αντίστοιχα, η διαδικασία τερματισμού μιας κλήσης αποτελεί ξεχωριστή συναλλαγή.

✦ Call-stateful Proxies, οι οποίοι διατηρούν όλες τις απαραίτητες πληροφορίες κατά όλη τη διάρκεια μιας κλήσης. Εκτός από τους Proxies υπάρχουν και άλλοι δύο τύποι εξυπηρετητών οι οποίοι είναι απαραίτητοι για την επιτυχή διαχείριση των συνόδων. Ο πρώτος είναι ο Ληξίαρχος (Registrar), ο οποίος δέχεται αιτήσεις καταχώρησης από τελικούς χρήστες και τις αποθηκεύει στον Εξυπηρετητή Τοποθεσίας (Location Server), που είναι ο δεύτερος τύπος. Αυτή η αντιστοίχιση μεταξύ αναγνωριστικού χρήστη και δικτυακής διεύθυνσης διατηρείται στον Εξυπηρετητή Τοποθεσίας που ουσιαστικά είναι μία βάση δεδομένων. Στο σημείο αυτό αξίζει να σημειωθεί ότι ο πάροχος διατηρεί αυτήν τη συσχέτιση ακόμη και στην περίπτωση περιαγωγής (Abdelnur et al, 2009).

Τα βασικά μηνύματα SIP είναι τα εξής (Vrakas et al, 2012):

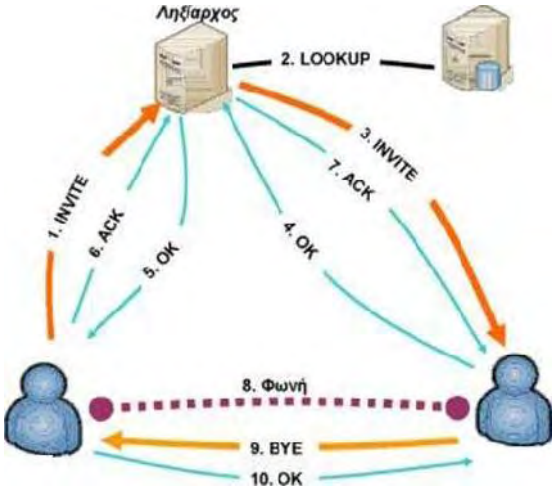
- REGISTER με το οποίο ένας χρήστης πληροφορεί τον πάροχο για την τρέχουσα δικτυακή διεύθυνση της συσκευής που χρησιμοποιεί. Να σημειωθεί ότι ένας χρήστης μπορεί να καταχωρήσει πολλές συσκευές ταυτόχρονα σε μία διεύθυνση SIP (αναγνωριστικό χρήστη). Όλες αυτές θα διατηρούνται στον Εξυπηρετητή Τοποθεσίας.
- INVITE με το οποίο ένας χρήστης αιτείται την έναρξη μιας συνόδου προς το αναγνωριστικό του χρήστη που περιέχεται μέσα στο μήνυμα. Αυτό είναι το σημαντικότερο μήνυμα στο SIP και η αντίδραση ενός Proxy εξαρτάται από την πολιτική

του παρόχου. Μπορούμε, ωστόσο, να διακρίνουμε δύο περιπτώσεις (Abdelnur et al, 2009):

1. Στην περίπτωση που ο προορισμός εξυπηρετείται άμεσα από ένα Proxy τότε αυτός αρκεί να προωθήσει την αίτηση σε όλες τις καταχωρημένες συσκευές του χρήστη. Με αυτό τον τρόπο είναι πιθανότερο ο καλούμενος να ακούσει και να απαντήσει την κλήση. Αυτή η εγγενής λειτουργία του SIP ονομάζεται forking και αποτέλεσε την ιδέα για ανάπτυξη ευέλικτων στρατηγικών δρομολόγησης κλήσεων.

2. Εάν ο προορισμός δεν εξυπηρετείται άμεσα από τον Proxy, τότε μπορεί να αναζητήσει επιπλέον αναγνωριστικά χρησιμοποιώντας κάποιον από τους μηχανισμούς που περιγράφηκαν, και στη συνέχεια για κάθε επιλεγμένο αναγνωριστικό να επιλέξει έναν ή περισσότερους κόμβους στους οποίους να προωθήσει την αίτηση.

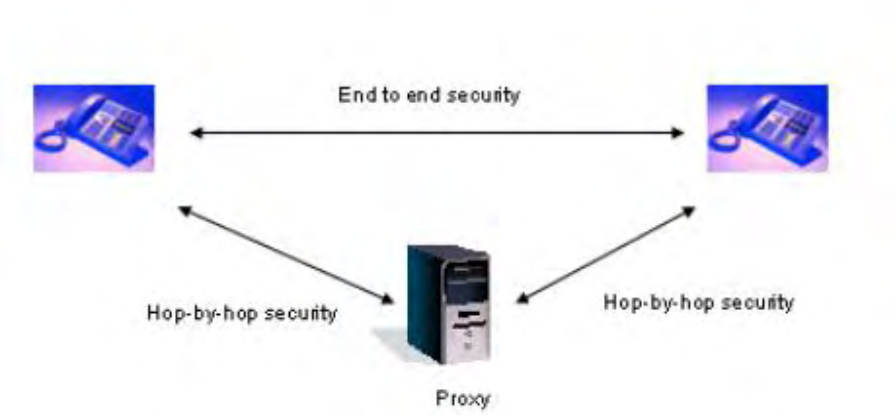
- CANCEL με το οποίο ένας Proxy ενημερώνει κάποιους άλλους να διακόψουν μία απόπειρα εγκατάστασης κλήσης. Αυτό το μήνυμα μπορεί να είναι χρήσιμο για κάποιον Proxy που εφαρμόζει τις προτεινόμενες στρατηγικές. Για παράδειγμα, αν ο χρήστης απαντήσει αλλά το μήνυμα INVITE έχει προωθηθεί προς εναλλακτικά αναγνωριστικά του ίδιου χρήστη, τότε ο εξυπηρετητής μπορεί να ακυρώσει τις αιτήσεις προς τα πλεονάζοντα αναγνωριστικά στέλνοντας ένα μήνυμα CANCEL. Μία ιδιαίτερη περίπτωση εξυπηρετητών Call-stateful Proxies είναι οι Back-to-Back User Agents, οι οποίοι λειτουργούν ταυτόχρονα σαν τερματικά και σαν εξυπηρετητές. Εάν για παράδειγμα, μεσολαβεί ένας τέτοιος εξυπηρετητής μεταξύ δύο τερματικών τότε η κλήση θα αποτελείται, εν αγνοία τους, από δύο μέρη. Το πρώτο σκέλος θα φτάνει μέχρι το Back-to-Back User Agent και εκεί θα γεφυρώνεται με το δεύτερο σκέλος της κλήσης. Αυτό φαίνεται στην εικόνα 3. Ο βασικός λόγος χρήσης τους είναι για μεγαλύτερο έλεγχο των παρεχόμενων υπηρεσιών (π.χ. προπληρωμένες κάρτες ομιλίας) αλλά και για καλύτερη ποιότητα υπηρεσίας (Vrakas et al, 2012).



Εικόνα 3- Επικοινωνία SIP

Πρωτόκολλο - Σύνδεση SIP

Μια σύνδεση SIP μπορεί είτε να παρέχεται απευθείας μεταξύ πρακτόρων-χρηστών είτε με τρόπο hop-by-hop, όπως φαίνεται στην εικόνα 4.



Εικόνα 4- Σύνδεση SIP

Τα παρακάτω παραδείγματα δείχνουν μια κλήση που δημιουργήθηκε και τερμάτισε για αυτά τα δύο σενάρια. Παράδειγμα 1 στην εικόνα 5 :

Αλίκη, sip: alice@atlanta.com, καλεί τον Bob, sip: bob@biloxi.com, σε μια κλήση και να δημιουργήσει επιτυχώς μια σύνοδο SIP απευθείας μεταξύ των δύο χρηστών:

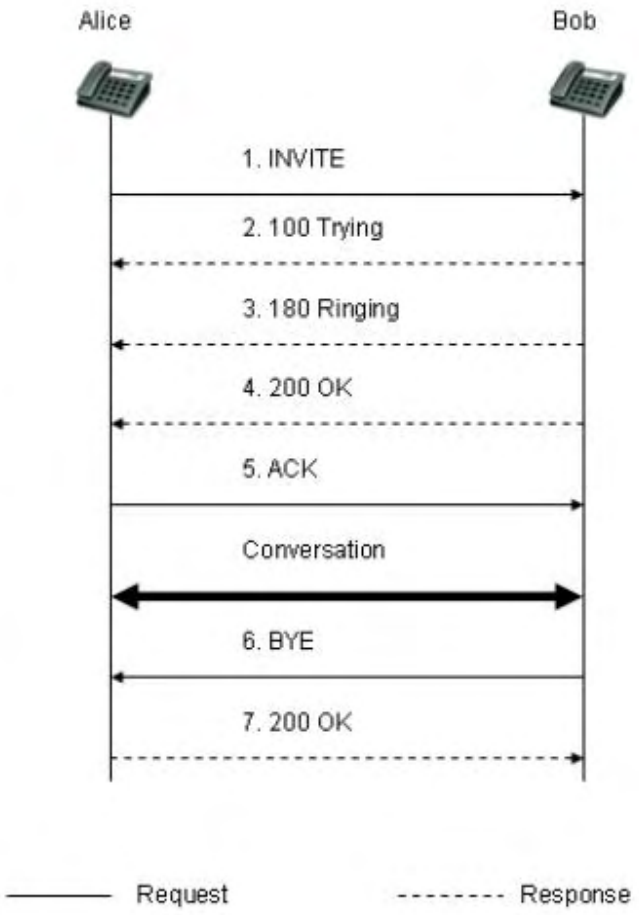
1. Η Alice (UAC) στέλνει ένα αίτημα (μήνυμα INVITE) απευθείας στον Bob (UAS).

2. Το UAS αποκρίνεται με ένα 100 μήνυμα που προσπαθεί.

3. Το UAS αποστέλλει επίσης 180 απαντήσεις που ενημερώνουν το UAC ότι το τηλέφωνο του Bob κουδουνίζει.

4. Ο Bob απαντά στο τηλέφωνο και το UAS στέλνει ένα μήνυμα 200 OK στο UAC

5. Το UAC αποστέλλει ένα μήνυμα ACK για να ενημερώσει το UAS ότι η απάντηση λήφθηκε. Έχει δημιουργηθεί μια περίοδος σύνδεσης και μεταφέρονται φωνητικά ή άλλα δεδομένα με το πρωτόκολλο RTP.



Εικόνα 5- Σύνδεση UA σε UA

6. Ο Bob ολοκληρώνει την κλήση και στέλνει ένα μήνυμα BYE.

7. Το UAC της Alice αποκρίνεται με ένα μήνυμα 200 OK και η συνεδρία ολοκληρώνεται.

Παράδειγμα 2 στην εικόνα 6:

Alice sip: alice@atlanta.com προσκαλεί Bob sip: bob@biloxi.com σε μια κλήση και να δημιουργήσει επιτυχώς μια σύνοδο SIP μεταξύ των δύο χρηστών που διέρχονται από δύο πληρεξούσια.

Ο έλεγχος ταυτότητας χρήστη δεν εμφανίζεται σε αυτό το παράδειγμα:

1. Η Alice (UAC) στέλνει ένα αίτημα (μήνυμα INVITE) στο proxy Atlanta.

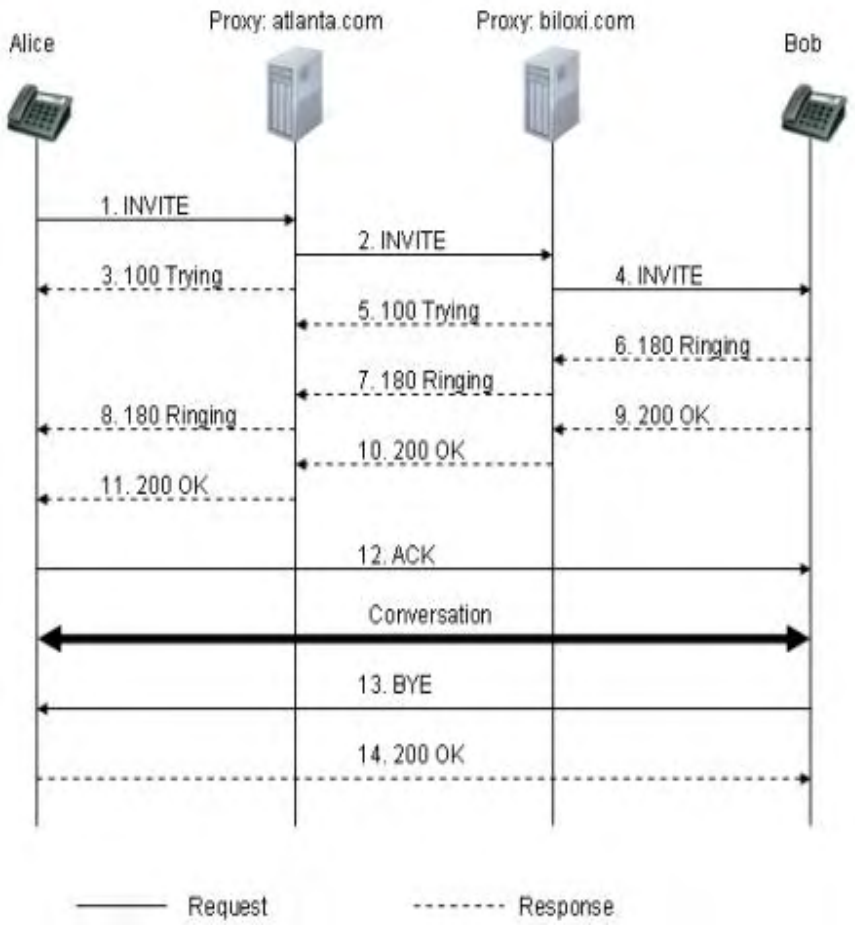
2. Το proxy atlanta προωθεί το μήνυμα INVITE στο Proxy Biloxi.

3. Το proxy atlanta αποκρίνεται με ένα 100 μήνυμα που προσπαθεί.

4. Proxy biloxi προωθεί το INVITE στο χρήστη Bob 5.

Το proxy biloxi απαντά με ένα 100 μήνυμα που προσπαθεί.

6. Το UAS στέλνει επίσης ένα 180 Ringing αποκρίνεται ενημερώνοντας τον πληρεξούσιο ότι το τηλέφωνο του Bob χτυπάει.



Εικόνα 6- Σύνδεση Sip με χρήση proxy

7. Το proxy biloxi προωθεί την απάντηση κλήσης 180 στο Atlanta.

8. Το proxy atlanta προωθεί την απάντηση κλήσης 180 στην Alice που θα πάρει έναν τόνο.

9. Ο Bob απαντά στο τηλέφωνο και το UAS στέλνει ένα μήνυμα 200 OK στο proxy του Biloxi.

10. Το proxy biloxi προωθεί το 200 OK απάντηση στο Atlanta.

11. Proxy atlanta προωθεί την απάντηση 200 OK στην Alice.

12. Το UAC στέλνει ένα μήνυμα ACK απευθείας στον Bob. Έχει δημιουργηθεί μια περίοδος σύνδεσης και μεταφέρονται φωνητικά ή άλλα δεδομένα με το πρωτόκολλο RTP.

13. Ο Bob ολοκληρώνει την κλήση και στέλνει ένα μήνυμα BYE κατευθείαν στην Alice

14. Η Alice απαντά με ένα 200 μήνυμα OK και η συνεδρία ολοκληρώνεται

Το RFC3261 προτείνει ότι ένας διακομιστής μεσολάβησης SIP θα πρέπει να χρησιμοποιεί έλεγχο ταυτότητας HTTP Digest για τον έλεγχο ταυτότητας ενός User Agent Client. Ο έλεγχος ταυτότητας HTTP digest προσφέρει προστασία ταυτότητας και επανάληψης επίθεσης για τα μηνύματα INVITE και REGISTER. Ωστόσο, δεν προστατεύει άλλα μηνύματα όπως CANCEL, BYE και απαντήσεις σε αιτήματα. Ο έλεγχος ταυτότητας HTTP digest είναι επίσης ευάλωτος σε επιθέσεις με λεξικό και δεν εισάγει ακεραιότητα ή εμπιστευτικότητα δεδομένων σε ένα μήνυμα όπως φαίνεται στο HTTP Digest Authentication.

Αυτό καθιστά εύκολη την παρακολούθηση των μηνυμάτων και τη χρήση διαφορετικών εργαλείων για την ανάκτηση ενός κωδικού πρόσβασης. Εργαλεία όπως SiVus, Cain και Wireshark που είναι διαθέσιμα στο Internet μπορούν να χρησιμοποιηθούν για να επιτευχθεί αυτό. Ο έλεγχος ταυτότητας HTTP digest που περιγράφεται στο RFC3261 δεν προσφέρει αμοιβαίο έλεγχο ταυτότητας καθιστώντας αδύνατον για τον χρήστη να πιστοποιήσει τον διακομιστή μεσολάβησης SIP.

Το IETF προτείνει στο σχέδιο Internet ότι η προδιαγραφή SIP θα πρέπει να ενημερωθεί με νέα πεδία επικεφαλίδας που θα επιτρέπουν τον αμοιβαίο έλεγχο ταυτότητας. Ο έλεγχος ταυτότητας HTTP digest είναι ένα πρωτόκολλο πρόκλησης-απόκρισης [18] όπου το nonce στέλνεται σε μια απάντηση από ένα διακομιστή για να αμφισβητήσει έναν πελάτη που έστειλε ένα αρχικό αίτημα (INVITE) και ζήτησε URI. Η απόκριση παράγεται από το όνομα χρήστη και τον κωδικό πρόσβασης. Αυτό συχνά γίνεται με τον αλγόριθμο κατακερματισμού MD5, αλλά μπορούν να χρησιμοποιηθούν και άλλοι αλγόριθμοι κατακερματισμού.

Ο πελάτης στέλνει ένα νέο αίτημα (INVITE) που περιέχει τώρα μια κεφαλίδα εξουσιοδότησης με την αντίδραση που δημιουργήθηκε. Η εικόνα 7, δείχνει ένα παράδειγμα

επαλήθευσης χρήστη με έλεγχο ταυτότητας HTTP digest όπως περιγράφεται στην προδιαγραφή SIP.

1. Η Alice (UAC) στέλνει ένα αίτημα (μήνυμα INVITE) στο proxy atlanta.

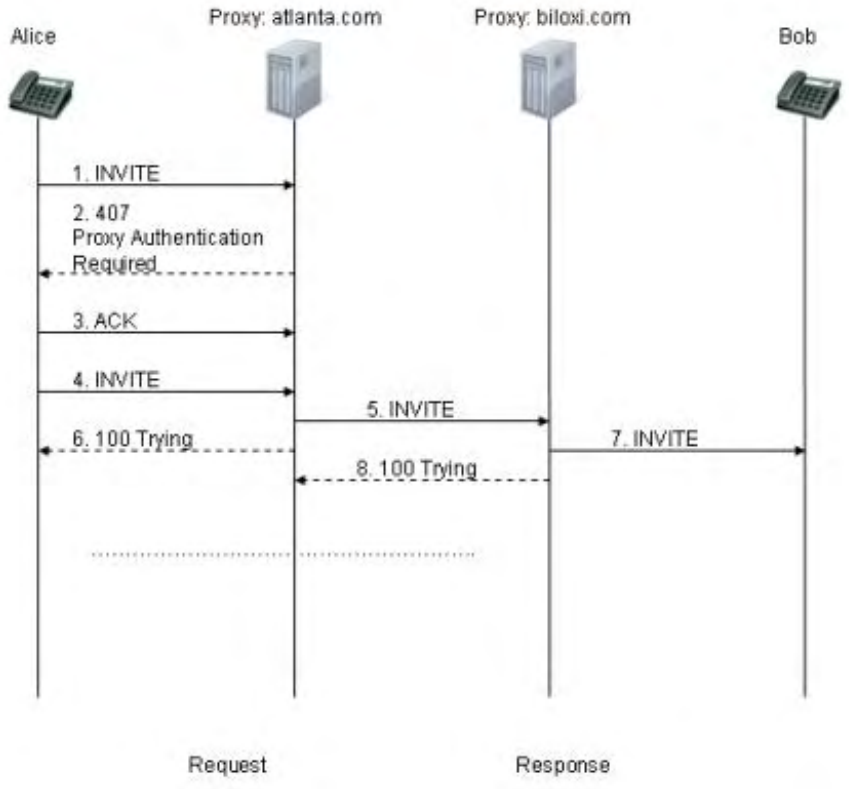
2. Το proxy atlanta απαιτεί έλεγχο ταυτότητας χρήστη και ανταποκρίνεται με ένα απαιτούμενο μήνυμα επαλήθευσης ταυτότητας 407 Proxy. Αυτή η απάντηση περιέχει ένα nonce που θα χρησιμοποιηθεί στη δημιουργία μιας απάντησης εξουσιοδότησης.

3. Η Alice (UAC) αναγνωρίζει το μήνυμα μεσολάβησης αποστέλλοντας ένα ACK.

4. Η Alice (UAC) στέλνει ένα νέο αίτημα (μήνυμα INVITE) στο proxy atlanta με πληροφορίες ταυτότητας που περιέχει την απάντηση εξουσιοδότησης.

5. Το proxy atlanta επαληθεύει τα διαπιστευτήρια και προωθεί το μήνυμα INVITE στο Proxy biloxi.

6. Το υπόλοιπο της ροής SIP είναι όπως περιγράφηκε προηγουμένως. Ο Pauli Vesterinen αναγνωρίζει στο έγγραφό του, ότι ο κωδικός χρήστη πρέπει να είναι γνωστός τόσο από τον χρήστη όσο και από τον πληρεξούσιο που χειρίζεται τον έλεγχο ταυτότητας. Αυτό πρέπει να θεωρηθεί ως μια αδυναμία στη λύση.



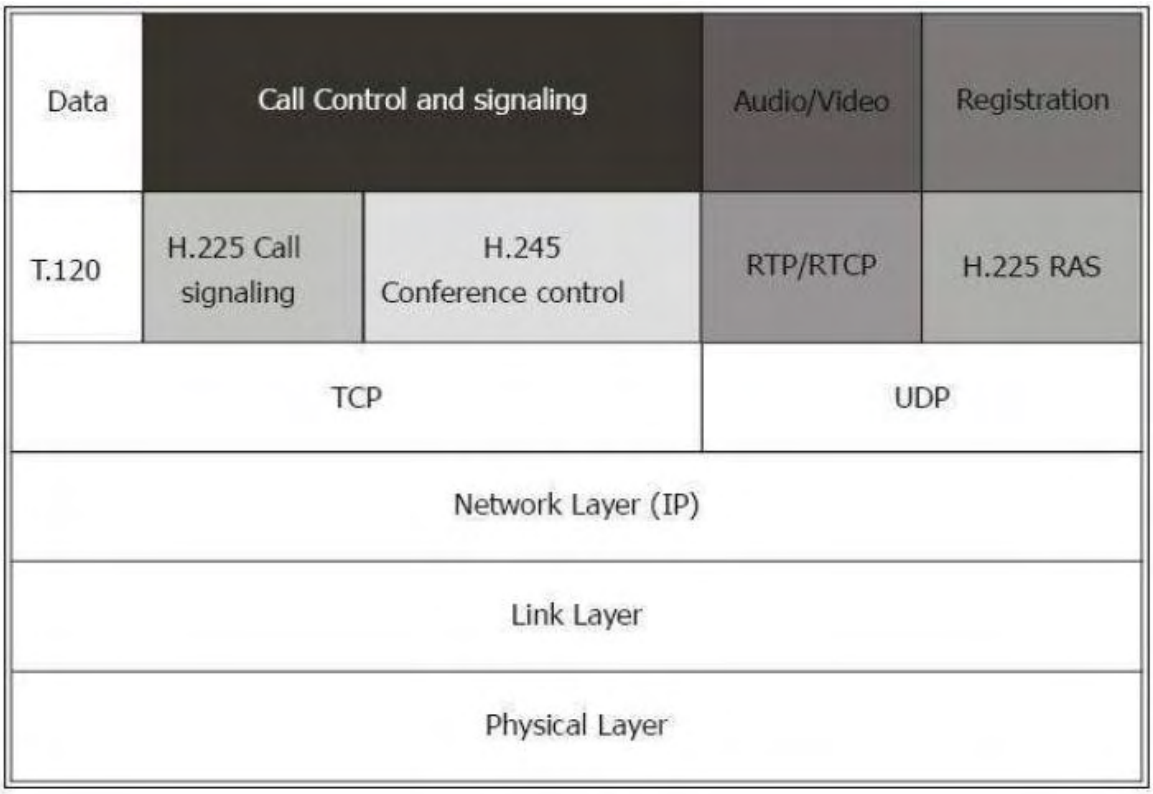
Εικόνα 7- HHTP digest

2.4.2. Πρωτόκολλο H.323

Το H.323 είναι μια σύσταση της ITU (Διεθνής Ένωση Τηλεπικοινωνιών) που προσδιορίζει μια πλήρη ομάδα πρωτοκόλλων για επικοινωνίες πολυμέσων πάνω από δίκτυα μεταγωγής πακέτου. Τα πρωτόκολλα αυτά προσδιορίζουν τα βήματα που πρέπει να γίνουν για την εγκατάσταση μιας κλήσης, μέχρι ειδικά πρότυπα κωδικοποίησης φωνής και video. Έχει παρόμοια λογική με το SIP καθώς το ρόλο του proxy αναλαμβάνει ο Gatekeeper, ο οποίος (αν και προαιρετικός) είναι υπεύθυνος για την εύρεση της δικτυακής διεύθυνσης του καλούμενου αλλά και την αποδοχή ή απόρριψη κλήσεων (call admission control).

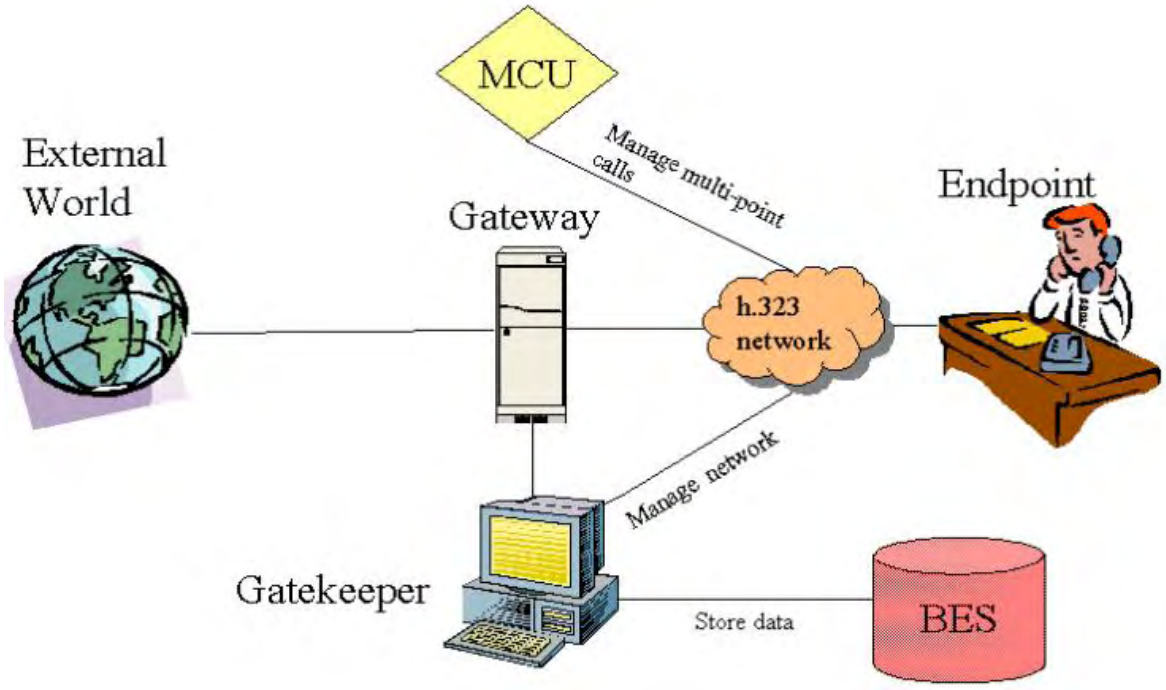
H.323 Protocol Stack

Πριν την περιγραφή των πρωτοκόλλων του H.323 προτύπου, αξίζει να σημειωθεί ότι τα πρωτόκολλα που υλοποιούν την εγκατάσταση μιας κλήσης χρησιμοποιούν το αξιόπιστο TCP ως πρωτόκολλο μεταφοράς των μηνυμάτων που ανταλλάσσονται μεταξύ των H.323 οντοτήτων, ενώ η μεταφορά των media δεδομένων κατά την εξέλιξη της κλήσης πραγματοποιείται μέσω του αναξιόπιστου πρωτοκόλλου UDP. Στην εικόνα 8 φαίνεται ένα διάγραμμα του H.323 protocol stack.



Εικόνα 8- H.323 protocol stack

Στην εικόνα 9 παρουσιάζεται η αρχιτεκτονική ενός συστήματος VOIP που στηρίζεται στο πρωτόκολλο H.323.



Εικόνα 9- Αρχιτεκτονική VOIP με χρήση του πρωτοκόλλου H.323

Μία σημαντική διαφορά είναι ότι ο Gatekeeper είναι υπεύθυνος και για την καταχώρηση των χρηστών, δηλαδή ενσωματώνει και το ρόλο του εξυπηρετητή τοποθεσίας. Επίσης, τα μηνύματα που ανταλλάσσονται είναι δυαδικά κωδικοποιημένα και επομένως χρησιμοποιούν πιο αποδοτικά τους δικτυακούς πόρους. Αντίθετα, τα μηνύματα του SIP είναι πιο εύκολα αναγνώσιμα από τους προγραμματιστές καθώς είναι σε μορφή κειμένου. Μία άλλη σημαντική διαφορά είναι ότι κατά τη φάση της εγκατάστασης μιας κλήσης χρησιμοποιούνται δύο πρωτόκολλα, το RAS και το H.225.0.

Το πρώτο χρησιμοποιείται για την επικοινωνία ενός τερματικού με το Gatekeeper, καθώς και για την επικοινωνία μεταξύ δύο Gatekeepers. Για την εγκατάσταση της κλήσης ανταλλάσσονται μηνύματα μεταξύ των τερματικών συσκευών.

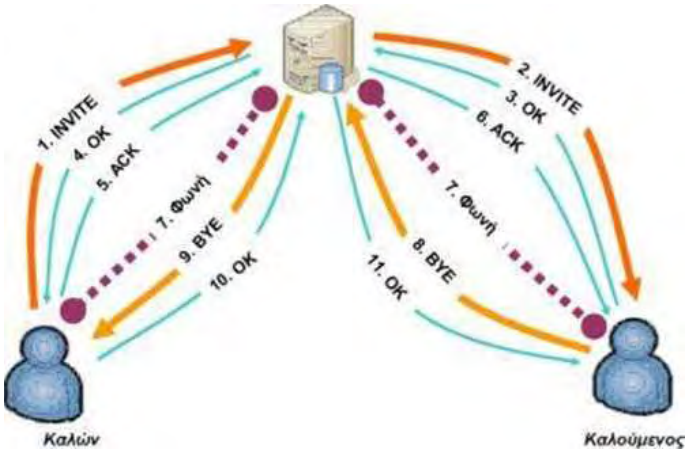
Στην εικόνα 10, απεικονίζονται τα βασικά βήματα για την εγκατάσταση μιας κλήσης όταν οι

δύο συμμετέχοντες στην κλήση ανήκουν σε διαφορετικούς παρόχους. Στα βήματα 1 έως 10 χρησιμοποιούνται μηνύματα του πρωτοκόλλου RAS, ενώ στα τελευταία μηνύματα του πρωτοκόλλου H.225.0:

1. Αρχικά, η τερματική συσκευή του χρήστη S στέλνει ένα μήνυμα RRQ στο Gatekeeper με το οποίο αντιστοιχεί το αναγνωριστικό του χρήστη με την τρέχουσα δικτυακή διεύθυνση. Δηλαδή, είναι το αντίστοιχο μήνυμα REGISTER στο SIP. Όπως και στο SIP ένας χρήστης μπορεί να έχει ταυτόχρονα πολλές ενεργές συσκευές.

2. Ο Gatekeeper εξετάζει τα στοιχεία λογαριασμού του χρήστη και (έστω ότι) του απαντάει θετικά με το μήνυμα R.CF.

Αργότερα, ο χρήστης S στέλνει ένα μήνυμα ARQ με το οποίο ζητά την εγκατάσταση μιας κλήσης με το χρήστη D.



Εικόνα 10- Η διαχείριση κλήσεων με H.225.0 RAS

3. Ο Gatekeeper του καλώντος θα αποφασίσει αν ο χρήστης έχει δικαίωμα να πραγματοποιήσει την κλήση. Στην περίπτωση που γίνεται δεκτή, ο Gatekeeper ελέγχοντας το αναγνωριστικό του προορισμού θα συμπεράνει ότι πρέπει να ρωτήσει το Gatekeeper για την τρέχουσα διεύθυνση IP του καλούμενου. Για αυτό το λόγο θα στείλει ένα μήνυμα LRQ.

4. Ο Gatekeeper θα βρει την τρέχουσα διεύθυνση IP του καλούμενου στην τοπική βάση δεδομένων και θα την προωθήσει στον Gatekeeper με το μήνυμα LCE. Ο Gatekeeper θα προωθήσει τη δικτυακή διεύθυνση του καλούμενου στον καλών με ένα μήνυμα ACF.

5. Ο χρήστης S είναι πλέον σε θέση να καλέσει τον D στέλνοντάς του ένα μήνυμα SETUP, από το οποίο μαθαίνει τη διεύθυνση IP του αποστολέα (καλών). Η τερματική συσκευή του D πριν ενημερώσει τον χρήστη για την εισερχόμενη κλήση πρέπει να πάρει έγκριση από τον Gatekeeper D. Αυτό γίνεται στέλνοντας ένα μήνυμα ARQ.

6. Εάν ο Gatekeeper κρίνει ότι η κλήση μπορεί να γίνει δεκτή τότε θα στείλει ένα μήνυμα ACF.

7. Τέλος, όταν η συσκευή του χρήστη αρχίσει να καλεί τότε θα στείλει ένα μήνυμα CONNECT. Αφού η κλήση γίνει δεκτή, οι δυο τερματικές συσκευές μπορούν στη συνέχεια να διαπραγματευτούν τα χαρακτηριστικά της κλήσης (π.χ. codec) με το πρωτόκολλο H.245. Συμπερασματικά, λοιπόν, το πρωτόκολλο H.225.0 είναι το πρωτόκολλο εγκατάστασης κλήσεων μεταξύ των τερματικών συσκευών, ενώ το RAS χρησιμοποιείται για:

- Καταχώρηση στο Gatekeeper του αναγνωριστικού ενός χρήστη με μία δικτυακή διεύθυνση, δηλαδή είναι το αντίστοιχο μήνυμα REGISTER στο SIP.
- Αίτηση ενός χρήστη στο Gatekeeper για έναρξη εισερχόμενης κλήσης ή αποδοχή εισερχόμενης κλήσης. Στο SIP δεν υπάρχει αντίστοιχο μήνυμα καθώς ο Proxy θα πάρει τις αντίστοιχες αποφάσεις λαμβάνοντας ένα μήνυμα INVITE. Η εύρεση της φυσικής διεύθυνσης του προορισμού μπορεί να γίνει ρωτώντας και τον τοπικό Border, ο οποίος διατηρεί πίνακα δρομολόγησης με πληροφορίες που έχει συλλέξει από άλλους Border. Οι Bonier βοηθούν στη συνεργασία των παροχών καθώς συμμετέχουν στην ανταλλαγή πληροφοριών δρομολόγησης με το πρωτόκολλο H.501.

Εικόνα 11- Η διαχείριση κλήσεων με Η.323

• Ενημέρωση του Gatekeeper για την κατάσταση μιας κλήσης, για παράδειγμα ότι η κλήση τελείωσε. Ούτε αυτός ο τύπος μηνύματος υπάρχει στο SIP καθώς οι Proxies λαμβάνουν όλα τα μηνύματα σηματοδοσίας.

• Ενημέρωση του Gatekeeper για την κατάσταση ενός Gateway (διαθέσιμα κυκλώματα όταν πλησιάζει στο μέγιστο της χωρητικότητάς του). Ούτε αυτό το μήνυμα υπάρχει στο SIP καθώς για αυτό το λόγο χρησιμοποιείται το TGREP.

Πρωτόκολλο IAX (Inter-Asterisk eXchange)

Το πρωτόκολλο IAX αναπτύχθηκε προκειμένου χρήστες διαφορετικών PBX Asterisk να μπορούν να επικοινωνήσουν μεταξύ τους. Αυτά τα συστήματα PBX βασίζονται σε λογισμικό διαθέσιμου κώδικα open source που μπορεί να εκτελεστεί σε έναν υπολογιστή ή σε έναν αφοσιωμένο εξυπηρετητή. Στη συνέχεια προστέθηκε στο Asterisk υποστήριξη για SIP και Η.323, σε συνδυασμό μεταξύ τους.

Το IAX είναι ειδικά σχεδιασμένο ώστε να ανταποκρίνεται στις ιδιαιτερότητες του VoIP και όχι γενικά για πολυμεσικές εφαρμογές, όπως το SIP και το Η.323. Για παράδειγμα, τα μηνύματα ή εντολές είναι δυαδικά κωδικοποιημένα (όπως και στο Η.323) και επομένως κάθε

πακέτο έχει κεφαλίδες μικρότερου μεγέθους, επιτρέποντας αποδοτικότερη χρήση του διαθέσιμου εύρους ζώνης. Επιπλέον, το πρωτόκολλο αυτό εκτελείται κατά κύριο λόγο στους εξυπηρετητές και όχι στις συσκευές.

Ωστόσο, ο εξυπηρετητής ανήκει στον οργανισμό και όχι σε κάποιον πάροχο. Επομένως, είναι εφικτός ο καθορισμός της επιθυμητής πολιτικής δρομολόγησης κλήσεων. Η πολιτική αυτή ορίζεται ως μία σειρά κανόνων (dialplan), που ξεκινά από τη γενικότερη περίπτωση και καταλήγει στην ειδικότερη. Αξίζει να σημειωθεί ότι μεγαλύτερη προτεραιότητα έχουν οι ειδικότερες περιπτώσεις επειδή λειτουργούν σαν εξαιρέσεις. Για διευκόλυνση επιτρέπεται η ομαδοποίηση κανόνων σε context (Ormazabal et al, 2008).

Ένα context χαρακτηρίζεται από ένα μοναδικό όνομα και περιγράφει τους προορισμούς στους οποίους επιτρέπεται να γίνουν κλήσεις, καθώς και πληροφορίες δρομολόγησης (π.χ. ποια είναι η διεύθυνση IP του επόμενου εξυπηρετητή). Επίσης, εκεί περιγράφεται πότε επιτρέπεται να ενεργοποιηθεί ένα context, για παράδειγμα από ποιους εξυπηρετητές θα γίνουν δεκτές εισερχόμενες κλήσεις για τους προορισμούς ενός context. Οι τερματικές συσκευές μπορούν να επικοινωνούν με έναν εξυπηρετητή Asterisk χρησιμοποιώντας είτε το IAX είτε τα SIP και H.323. Εάν υποθέσουμε ότι οι τερματικές συσκευές χρησιμοποιούν το IAX, τότε αρχικά καταχωρούν τα στοιχεία τους στον εξυπηρετητή στέλνοντας ένα μήνυμα REGREQ. Ο εξυπηρετητής θα απαντήσει θετικά ή αρνητικά ανάλογα με τη νομιμότητα του χρήστη.

Όταν ένας χρήστης ξεκινήσει μία κλήση, τότε η συσκευή του στέλνει ένα μήνυμα NEW στο οποίο περιλαμβάνεται το αναγνωριστικό του καλούμενου. Ο εξυπηρετητής το λαμβάνει και το προωθεί στον πλέον κατάλληλο εξυπηρετητή. Αν αυτός είναι ένας Asterisk και δεχτεί την κλήση, τότε θα απαντήσει με ένα μήνυμα ACCEPT. Ο Asterisk του καλούμενου θα το προωθήσει στον καλών και ταυτόχρονα θα επιβεβαιώσει τη λήψη του μηνύματος αυτού με ένα μήνυμα ACK. Όταν η κλήση πραγματοποιηθεί (δηλαδή ο καλούμενος σηκώσει το ακουστικό του) τότε τα δεδομένα φωνής θα εξακολουθήσουν να διέρχονται από τον εξυπηρετητή. Μάλιστα, αυτά θα χρησιμοποιούν το ίδιο πρωτόκολλο (UDP) και θύρα (port). Αυτό συμβαίνει γιατί το IAX συνδυάζει έλεγχο κλήσεων και μετάδοση δεδομένων φωνής με το ίδιο πρωτόκολλο (Geneiatakis et al, 2005).

ΚΕΦΑΛΑΙΟ 3- Ασφάλεια VoIP

Η τεχνολογία της μετάδοσης φωνής πάνω από το πρωτόκολλο του διαδικτύου (Voice Over IP), επεκτείνεται συνεχώς και κερδίζει όλο και μεγαλύτερα μερίδια αγοράς από την παραδοσιακή τηλεφωνία (Myers, 2012). Οι μεγαλύτεροι κατασκευαστές παραδοσιακών προϊόντων αναλογικής και ψηφιακής τηλεφωνίας σχεδιάζουν και εισάγουν στην αγορά νέα προϊόντα βασισμένα στην τεχνολογία της μετάδοσης φωνής πάνω από το πρωτόκολλο του διαδικτύου. Στο επίπεδο εφαρμογής (application layer) του διαδικτυακού πρωτόκολλου για τη μετάδοση φωνής υπάρχουν σήμερα δύο δημοφιλείς υλοποιήσεις. Το πρωτόκολλο εγκαθίδρυσης συνεδρίας (SIP) και το πρωτόκολλο H.323 που αποτελείται με τη σειρά του από ένα σύνολο από επί μέρους πρωτόκολλα. Το πρώτο (SIP) από αυτά έχει αναπτυχθεί ύστερα από προσπάθειες της κοινότητας του διαδικτύου και περιγράφεται από ένα σύνολο από απαιτήσεις για σχόλια (Request For Comment). Από την άλλη πλευρά το H.323 έχει αναπτυχθεί και προταθεί από τους κύριους κατασκευαστές προϊόντων τηλεφωνίας και σήμερα αποτελεί πρότυπο της ένωσής τους, της διεθνής ένωσης τηλεπικοινωνιών (ITU).

Με την έλευση της τεχνολογίας VoIP έκαναν την εμφάνισή τους και οι πρώτες απειλές εναντίον της ασφαλής λειτουργίας του. Μπορούμε να αναφέρουμε ενδεικτικά τις πιο σημαντικές από αυτές. Καταγραφή της τηλεφωνικής κλήσης τόσο των δεδομένων της, όσο και του περιεχομένου της, τηλεφωνική κλήση εμφανίζοντας ψεύτικα στοιχεία, πραγματοποίηση ατελών κλήσεων, κλήση εμφανίζοντας παραποιημένο αριθμό καλούμενου, μεταφορά κλήσης σε τρίτο προορισμό και ενοχλητικά διαφημιστικά μηνύματα μέσω τηλεφωνίας (Dwivedi, 2009).

3.1. Απειλές VoIP

Το VoIP είναι μια επεκτεινόμενη τεχνολογία. Εντούτοις, εντοπίστηκαν ορισμένα σημεία ευπάθειας για αυτό (Keromytis, 2010). Φαίνεται ότι υφιστάμενοι και παραδοσιακοί έλεγχοι ασφαλείας και λύσεις όπως τείχη προστασίας και IPSec δεν μπορούν να αντιμετωπίσουν

πλήρως τις απειλές αυτές, καθώς τα VoIP λειτουργούν σε ετερογενή περιβάλλοντα (Walsh & Kuhn, 2005). Οι κοινές απειλές για την ασφάλεια VoIP περιλαμβάνουν (Dwivedi, 2009):

- VoIP sniffing
- VoIP Phishing
- Δημιουργία ελεύθερων βαλβίδων
- Spoofing αναγνώρισης καλούντος
- Ανώνυμη υποκλοπή κλήσεων και ανακατεύθυνση κλήσεων
- Spam μέσω τηλεφωνίας μέσω Internet (Gritzalis et al, 2013)

3.2. Πλαίσιο καταγραφής δικτύου

Το πλαίσιο αυτό επικεντρώνεται σε αντικείμενα που μπορούν να συλλεχθούν σε μια υπηρεσία VoIP και ειδικά στις κεφαλίδες SIP και στο μήνυμα του σώματος SIP όπου βρίσκονται τα δεδομένα SDP. Το SDP χρησιμοποιείται για τη μετάδοση λεπτομερειών πολυμέσων, διευθύνσεων μεταφοράς και άλλων δεδομένων περιγραφής περιόδων στους συμμετέχοντες κατά τη διάρκεια μιας κλήσης στο Internet.

Το SDP περιέχει πληροφορίες στις κεφαλίδες του που έχουν ιδιαίτερη εγκληματολογική αξία, καθώς περιλαμβάνουν την ιδιωτική διεύθυνση IP του User Agent. Η ιδιωτική διεύθυνση IP θα πρέπει να χρησιμοποιείται από ενδιάμεσες συσκευές μεταξύ του διακομιστή SIP και του πράκτορα χρήστη, όπως τείχη προστασίας ή δρομολογητές, προκειμένου να δημιουργηθεί και να διατηρηθεί δυναμικά η αμφίδρομη επικοινωνία. Όταν οι ενδιάμεσες συσκευές δεν επεξεργάζονται αυτές τις κεφαλίδες (είτε είναι ανίκανες είτε δεν έχουν ρυθμιστεί ανάλογα), η ιδιωτική διεύθυνση IP μπορεί να φτάσει στον απομακρυσμένο διακομιστή SIP, διαρρέοντας έτσι πληροφορίες μιας ιδιωτικής τοπολογίας δικτύου. Εκτός από τις ιδιωτικές διευθύνσεις IP, μπορούν να συλλεχθούν και άλλα χρήσιμα αντικείμενα από αυτές τις κεφαλίδες, τα

περισσότερα από τα οποία δεν καταγράφονται από τους διακομιστές SIP, όπως επιβεβαιώθηκε κατά την εμπειρική αξιολόγηση αυτής της εργασίας.

3.3. Η χρήση του VoIP στον τομέα της εγκληματολογίας

Η χρήση VoIP forensics είναι ένας σχετικά νέος τομέας έρευνας στον τομέα της εγκληματολογίας δικτύων. Οι ερευνητές, οι αρχές επιβολής του νόμου και οι ψηφιακοί ερευνητές πρότειναν μεθόδους και ανέπτυξαν τεχνικές σε μια προσπάθεια να συλλέξουν και να χειριστούν τα ψηφιακά στοιχεία που αφορούν δραστηριότητες VoIP. Οι Simon και Slay (2006) προτείνουν το λεγόμενο μοντέλο 4Ps, το οποίο περιλαμβάνει την Πρόληψη (firewalls, IDS / IPS κλπ), Προστασία (κρυπτογράφηση, διαχείριση ασφάλειας κ.λπ.), Διατήρηση (αρχεία, αρχεία και ανάλυση) και Παρουσίαση (Μηχανισμοί διαχείρισης και επιδιόρθωσης ευπάθειας).

Ο Lin και ο Yen (2011) επέκτειναν περαιτέρω το μοντέλο 4Ps και το έχουν προσαρμόσει ώστε να ικανοποιούν τις ανάγκες VoIP σε μια λεπτομερή διαδικασία εγκληματολογίας που ονομάζεται VoIP DEFSOP. Το στάδιο Διατήρησης έχει πλέον χαρτογραφηθεί στην Επιχειρησιακή Σκηνή και επεκτείνεται περαιτέρω στα στάδια Συλλογή, Ανάλυση και Ιατροδικαστική. Ένας τεχνικός περιορισμός αυτού του μοντέλου είναι ότι όταν εφαρμόζεται, απαιτεί την ανάπτυξη πρακτόρων σε όλους τους συμμετέχοντες κόμβους (και οι δύο πελάτες και ο εξυπηρετητής) για τη συλλογή των δεδομένων, τα οποία σε ορισμένες περιπτώσεις μπορεί να μην είναι πρακτικά εφικτά, με τους διακομιστές και, επιπλέον, ενδέχεται να υπάρχουν ιδιόκτητες ή ενσωματωμένες συσκευές (όπως τηλέφωνα SIP υλικού) χωρίς δυνατότητα εγκατάστασης πρόσθετου λογισμικού.

Οι Yen, Lin και Wu (2011) παρουσιάζουν μια μελέτη περίπτωσης που βασίζεται σε VoIP DEFSOP παρόμοιες με τις παραπάνω, η συλλογή δεδομένων απαιτεί την τοπική απόκτηση και ειδικές απαιτήσεις που πρέπει να πληρούνται, όπως η προηγούμενη εγκατάσταση συγκεκριμένου λογισμικού τόσο στον εξυπηρετητή όσο και στους πελάτες.

Οι Hsu, Sun, and Chen (2011) περιγράφουν ένα συνεργατικό σχέδιο για την ανίχνευση VoIP. Η ανίχνευση VoIP είναι μια δύσκολη εργασία, διότι τα αντικείμενα διανέμονται γεωγραφικά σε διαφορετικά μέρη μεταξύ διαφόρων μέσων, εξυπηρετητών και εξοπλισμού δικτύου, τα οποία διαχειρίζονται διάφοροι διαχειριστές ή ακόμα χειρότερα από διαφορετικούς οργανισμούς. Ως εκ τούτου, σε ένα σενάριο όπου ένας χρήστης κατοικεί σε ένα ιδιωτικό δίκτυο, θα πρέπει να ζητηθεί από τον απομακρυσμένο χειριστή δικτύου η ιδιωτική διεύθυνση IP. Στο προτεινόμενο έργο αποδεικνύεται ότι αυτές οι πληροφορίες μπορούν να ληφθούν με την εξόρυξη των επικεφαλίδων SDP που μπορούν να συλλεχθούν τοπικά, χωρίς να χρειάζεται η συνεργασία του χειριστή δικτύου, εξοικονομώντας έτσι διοικητικά έξοδα.

Οι Irwin και ο Slay (2011) ανέπτυξαν μια εφαρμογή που αναζητά αντικείμενα VoIP στην πτητική μνήμη του υπολογιστή. Έδειξαν ότι οι συνομιλίες του πρωτόκολλου μεταφοράς πραγματικού χρόνου (RTP) μπορούν να ανακατασκευαστούν με σημαντική πιθανότητα επιτυχίας από τα δεδομένα που διαμένουν στη μνήμη RAM. Αυτή η προσέγγιση μπορεί να αυξήσει σημαντικά και να συμπληρώσει τη μέθοδο που προτείνουμε. Οι Psaroudakis et al (2014) απέδειξαν ότι στην περίπτωση ενός πελάτη VoIP smartphone, η επικεφαλίδα User Agent μπορεί να οδηγήσει στην πλήρη αποκάλυψη της μάρκας, του μοντέλου και του λειτουργικού συστήματος ενός smartphone. Αυτό έχει επίσης επαληθευτεί στην παρούσα εργασία για ορισμένους νόμιμους χρήστες.

Οι Frangois, State, Engel και Festor (2010) πρότειναν μια μέθοδο για λήψη δακτυλικών αποτυπωμάτων από το SIP User Agent. Αυτή η μέθοδος θα μπορούσε να συμβάλει σε μια προσπάθεια να ανακαλυφθούν οι επικεφαλίδες χρηστών του SIP User Agents από κακόβουλους χρήστες.

Η τεχνολογία VoIP βασίζεται στο προηγουμένως απειλητικό δίκτυο IP και προσθέτει επίσης τηλεφωνικές απειλές. Καθώς η τεχνολογία VoIP εξελίσσεται, συλλέγει τις ευπάθειες και τις απειλές τόσο των τεχνολογιών Internet όσο και των τηλεπικοινωνιών. Παρόλο που έχουν υπάρξει πολλά άρθρα σχετικά με θέματα ασφάλειας, οι οργανώσεις εξακολουθούν να στερούνται οποιασδήποτε εφαρμογής των μέτρων υποδομής ασφάλειας για VoIP. Σύμφωνα

με το (Schwartau, 2005) ο κόσμος της επικοινωνίας που κινείται προς την τεχνολογία VoIP δε διαθέτει εμπειρία στον τομέα της ασφάλειας. Ο λόγος είναι ότι ένα μικρό ποσό του προϋπολογισμού διατίθεται για την ασφάλεια.

Η έννοια της ασφάλειας που σχετίζεται με το VoIP έχει πολλές διαφορετικές πτυχές, αλλά υπάρχουν τρία κύρια βασικά στοιχεία: Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα (CIA) (Pfleeger και Pfleeger, 2002).

- ✓ **Εμπιστευτικότητα**

Η εμπιστευτικότητα αναφέρεται στους μηχανισμούς που εξασφαλίζουν ότι μόνο ο προοριζόμενος παραλήπτης έχει πρόσβαση στην κλήση VoIP. Οι επιθέσεις "man in the middle" θεωρούνται παραβιάσεις εμπιστευτικότητας, συμπεριλαμβανομένης της υποκλοπής, εισπνοής και επιθέσεων εφαρμογής. Πολλά δωρεάν εργαλεία όπως το dsniff, το tcpdump είναι διαθέσιμα (Porter, 2006). Η προσθήκη κεφαλίδων πακέτων μπορεί να οδηγήσει σε αποκάλυψη δικτύων και υποδομών, ενώ η παρεμπόδιση των πακέτων οδηγεί σε διαρροή ιδιωτικών δεδομένων. Η παρακολούθηση ARP, η κρυπτογράφηση, το VPN είναι μερικές τεχνικές για την άμβλυνση τέτοιων επιθέσεων.

- ✓ **Ακεραιότητα**

Η ακεραιότητα αναφέρεται στην πρόληψη οποιασδήποτε μη εξουσιοδοτημένης τροποποίησης των πακέτων φωνής. Οι παραβιάσεις των κωδικών πρόσβασης είναι συνηθισμένες όταν ένας διακόπτης επανενεργοποιεί και εκκινεί με τις προεπιλεγμένες ρυθμίσεις (Kuhn et.al, 2005). Περισσότερες επιθέσεις περιλαμβάνουν την spoofing IP, την υποβάθμιση της ποιότητας, την απόπειρα καταχώρησης / συνόδου και την προσθήκη server (Ransom and Rittinghouse, 2005). Τα πακέτα πρέπει να αποκλείονται με χρήση VLAN (κατάτμηση), επαλήθευση ταυτότητας καλούντος και σταθερών μηχανισμών δρομολόγησης (Green, 2002).

- ✓ **Διαθεσιμότητα**

Η διαθεσιμότητα αναφέρεται στις υπηρεσίες VoIP, οι οποίες είναι πάντα διαθέσιμες όταν χρειάζεται. Η άρνηση παροχής υπηρεσιών, η οποία αποτελεί απειλή για τη διαθεσιμότητα, θα μπορούσε να έχει αρνητικές επιπτώσεις εάν το δίκτυο τηλεφωνικών κέντρων VoIP έχει πληγεί από τέτοια επίθεση. Άλλες επιθέσεις περιλαμβάνουν το TCP SYN, το SIP INVITE flood (Goode B, 2002) και το Spam μέσω τηλεφωνίας μέσω Internet (SPIT). Οι απαιτούμενες ενέργειες χρησιμοποιούν πλήρεις τείχη προστασίας από το κράτος, ανίχνευση εισβολών και φίλτρα ανεπιθύμητης αλληλογραφίας σε διακομιστές (Eyeball, 2006)

- ✓ **Απειλές και ευπάθειες**

Υπάρχει ένας αριθμός κινδύνων που συνδέονται με το δίκτυο VoIP. Οι διάφορες απειλές και τρωτά σημεία ταξινομούνται σε διάφορες κατηγορίες επίθεσης. Η τεχνολογία πρέπει να παρέχει ασφάλεια, καθώς τα πακέτα λαμβάνουν μια απροσδιόριστη διαδρομή ενώ διασχίζουν από την πηγή μέχρι το προορισμό. Η ανάλυση των τρωτών σημείων και των απειλών κατά την εφαρμογή των μέτρων ασφαλείας είναι γνωστή ως «Αναγνώριση κινδύνου».

3.4. Είδη Επιθέσεων

3.4.1. Επιθέσεις κατάθεσης

Αυτές είναι οι επιθέσεις στις οποίες ο επιτιθέμενος προσπαθεί να εισέλθει στο σύστημα ή θα μπορούσε να οριστεί ως εκείνες στις οποίες ένας εισβολέας εκμεταλλεύεται τις ευπάθειες στην εγγραφή εισάγοντας τον εαυτό του στη διαδρομή σήματος του δικτύου VoIP. Διάφοροι τύποι επιθέσεων εγγραφής περιλαμβάνουν το IP Spoofing, την κλοπή υπηρεσίας, την αντανακλαστική επίθεση, την Brute Force Attack.

3.4.2. Επιθέσεις κατά τη διάρκεια της πραγματοποίησης κλήσεων

Οι επιθέσεις αυτές πραγματοποιούνται κυρίως όταν ένα άτομο λαμβάνει μια κλήση. Ο εισβολέας παρακολουθεί τη διαδρομή όπου αποστέλλονται τα πακέτα φωνής / δεδομένων.

Καλέστε την αεροπειρατεία, την υποκλοπή, την πλαστογράφηση ARP (Porter, 2006), την πειρατεία σύνδεσης, το πρωτόκολλο σημάτων.

3.4.3. Επιθέσεις άρνησης παροχής υπηρεσιών

Αυτές οι επιθέσεις δεν έχουν καμία ανησυχία για την απόκτηση οποιωνδήποτε πολύτιμων πληροφοριών. Αυτό απλά απομονώνει το τελικό σημείο του δικτύου από τον υπόλοιπο κόσμο, παρεμποδίζοντας τους διακόπτες και το IP PBX με φορτία αιτημάτων rouge. Οι διάφορες κατηγορίες περιλαμβάνουν το SIP INVITE Flood, το TCP SYN Flood και τα κακόβουλα ρεύματα RTP (Reynolds and Ghosal, 2002).

3.4.4. Επιθέσεις σε στοιχεία VoIP

Αυτές οι επιθέσεις είναι κυρίως στις συσκευές, καθώς φαίνεται να επηρεάζονται εύκολα. Οι πιο κοινές επιθέσεις αφορούν το IP PBX και τα τηλέφωνα IP. Επιπλέον επιθέσεις περιλαμβάνουν επιθέσεις εφαρμογής και επιθέσεις SPIT.

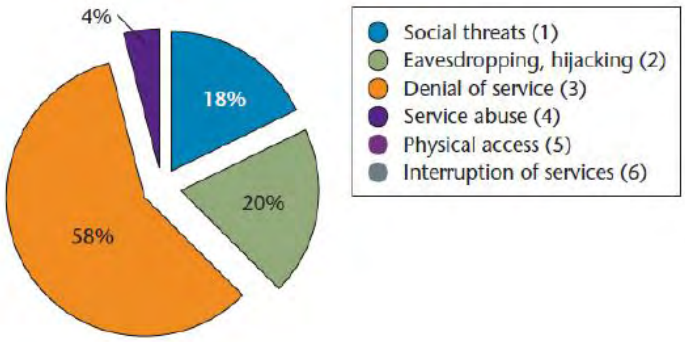
«On-Net» και «Off-Net»

Οι όροι “On-Net” και “Off-Net” χρησιμοποιούνται για την περιγραφή των τύπων κλήσεων ή μηνυμάτων. Το “On-Net” χρησιμοποιείται όταν η κλήση ή το μήνυμά σας προέρχεται από το δίκτυο του τοπικού σας φορέα και τερματίζεται σε έναν άλλο κινητό αριθμό που βρίσκεται στον φορέα εκμετάλλευσης. Δεν έχει σημασία αν το πρόσωπο που καλείτε χρησιμοποιεί το οικιακό δίκτυο ή χρησιμοποιεί περιαγωγή με διαφορετικό παροχέα. Το "Off-Net" ισχύει όταν η κλήση ή το μήνυμα γίνεται σε διαφορετικό δίκτυο, π.χ. ενώ βρίσκεστε σε περιαγωγή ή χρησιμοποιείτε το οικιακό σας δίκτυο και πραγματοποιείτε μια κλήση ή στέλνετε ένα μήνυμα σε έναν αριθμό που ανήκει σε διαφορετικό παροχέα δικτύου (Keromytis, 2009).

3.5. Ευπάθειες του VOIP

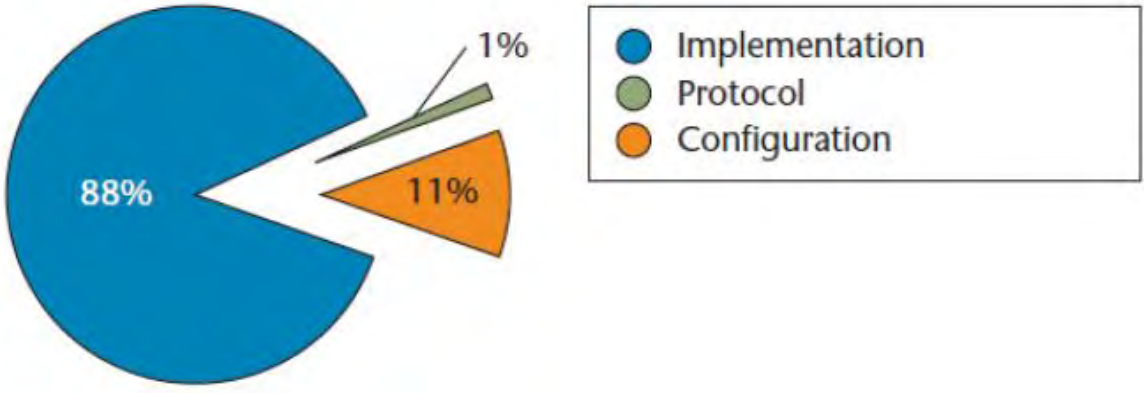
Στα πλαίσια του vampire project (http://vampire.gforge.inria.fr) χρηματοδοτούμενο από το Γαλλικό Εθνικό Γραφείο Έρευνας (ANR) και για την καλύτερη κατανόηση της ευρύτερης ασφάλειας του VoIP, πραγματοποιήθηκε μια έρευνα που περιλάμβανε 221 επιθέσεις που έλαβαν χώρα από το 1999 έως το Νοέμβριο του 2009. Αυτά τα προβλήματα ασφάλειας περιλαμβάνουν επιθέσεις σχετικά απλές όπως denial of service (DoS) ως και σοβαρότερες όπως υποκλοπή (eavesdrop) στις τηλεπικοινωνίες, απομακρυσμένη διαχείριση εξυπηρετητών ή ακουστικών, αποφυγή πληρωμών ή χρέωση άλλου χρήστη (toll fraud).

Στην εικόνα 12 απεικονίζονται οι ευπάθειες ανά τύπο, χρησιμοποιώντας την ταξινόμηση του VoIP Security Alliance (VoIPSA). Παρατηρείται ότι τα περισσότερα προβλήματα αφορούν επιθέσεις DoS, συνήθως μέσω του εξυπηρετητή ή του εξοπλισμού του χρήστη. Στο σημείο αυτό πρέπει να σημειωθεί ότι και οι λιγότερο προφανείς επιθέσεις DoS, τις οποίες οι χρήστες και οι διαχειριστές δεν αντιλήφθησαν αμέσως, έχουν επίσης καταγραφεί. Θα πρέπει να αναφέρουμε ότι στην κατάταξη των απειλών δεν υπολογίζεται σωστά ο πιθανός αριθμός των σοβαρότερων επιθέσεων, γιατί σε πολλές από τις περιπτώσεις όπου έχει καταγραφεί επίθεση DoS, οι επιτιθέμενοι θα μπορούσαν επίσης να έχουν προβεί σε επίθεση buffer overflow, αλλά δεν ακολουθήθηκε κάποια λεπτομερής ανάλυση. Αυτό το οποίο η εικόνα 12 δεν απεικονίζει σωστά, είναι ότι οι VoIP εξυπηρετητές και πελάτες, αντιπροσωπεύουν περίπου το μισό των επιθέσεων DoS (Dwivedi, 2009).



Εικόνα 12 Ευπάθειες του voip

Στην εικόνα 13 φαίνεται από πού πηγάζουν οι επιθέσεις αυτές. Δεδομένης της φύσης του δείγματος, δεν είναι πολύ περίεργο το γεγονός ότι οι περισσότερες από τις απειλές πηγάζουν από προβλήματα εφαρμογής.



Εικόνα 13- Πηγές και αιτίες των ευαίσθητων σημείων

3.6. Κοινωνικές απειλές

SPIT

Το Voice Spam ή Spam over Internet Telephony (SPIT) είναι ένα πρόβλημα παρόμοιο με το Spam το οποίο θα επηρεάσει στο μέλλον το VoIP. Με το SPIT αναφερόμαστε στις μαζικές και ακούσιες κλήσεις που παράγονται αυτόματα. Οι κλασικές τηλεφωνικές πωλήσεις δεν θεωρούνται SPIT (Sisalem et al, 2008).

Στις κλασικές τηλεπωλήσεις, χρησιμοποιούνται auto-dialers, οι οποίοι καλούν νούμερα μέχρι να σηκώσει το τηλέφωνο κάποιος. Τότε μεταφέρεται η γραμμή σε έναν εκπρόσωπο της εταιρίας ο οποίος ξεκινά την προσπάθειά του για να κάνει την πώληση. Αυτοί οι auto-dialers μπορούν και ξεχωρίζουν την φωνή κάποιου που απαντά στην κλήση από τη φωνή που ακούγεται στο μήνυμα του αυτόματου τηλεφωνητή. Το SPIT είναι σαν τις τηλεπωλήσεις αλλά με αρκετά μεγαλύτερη συχνότητα και μπορεί να συγκριθεί με τη συχνότητα του SPAM. Οι τηλεπωλήσεις είναι ενοχλητικές, αλλά η συχνότητα των τηλεφωνημάτων συγκρινόμενη με το SPAM είναι πολύ μικρή.

Ένας άλλος τομέας που το SPIT υπερτερεί από τις τηλεπωλήσεις είναι το θέμα του κόστους. Για να στηθεί ένα απλό τηλεφωνικό κέντρο, όπου θα μπορεί να καλέσει ταυτόχρονα 100 πιθανούς πελάτες και να έχει 10 τηλεφωνικές συσκευές σε περίπτωση που απαντήσει κάποιος το τηλεφώνημα θα χρειαστεί ένα ανάλογο PBX.

Η Man-in-the-middle επίθεση πραγματοποιεί μια τριπλή επικοινωνία μεταξύ των δύο συμβαλλόμενων μερών και του επιτιθεμένου ανάμεσα τους. Καθ' όλη την διάρκεια της συνόδου της επικοινωνίας, τα δύο συμβαλλόμενα μέρη δεν παρατηρούν τη συμμετοχή του επιτιθεμένου. Ο επιτιθέμενος πετυχαίνει τη δρομολόγηση της κυκλοφορίας μεταξύ των δύο συμβαλλόμενων μερών μέσω αυτού. Οι πληροφορίες που στέλνονται πέρα δώθε παρεμποδίζονται, τροποποιούνται ή και διαβάζονται. Ένα τυπικό παράδειγμα αυτής της επίθεσης είναι η εναλλακτική Diffie Helman Key φάση ανταλλαγής σε μια TLS handshake διαδικασία οργάνωσης κλήσης. Αυτή η διαδικασία είναι τρωτή σε αυτήν την επίθεση

καθιστώντας ενδεικνυόμενη τη χρησιμοποίηση της δημόσιας κρυπτογράφησης κλειδιών όπως η RSA έναντι της ανταλλαγής κλειδιών. Η RSA παρέχει αρκετές βάσεις για τη μείωση της επίθεσης (Zhang et al, 2010).

Man-In-The-middle επίθεση

Η Man-in-the-middle επίθεση πραγματοποιεί μια τριπλή επικοινωνία μεταξύ των δύο συμβαλλόμενων μερών και του επιτιθέμενου ανάμεσά τους. Καθ' όλη τη διάρκεια της συνόδου της επικοινωνίας, τα δύο συμβαλλόμενα μέρη δεν παρατηρούν τη συμμετοχή του επιτιθεμένου. Ο επιτιθέμενος πετυχαίνει τη δρομολόγηση της κυκλοφορίας μεταξύ των δύο συμβαλλόμενων μερών μέσω αυτού. Οι πληροφορίες που στέλνονται πέρα δώθε παρεμποδίζονται, τροποποιούνται ή και διαβάζονται. Ένα τυπικό παράδειγμα αυτής της επίθεσης είναι η εναλλακτική Diffie Helman Key φάση ανταλλαγής σε μια TLS handshake διαδικασία οργάνωσης κλήσης. Αυτή η διαδικασία είναι τρωτή σε αυτήν την επίθεση καθιστώντας ενδεικνυόμενη τη χρησιμοποίηση της δημόσιας κρυπτογράφησης κλειδιών όπως η RSA έναντι της ανταλλαγής κλειδιών. Η RSA παρέχει αρκετές βάσεις για τη μείωση της επίθεσης (Zhang et al, 2010).

3.7. Θέματα Κινήτρων στην Αγορά του VoIP

Στο κεφάλαιο αυτό θα εξετάσουμε τα κίνητρα των παρόχων VoIP σχετικά με τις συμφωνίες συνεργασίας, τη σηματοδοσία μιας συνόδου αλλά και το μονοπάτι που θα ακολουθήσουν τα δεδομένα. Προκειμένου να συμπεριλάβουμε όλους τους πιθανούς παρόχους θα μελετήσουμε την ακραία περίπτωση που τόσο η αφετηρία όσο και ο προορισμός μιας κλήσης είναι σε κατάσταση περιαγωγής και ενδέχεται να μεσολαβούν και άλλοι ενδιάμεσοι πάροχοι. Στην ανάλυσή μας θα υποθέσουμε ότι το SIP χρησιμοποιείται ως πρωτόκολλο σηματοδοσίας.

3.7.1. Συμφωνίες Συνεργασίας

Εάν ο πάροχος του καλούντος έχει στη διάθεσή του ένα αναγνωριστικό SIP για τον καλούμενο τότε έχει κίνητρο η κλήση να πραγματοποιηθεί εξ ολοκλήρου μέσω VoIP. Ο βασικός λόγος είναι ότι τέτοιες κλήσεις ενδέχεται να μη χρεώνονται από τον πάροχο του καλούμενου. Αυτό βασίζεται στην αρχική θεώρηση του VoIP ως μία εφαρμογή του Internet, όπως το E-mail, για την οποία δεν υπάρχει άμεση χρέωση μεταξύ των παρόχων. Από αυτό το πρίσμα, όλοι οι πάροχοι θεωρούνται ομότιμοι και εφαρμόζουν την τακτική 'bill and keep', με την οποία κάθε πάροχος εισπράττει έσοδα από υπηρεσίες που προσφέρει χωρίς να τα μοιράζεται με τους υπόλοιπους παρόχους που συμμετέχουν σε αυτές. Αυτή η μορφή συνεργασίας έχει επικρατήσει με τον όρο VoIP Peering (Nassar et al, 2017).

Το VoIP Peering δεν ανταποκρίνεται, ωστόσο, πάντα στην πραγματικότητα καθώς τα τελευταία χρόνια αρκετοί πάροχοι ζητούν τέλη τερματισμού. Ουσιαστικά, οι πάροχοι αυτοί προσπαθούν να επιβάλουν την πολιτική χρέωσης ώστε να χρεώνουν τον τερματισμό κλήσεων. Σύμφωνα με αυτή την πολιτική, ένας πάροχος πληρώνει τον επόμενο στην αλυσίδα αξίας κρατώντας ένα μέρος από αυτά που εισέπραξε ο ίδιος από τον προηγούμενό του. Παρατηρούμε, δηλαδή, ότι υπάρχει μία τάση σύγκλισης ανάμεσα στην 'παραδοσιακή' αγορά τηλεφωνίας και σε αυτή του VoIP στον τρόπο χρέωσης. Αυτό σημαίνει όμως ότι υπάρχει πιθανότητα ο πάροχος του καλούμενου να μη δεχτεί να προωθήσει μία εισερχόμενη κλήση VoIP αν δεν πληρωθεί.

Ας δούμε με λίγο περισσότερη λεπτομέρεια γιατί συμβαίνει αυτό. Οι ITSPs που προσφέρουν υπηρεσίες τηλεφωνίας (σχεδόν) ισοδύναμες με αυτές των παραδοσιακών, όπως για παράδειγμα η Vonage στην Αμερική, εκχωρούν στους πελάτες τους δύο ειδών αναγνωριστικά· έναν αριθμό E.164 και μία διεύθυνση SIP. Η υποστήριξη εισερχόμενων κλήσεων στους αριθμούς E.161 απαιτεί την επένδυση σε μεταγωγείς και Gateways, τα οποία αυξάνουν το κόστος λειτουργίας του παρόχου. Επομένως, ο ITSP έχει κίνητρο να χρεώνει τον τερματισμό των εισερχόμενων κλήσεων προς τον αριθμό E.1G1 με τιμή αντίστοιχη αυτής των παραδοσιακών παρόχων. Αν τα αναμενόμενα έσοδα από τις εισερχόμενες κλήσεις στους

αριθμούς E.1G4 δεν καλύπτουν το κόστος της επένδυσης, τότε ο ITSP έχει κίνητρο να χρεώνει τις κλήσεις προς τη διεύθυνση SIP του χρήστη. Επομένως, ο ITSP θα δεχτεί κλήσεις VoIP μόνο από τους παρόχους με τους οποίους έχει προηγουμένως συμφωνήσει τους οικονομικούς όρους του συμβολαίου.

Η εφαρμογή αυτής της πολιτικής αποδοχής κλήσεων είναι και ο λόγος που πολλές κλήσεις μεταξύ παρόχων VoIP πραγματοποιούνται μέσω του PSTN. Σχετικά πρόσφατα αναπτύχθηκαν πάροχοι οι οποίοι διαθέτουν πολλές συνεργασίες για διαβίβαση κλήσεων VoIP και είναι γνωστοί ως Aggregators. Ένας ITSP μπορεί άμεσα να υποστηρίζει κλήσεις προς οποιοδήποτε παραδοσιακό τηλεφωνικό προορισμό έχοντας συμφωνία με ένα μόνο Aggregator. Διαφορετικά, θα έπρεπε να συνάψει πολλές συμφωνίες με ITSPs προκειμένου οι κλήσεις να μην περνούν από το PSTN, το οποίο συνεπάγεται σημαντικό διαχειριστικό κόστος. Ένα άλλο σημαντικό χαρακτηριστικό των Aggregators είναι το γεγονός ότι εφαρμόζουν εξελιγμένες πολιτικές δρομολόγησης προκειμένου να επιτυγχάνουν υψηλή ποιότητα υπηρεσίας. Για αυτό το λόγο, σε επόμενο κεφάλαιο θα εξετάσουμε βέλτιστες πολιτικές δρομολόγησης για Aggregators, αν και αυτό δεν περιορίζει καθόλου την εφαρμογή τους από ITSPs (Nassar et al, 2017).

Δύο ITSPs με παρόμοιο μέγεθος πελατειακής βάσης αναγνωρίζοντας ότι η μεσολάβηση των Aggregators αυξάνει το κόστος λειτουργίας τους, προβαίνουν στην σύναψη συμφωνιών ομότιμης συνεργασίας. Ένα επιπλέον πλεονέκτημα της τακτικής ’bill and keep’ είναι η απλότητα στην εφαρμογή της καθώς οι πάροχοι δε χρειάζεται να προβαίνουν σε μεταξύ τους πληρωμές, οι οποίες αν ειδωθούν αθροιστικά για μία μεγάλη περίοδο θα τείνουν να γίνουν μηδενικές. Παρατηρούμε δηλαδή, μία ομοιότητα στη συμπεριφορά των ITSPs με αυτήν των ISI’s.

Επομένως, ο πάροχος του καλούμενου δεν έχει κίνητρο να δεχτεί εισερχόμενες κλήσεις αν δεν αποζημιωθεί, είτε εισπράττοντας τέλη τερματισμού ή κερδίζοντας το δικαίωμα να πραγματοποιεί και ο ίδιος δωρεάν κλήσεις προς τους πελάτες των ομότιμων συνεργατών του. Αντίστοιχα, και οι υπόλοιποι πάροχοι που ενδεχομένως συμμετέχουν στην εγκατάσταση μιας συνόδου, π.χ. ο πάροχος περιαγωγής του καλούντος ή ο πάροχος περιαγωγής του

καλούμενου επιθυμούν να ανταμειφθούν για τη συνεισφορά τους.

Αξίζει να σημειωθεί ότι, αν ο πάροχος του καλούμενου δε δέχεται κλήσεις VoIP από κάποιον πάροχο, τότε ο τελευταίος έχει κίνητρο να τον παρακάμψει επιχειρώντας να φτάσει στον προορισμό εκμεταλλευόμενος γνώση για τη δικτυακή διεύθυνση του προορισμού από προηγούμενες κλήσεις. Ενδέχεται βέβαια αυτή η πληροφορία να μην είναι ακριβής και η κλήση να μην πραγματοποιηθεί. Σε αυτό συμβάλει και η χρήση ειδικού τύπου από SIP proxies, τους Session Border Controllers οι οποίοι θα περιγραφούν στη συνέχεια.

3.7.2. Έλεγχος Σηματοδοσίας

Όταν ένας χρήστης εγγράφεται στην υπηρεσία ενός μόνο παρόχου VoIP τότε ο πάροχος αυτός αποκτά το δικαίωμα να συμμετέχει στη διαδικασία εγκατάστασης των συνόδων. Αυτό οφείλεται στο γεγονός ότι μόνο ο συγκεκριμένος πάροχος θα γνωρίζει ανά πάσα στιγμή πώς θα εντοπίσει τον χρήστη προκειμένου να τον ενημερώσει για μία εισερχόμενη σύνοδο. Συγκεκριμένα, είναι αυτός που γνωρίζει την τρέχουσα διεύθυνση IP είτε της συσκευής του χρήστη ή του εξυπηρετητή που του προσφέρει υπηρεσίες όταν είναι σε κατάσταση περιαγωγής.

Εάν ο χρήστης εγγραφεί και σε άλλους παρόχους τότε παίζει ρόλο ποιο αναγνωριστικό χρήστη διαδίδει στο περιβάλλον του και τελικά θα χρησιμοποιήσει ο καλών. Ο πάροχος αυτού του αναγνωριστικού θα συμμετέχει στη διαδικασία εγκατάστασης της συνόδου. Υπάρχει μία εξαίρεση σε αυτήν την παρατήρηση· εάν κάποιος πάροχος αναζητήσει εναλλακτικά αναγνωριστικά του καλούμενου στο Δημόσιο ENUM και εκείνος είναι εγγεγραμμένος τότε ο πάροχος αυτός θα έχει δυνατότητα επιλογής. Βλέπουμε λοιπόν ότι το Δημόσιο ENUM έχει τη δυνατότητα να αντιμετωπίσει το φαινόμενο 'μονοπώλιο του τερματισμού' δίνοντας περισσότερο έλεγχο στους παρόχους έναρξης και διαβίβασης κλήσεων. Μάλιστα, αυτός ο αυξημένος έλεγχος ενδέχεται να φθίνει κατά την πορεία μίας κλήσης από την έναρξη προς τη διαβίβαση. Αυτό οφείλεται στον περιορισμό του Δημοσίου ENUM να έχει ως μοναδικό

κριτήριο αναζήτησης τους τηλεφωνικούς αριθμούς που ακολουθούν το πρότυπο Κ. 164.

Ας εξετάσουμε το σενάριο ενός ITSP που προωθεί σε ένα Aggregator όλες τις κλήσεις για προορισμούς που δεν είναι πελάτες του. Έστω μία τέτοια κλήση, όπου το αναγνωριστικό καλούμενου είναι ένας τηλεφωνικός αριθμός Ε.164 και ότι ο ITSP μαθαίνει για την ύπαρξη μιας διεύθυνσης SIP ρωτώντας στο Δημόσιο ENUM. Σε αυτή την περίπτωση η αίτηση SIP που θα προωθήσει θα είναι για το νέο αναγνωριστικό που έμαθε, με αποτέλεσμα ο Aggregator να έχει πλέον λιγότερες εναλλακτικές επιλογές. Ουσιαστικά, ο Aggregator είναι ελεύθερος να επιλέξει μόνο τον επόμενο εξυπηρετητή σηματοδοσίας και όχι από "ζευγάρια" (αναγνωριστική διεύθυνση, ικανός εξυπηρετητής).

Υπάρχουν, όμως, και περιπτώσεις στις οποίες οι πάροχοι στο μονοπάτι σηματοδοσίας που βρίσκονται πλησιέστερα στον προορισμό αποκτούν σημαντικό έλεγχο. Για παράδειγμα, έστω μία κλήση VoIP προς ένα προορισμό που είναι εγγεγραμμένος στο E.NUM και διαθέτει τηλεφωνικό αριθμό καθώς και διεύθυνση SIP. Ενδέχεται ο καλών να προτιμά η κλήση να δρομολογηθεί μέσω ενός Gateway προς το PSTN, παρόλο που υπάρχει δυνατότητα αποφυγής του. Αυτό όμως δε σημαίνει ότι θα αποτρέψει τον πάροχό του (ή κάποιον μεταγενέστερο) να ξαναρωτήσει το ENUM και να προωθήσει την κλήση στον πάροχο SIP του καλούμενου. Ακόμη και αν οι πάροχοι ήταν αδιάφοροι για τη μέθοδο δρομολόγησης δεν υπάρχει ο μηχανισμός που θα τους πληροφορεί για τις προτιμήσεις του καλούντος.

Βέβαια απαραίτητη προϋπόθεση για τη λειτουργία του Δημοσίου ENUM είναι οι καλούμενοι χρήστες να εγγραφούν. Αν και ενδέχεται κάποιοι χρήστες να υιοθετούν γρήγορα νέες τεχνολογίες, αυτοί θα εξακολουθούν να είναι συνδρομητές αν αναμένουν ότι και άλλοι θα τους μιμηθούν ώστε τελικά να δικαιωθούν από την επιλογή τους. Οι υπόλοιποι χρήστες θα εξετάσουν πιο βραχυπρόθεσμους παράγοντες, όπως α) τα τέλη συνδρομητή από τους παρόχους υπηρεσιών Δημοσίου ENUM, β) το κόστος απόκτησης εναλλακτικών αναγνωριστικών διευθύνσεων και γ) το όφελος από αυτή την υπηρεσία. Ειδικά σε ό,τι αφορά το όφελος ενός καλούμενου αυτό μπορεί να περιλαμβάνει τη λήψη εξελιγμένων υπηρεσιών, όπως για παράδειγμα ευέλικτη υπηρεσία τηλεφωνητή. Επομένως, φαίνεται αρχικά το Δημόσιο ENUM απευθύνεται σε εταιρικούς χρήστες οι οποίοι επιδιώκουν τη μείωση των

χαμένων κλήσεων. Με άλλα λόγια, το Δημόσιο ENUM φαίνεται να ωφελεί περισσότερο το χρήστη που καλεί (και τους παρόχους έναρξης, διαβίβασης) παρά τον καλούμενο.

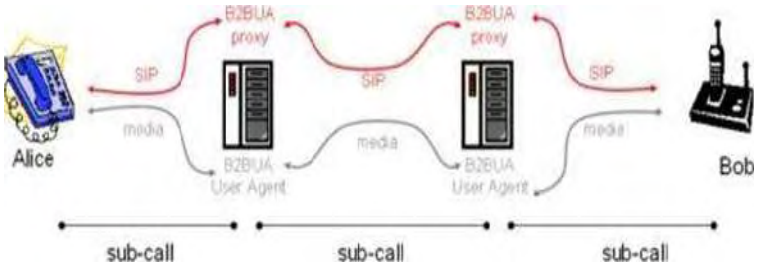
Αυτό σημαίνει ότι, δεν είναι προφανές πώς το Δημόσιο ENUM θα αποκτήσει την απαραίτητη κρίσιμη μάζα συνδρομητών ώστε τελικά να χρησιμοποιείται από τους παρόχους υπηρεσιών πολυμεσικής επικοινω*νίας*. Εξάλλου, οι πάροχοι πρέπει να αντισταθμίσουν την επιθυμία τους για εύρεση εναλλακτικών αναγνωριστικών του καλούμενου με την καθυστέρηση που θα προκληθεί στο χρόνο εγκατάστασης της κλήσης. Θεωρούμε ότι οι στρατηγικές βέλτιστης δρομολόγησης που εξετάζουμε σε επόμενο κεφάλαιο μπορούν να δώσουν την ώθηση που απαιτείται ώστε να αναζητούνται εναλλακτικά αναγνωριστικά ακόμη και όταν δεν έχουν υψηλά επίπεδα επιτυχίας (hit ratio).

Ως τώρα εξετάσαμε τα κίνητρα των παροχών ως προς την επιλογή του παρόχου που θα τερματίσει την κλήση. Στη συνέχεια αυτής της ενότητας θα περιγράψουμε τα κίνητρα των παρόχων έναρξης και διαβίβασης κλήσεων για συμμετοχή στην εγκατάσταση μιας συνόδου. Αυτό είναι ιδιαίτερα σημαντικό για τον πάροχο SIP του καλώντος, ο οποίος θέλει να συμμετέχει σε κάθε απόπειρα νέας συνόδου ώστε να εφαρμόζει την πολιτική του για επιλογή του επόμενου εξυπηρετητή.

Για παράδειγμα, ο πάροχος ενδέχεται να διαθέτει κάποια χρεώσιμη υπηρεσία που αναζητά ο χρήστης και επομένως είναι προς το συμφέρον του να περιορίσει τις επιλογές του τελευταίου. Για αυτό το λόγο, κάποιοι πάροχοι δεν επιτρέπουν στους πελάτες να χρησιμοποιήσουν την αναγνωριστική διεύθυνση SIP με άλλη συσκευή, εκτός αυτής που είναι “κλειδωμένη” να παρέχει ένα υποσύνολο των λειτουργιών. Αυτή η πολιτική των παρόχων είναι γνωστή με τον αγγλικό όρο walled garden, με την έννοια ότι ο συνδρομητής δεν έχει πλήρη ελευθερία επιλογής για τον πάροχο μιας συμπληρωματικής υπηρεσίας ή περιεχομένου (π.χ. video), και είναι χαρακτηριστική στους παρόχους κινητής τηλεφωνίας. Είναι χαρακτηριστικό ότι, η αποδοχή της πλατφόρμας IMS από πολλούς τέτοιους παρόχους οφείλεται σε μεγάλο βαθμό στην ενσωμάτωση μηχανισμών οι οποίοι επιτρέπουν τον έλεγχο των υπηρεσιών που λαμβάνει ο χρήστης.

Όπως περιγράψαμε στην ενότητα του Δημοσίου ENUM, ο συνδρομητής μπορεί να προσδιορίσει τις προτιμήσεις του στα αναγνωριστικά διευθύνσεων με τα οποία συσχετίζεται. Ωστόσο, αυτές δεν μπορεί να επιβληθούν στον καλούντα και στους παρόχους έναρξης και διαβίβασης κλήσης, οι οποίοι θα δρομολογήσουν την κλήση με βάση τα δικά τους κριτήρια. Όπως αναφέραμε και προηγουμένως, ο έλεγχος που μπορεί να ασκήσει κάποιος μειώνεται όσο πλησιέστερα στον προορισμό βρίσκεται.

Γενικά, όλοι οι πάροχοι που συμμετέχουν στη σηματοδοσία μιας συνόδου έχουν κίνητρο να χρησιμοποιούν ένα ειδικό τύπο από SIP Proxies που ονομάζονται SBC (Session Border Controllers) ή B2BUA (Back-to-Back User Agents). Ο λόγος είναι ότι, έτσι μπορούν να αποκρύψουν πληροφορίες για την εσωτερική δομή του δικτύου τους (topology hiding), την οποία θα μπορούσαν να εκμεταλλευτούν κακόβουλοι χρήστες ή άλλοι πάροχοι. Επίσης, με αυτόν τον τρόπο όσοι προηγούνται στο μονοπάτι σηματοδοσίας (χρήστης και τυχόν πάροχοι) δε θα μπορούν να συλλέξουν χρήσιμες πληροφορίες με τις οποίες θα παρακάμπτουν τον πάροχο σε επόμενες συνόδους. Στην εικόνα 14, φαίνεται η περίπτωση εγκατάστασης κλήσης μεταξύ δυο παρόχων όταν ο καθένας διαθέτει ένα Session Border Controller. Παρατηρούμε ότι η ίδια κλήση αποτελείται από τρία σκέλη και κάθε Session Border Controller αναλαμβάνει να 'γεφυρώσει' δύο από αυτά προκειμένου να ολοκληρωθεί η κλήση χωρίς να αντιληφθούν κάτι παράξενο οι τελικοί χρήστες. Βέβαια, όπως γίνεται αντιληπτό μία τέτοια πολύπλοκη διαδικασία αυξάνει το χρόνο εγκατάστασης της κλήσης.



Εικόνα 14- Η διαχείριση κλήσεων μέσω Session Border Controllers

Οι συμφωνίες ομότιμης συνεργασίας έχουν ισχύ μόνο ανά ζευγάρια παρόχων και μάλιστα για απευθείας προώθηση του αιτήματος μεταξύ τους. Ας υποθέσουμε ότι, ο καλούμενος χρήστης είναι σε καθεστώς περιαγωγής και ο πάροχος του καλώντος με τον πάροχο περιαγωγής του καλούμενου έχουν συμφωνία ομότιμης συνεργασίας. Αν ο πάροχος του καλούμενου επέλεγε να ανακατευθύνει την αίτηση, αντί να την προωθήσει προς τον πάροχο περιαγωγής, τότε ο πάροχος του καλούμενου θα ολοκλήρωνε την κλήση με ανταποδοτικό τρόπο και όχι με χρέωση. Βλέπουμε λοιπόν ότι, η ενεργή συμμετοχή ενός παρόχου επηρεάζει ποιες συμφωνίες συνεργασίας θα ενεργοποιηθούν για την εγκατάσταση μιας κλήσης, το οποίο μπορεί να έχει αρνητικό αντίκτυπο για κάποιον άλλο πάροχο.

3.7.3. Έλεγχος Μονοπατιού Δεδομένων

Εκτός από την επιθυμία για συμμετοχή στη σηματοδοσία μιας συνόδου πολυμέσων, οι ITSPs ενδέχεται να επιθυμούν έλεγχο και στο μονοπάτι που ακολουθούν τα πακέτα δεδομένων. Όπως είδαμε σε προηγουμένη ενότητα το πρωτόκολλο SIP δεν μπορεί να καθορίσει το μονοπάτι αυτό άμεσα αλλά οι πάροχοι έχουν τη δυνατότητα να το κάνουν χρησιμοποιώντας τους Session Border Controllers.

Ο Session Border Controller μοιάζει με ένα χρήστη (User Agent) ο οποίος συμμετέχει σε δύο κλήσεις ταυτόχρονα (μία από κάθε πλευρά) και ό,τι ακούει στο ένα σκέλος της κλήσης το μεταφέρει στο άλλο. Το γεγονός αυτό δίνει τη δυνατότητα στους ITSPs να πετυχαίνουν το επιθυμητό επίπεδο ποιότητας υπηρεσίας επειδή οι ειδικοί αυτοί SIP proxies μπορούν να υποδείξουν στους δρομολογητές MPLS ποιο εικονικό μονοπάτι να χρησιμοποιηθεί. Επίσης, μπορούν να ξεπεραστούν ευκολότερα προβλήματα διάσχισης τειχών προστασίας και εξυπηρετητών NAT (Network Address Translation). Βέβαια, όσο περισσότεροι Session Border Controllers συμμετέχουν σε μία κλήση τόσο μεγαλύτερος ο κίνδυνος τα χαρακτηριστικά του μονοπατιού να υποβαθμιστούν.

Αυτό θα μπορούσε να συμβεί στις περιπτώσεις που αυτοί οι κόμβοι είναι απομακρυσμένοι. Αξίζει να τονιστεί ότι υπάρχουν πάροχοι οι οποίοι δίνουν τη δυνατότητα

στους χρήστες να επιλέξουν τη συμμετοχή ή όχι ενός Session Border Controller (π.χ. η Voxalot).

ΚΕΦΑΛΑΙΟ 4- ΜΕΘΟΔΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ VOIP

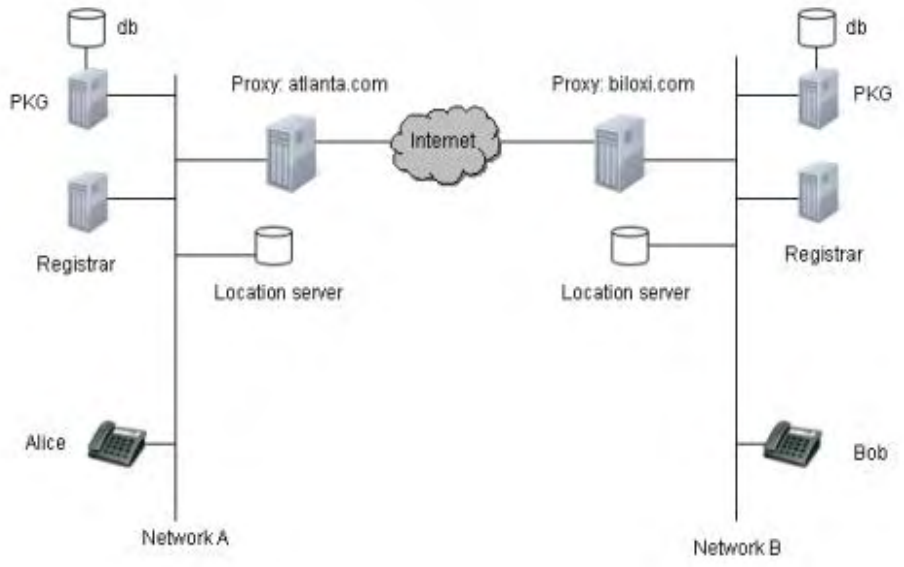
4.1. Αρχιτεκτονική συστήματος

Αυτή η ενότητα προσδιορίζει και ορίζει τα διάφορα στοιχεία που πρέπει να υπάρχουν σε ένα σύστημα VoIP που χρησιμοποιεί μια έκδοση IBE του S / MIME για την εξασφάλιση της σηματοδότησης SIP. Εξετάστε το ακόλουθο σενάριο (εικόνα 15): Η Alice είναι χρήστης του Δικτύου Α και θέλει να μιλήσει με τον Bob που είναι χρήστης στο Δίκτυο Β. Το Δίκτυο Α και το Δίκτυο Β είναι χωριστά δίκτυα που διασυνδέονται μέσω πύλης / πληρεξουσίων.

Το όνομα τομέα για το δίκτυο Α είναι atlanta.com και το biloxi.com για το δίκτυο Β.

Το Internet χρησιμοποιείται ως μέσο μεταφοράς για την κυκλοφορία μεταξύ των διαφόρων τομέων. Κάθε μήνυμα SIP δρομολογείται μέσω ενός ή περισσοτέρων κόμβων στο Internet. Αυτοί οι κόμβοι δεν εποπτεύονται από παρόχους υπηρεσιών στο δίκτυο Α ή Β και δεν μπορούν να θεωρηθούν ασφαλείς. Η Alice και η Bob έχουν το τηλέφωνο VoIP που μπορεί να είναι μια συσκευή υλικού ή ένα softphone. Κάθε συσκευή μπορεί να συνδεθεί στο τοπικό δίκτυο με καλώδιο ή ασύρματη μετάδοση. Κάθε δίκτυο περιέχει έναν καταχωρητή και έναν διακομιστή τοποθεσίας που περιέχει πληροφορίες για κάθε χρήστη. Αυτοί οι διακομιστές περιέχουν συνήθως πληροφορίες εγγραφής και ελέγχου ταυτότητας μαζί με διευθύνσεις και κατάσταση IP για κάθε παράγοντα χρήστη. Η Alice είναι εγγεγραμμένη στο domain atlanta.com και ο Bob είναι εγγεγραμμένος στο biloxi.com. Η διεύθυνση IP της συσκευής αποθηκεύεται στο διακομιστή τοποθεσίας όταν ένα τηλέφωνο συνδέεται στο τοπικό δίκτυο.

Το νέο στοιχείο που εισάγεται είναι ένας διακομιστής ιδιωτικού κλειδιού (PKG) με μια συνημμένη βάση δεδομένων. Το PKG είναι υπεύθυνο για την παράδοση των παραμέτρων του συστήματος IBE και για τον υπολογισμό δημόσιων και ιδιωτικών κλειδιών για τους τοπικούς χρήστες. Οι παράμετροι και τα κλειδιά αποθηκεύονται σε συνημμένα βάση δεδομένων. Πρέπει να υπάρχει τουλάχιστον ένα PKG σε κάθε δίκτυο παρόχου.



Εικόνα 15- Αρχιτεκτονική συστήματος

Ένας παράγοντας χρήστη πρέπει να επικοινωνήσει με το PKG για να πάρει αυτές τις παραμέτρους του συστήματος και για να πάρει δημόσια και ιδιωτικά κλειδιά. Αυτό απαιτεί ένα νέο πρωτόκολλο για την επικοινωνία μεταξύ μιας UA και μιας PKG.

Σχεδιασμός πρωτοκόλλου

Οι ακόλουθες μέθοδοι προσδιορίζονται στο πρωτόκολλο μεταξύ μιας UA και της τοπικής PKG.

- Είσοδος χρήστη. Ο χρήστης πρέπει να έχει πιστοποιηθεί πριν εκτελέσει άλλες εντολές.
- Αποσυνδεδεμένος χρήστης. Αποσυνδεθείτε από το διακομιστή PKG.
- Λήψη παραμέτρων του συστήματος.

Ένα τηλέφωνο που είναι συνδεδεμένο σε δίκτυο για πρώτη φορά χρειάζεται να πάρει τις παραμέτρους του συστήματος που χρησιμοποιούνται από το σύστημα IBE. Μπορεί επίσης να χρειαστεί να λαμβάνετε ενημερώσεις από καιρό σε καιρό από το τοπικό PKG.

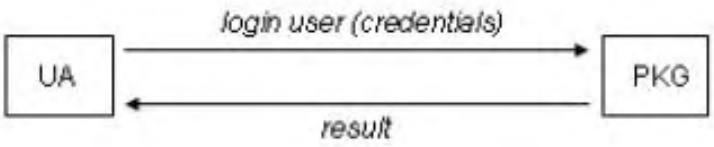
• Λήψη δημόσιου κλειδιού από τον πάροχο.

• Απόκτηση ιδιωτικού κλειδιού για την σύνδεση UA. Η επικοινωνία μεταξύ ενός UA και ενός PKG θα πρέπει, εάν είναι δυνατόν, να κρυπτογραφηθεί για να αποτρέψει έναν εισβολέα από την υποκλοπή στην επικοινωνία που μπορεί να περιέχει ευαίσθητες πληροφορίες. Αυτό γίνεται συνήθως με την προσθήκη ενός πιστοποιητικού διακομιστή στο PKG και θα χρησιμοποιηθεί επίσης για την αναγνώριση του διακομιστή PKG στους πελάτες.

Χρήστης σύνδεσης

Το PKG περιέχει ευαίσθητες πληροφορίες όπως το βασικό κλειδί του παροχέα που χρησιμοποιείται για την παραγωγή όλων των άλλων κλειδιών. Το PKG μπορεί επίσης να περιέχει όλα τα ιδιωτικά κλειδιά που υπολογίζονται και δημόσια κλειδιά για διαφορετικούς παρόχους υπηρεσιών.

Ο διακομιστής PKG πρέπει να τοποθετηθεί σε ασφαλή ζώνη και δεν πρέπει να είναι διαθέσιμο από απομακρυσμένα δίκτυα ή από το Internet. Μόνο χρήστες που είναι εγγεγραμμένοι και έχουν αποδείξει την ταυτότητά τους πρέπει να μπορούν να επικοινωνούν με το PKG. Αυτό υποδεικνύει ότι πρέπει να χρησιμοποιηθεί κάποια μέθοδος ελέγχου ταυτότητας. Εντούτοις εναπόκειται στους διάφορους παρόχους να αποφασίσουν το επίπεδο ασφάλειας στην PKG. Οι πιθανές μέθοδοι επαλήθευσης είναι το όνομα χρήστη / κωδικό πρόσβασης ή οι έξυπνες κάρτες με στοιχεία ταυτότητας / πιστοποιητικό ταυτότητας που αποδεικνύουν την ταυτότητα των χρηστών. Ένα UA επικυρώνει τον εαυτό του με την παροχή της απαραίτητης πιστοποίησης, (εικόνα 16). Αποτέλεσμα του ελέγχου ταυτότητας επιστρέφεται και δημιουργείται μια περίοδος μεταξύ UA και PKG



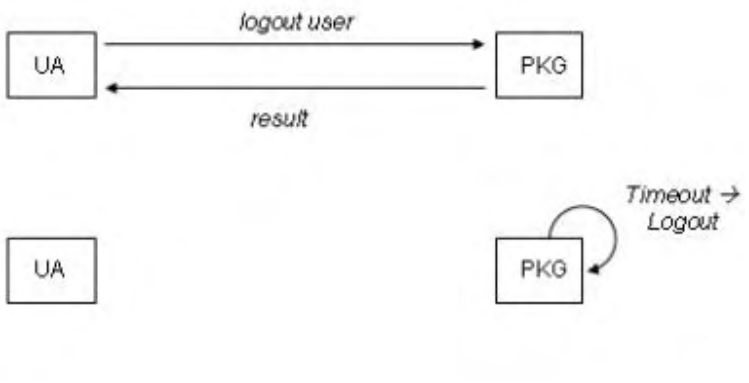
Εικόνα 16- Είσοδος χρήστη στο PKG

Ένας χρήστης που έχει συνδεθεί πρέπει να παραμείνει ενεργός για ένα προκαθορισμένο χρονικό διάστημα για να μπορεί να εκτελέσει επιπλέον ερωτήματα.

Αποσυνδεδεμένος χρήστης

Ένας χρήστης που αποσυνδέεται θα πρέπει επίσης να αποσυνδεθεί από το διακομιστή PKG για να αποφευχθεί η κατάχρηση. Αυτό γίνεται από το UA εκτελώντας μια εντολή αποσύνδεσης(εικόνα 17).

Το αποτέλεσμα από την εντολή επιστρέφεται στην UA.



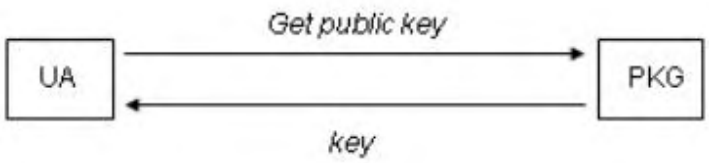
Εικόνα 17- Έξοδος χρήστη στο PKG

Αυτές οι παράμετροι είναι στατικές και είναι οι ίδιες για όλους τους παρόχους υπηρεσιών που χρησιμοποιούν τον ίδιο αλγόριθμο IBE και χρειάζονται μόνο μία φορά. Μια UA πρέπει στη συνέχεια να αποθηκεύσει αυτές τις παραμέτρους τοπικά και να τις χρησιμοποιήσει μαζί με πληροφορίες συγκεκριμένων παρόχων κατά την κρυπτογράφηση / αποκρυπτογράφηση μηνυμάτων.

Λήψη δημόσιου κλειδιού

Το δημόσιο κλειδί είναι στην περίπτωση αυτή ένα κλειδί συγκεκριμένου φορέα παροχής υπηρεσιών. Αυτό το κλειδί πρέπει, όταν κρυπτογραφεί ένα μήνυμα ή όταν επικυρώνεται μια υπογραφή, να χρησιμοποιείται μαζί με τη συμβολοσειρά που προσδιορίζει τον παραλήπτη ενός μηνύματος.

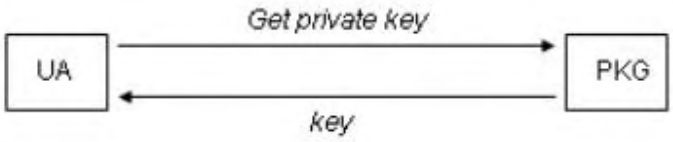
Η υπηρεσία συνδυασμού ενός δημόσιου κλειδιού παροχής και μιας συμβολοσειράς αναγνωριστικού πρέπει να επισημαίνει συνολικά τον παραλήπτη του μηνύματος. Μόνο ο παραλήπτης με το αντίστοιχο ιδιωτικό κλειδί είναι σε θέση να αποκρυπτογραφήσει αυτό το μήνυμα. Μια UA ζητά από το τοπικό PKG ένα συγκεκριμένο κλειδί για τον φορέα παροχής υπηρεσιών όταν καταγράφει αυτόν τον πάροχο για πρώτη φορά, εικόνα 18. Ένα δημόσιο κλειδί επιστρέφεται και πρέπει να αποθηκεύεται τοπικά από την UA για περαιτέρω χρήση (Wang, 2014).



Εικόνα 18- Λήψη δημόσιου κλειδιού από τον πάροχο

Απόκτηση ιδιωτικού κλειδιού

Ένας χρήστης που θέλει να αποκρυπτογραφήσει ένα ληφθέν μήνυμα ή να υπογράψει ένα μήνυμα για αποστολή, χρειάζεται ένα ιδιωτικό κλειδί. Αυτό το κλειδί υπολογίζεται από το PKG κατόπιν αιτήματος από UA (εικόνα 19). Η απαιτούμενη είσοδος είναι επειδή μια συμβολοσειρά αναγνωριστικού αναγνωρίζει τον αιτούντα χρήστη. Το ιδιωτικό κλειδί επιστρέφεται στην UA και πρέπει να αποθηκεύεται με ασφάλεια για περαιτέρω χρήση. Αυτό το κλειδί θα πρέπει να γνωρίζει μόνο ο ιδιοκτήτης και το PKG.

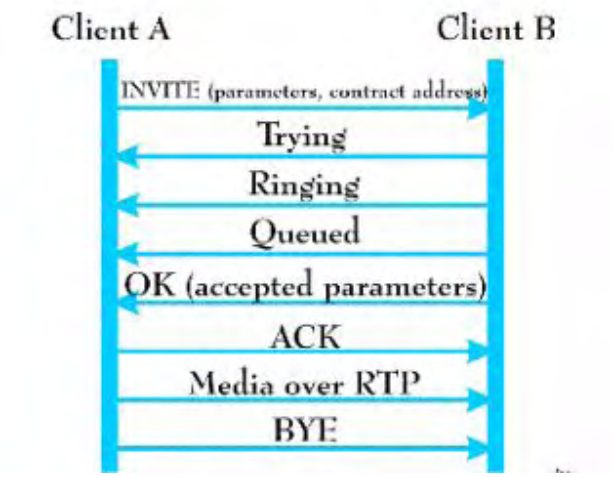


Εικόνα 19- Λήψη ιδιωτικού κλειδιού από το PKG

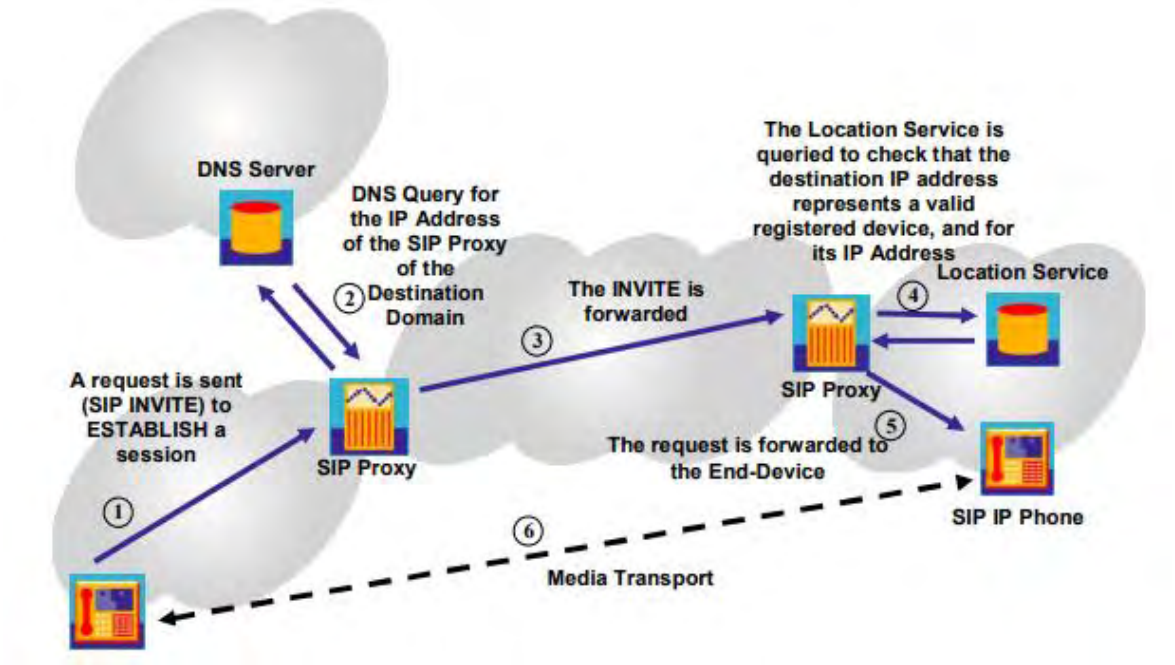
4.2. SIP (SESSION INITIATION PROTOCOL)

Το πρωτόκολλο έναρξης σύνδεσης (SIP) καθορίστηκε από την ομάδα εργασίας για την τεχνολογία του Διαδικτύου (IETF) για τη δημιουργία, τροποποίηση και τερματισμό συνεδριών μεταξύ δύο ή περισσοτέρων συμμετεχόντων.

Αυτές οι συνεδρίες δεν περιορίζονται σε κλήσεις VoIP. Το πρωτόκολλο SIP είναι ένα πρωτόκολλο βασισμένο σε κείμενο παρόμοιο με το HTTP και προσφέρει μια εναλλακτική λύση στα σύνθετα πρωτόκολλα H.323. Λόγω της απλούστερης φύσης του, το πρωτόκολλο γίνεται όλο και πιο δημοφιλές από την οικογένεια πρωτοκόλλων H.323 και πιθανόν να αναδειχθεί ως το κυρίαρχο πρότυπο τα επόμενα χρόνια. Μια εγκατάσταση SIP συνήθως χρησιμοποιεί διακομιστή μεσολάβησης για την πραγματοποίηση κλήσεων για λογαριασμό του τελικού σημείου (χρήστης ή τηλέφωνο VoIP) και διακομιστή τοποθεσίας για την παρακολούθηση της θέσης ενός τελικού σημείου. Αυτά τα στοιχεία απεικονίζουν μια τυπική κλήση βασισμένη σε SIP:



Εικόνα 20- Σύνδεση SIP και μεταφορά δεδομένων



Εικόνα 21- Κλήση SIP εν εξελίξει

Με βάση τις διάφορες απειλές και τεχνολογίες που συζητήθηκαν, ορισμένες συστάσεις θα μπορούσαν να δοθούν ως εξής:

• Το τελικό σημείο στις εγκαταστάσεις του χρήστη δεν θα πρέπει να χρειάζεται πρόσβαση στο Internet. Είναι εφικτή η σύνδεση με τον διαχειριστή κλήσεων και άλλα τηλέφωνα.

• Το τηλέφωνο ή το τελικό σημείο δεν πρέπει να έχουν πρόσβαση στα κανονικά δεδομένα, μια πιθανή εστία ιών ή το DoS θα μπορούσε να έχει ως αποτέλεσμα την εξάπλωση του ιού στα συστήματα δεδομένων.

• Όταν υπάρχει μια εμπιστευτική συνομιλία που διέρχεται στο δημόσιο δίκτυο απαιτείται πολύ υψηλή κρυπτογράφηση. Οι πληροφορίες μπορούν επίσης να περιέχουν μυστικό κλειδί.

• Όπως και τα δίκτυα δεδομένων, τα τηλέφωνα πρέπει επίσης να προστατεύονται από ένα τείχος προστασίας από απόσταση. Το τείχος προστασίας μπορεί να αρνηθεί οποιαδήποτε μη κρυπτογραφημένη κίνηση στο τηλέφωνο από το Internet.

• Το εσωτερικό δίκτυο δεδομένων θα πρέπει να υλοποιείται ξεχωριστά με το δίκτυο φωνής.

• Οποιεσδήποτε αναβαθμίσεις ή ρυθμίσεις που απαιτούνται σε οποιαδήποτε συσκευή πρέπει να χρειάζονται έλεγχο ταυτότητας.

4.3. Πρότυπα ασφαλείας στο VoIP

Τα πρότυπα ασφαλείας είναι η καλύτερη λύση για τα επαναλαμβανόμενα προβλήματα ασφάλειας των πληροφοριών (Schumacher και Roedig, 2001). Αποτελείται από μια επισκόπηση, περιγραφή του προβλήματος και λύση με συνέπειες. Τα τέσσερα μοτίβα που περιγράφονται σε αυτήν την ενότητα είναι Τμήμα φωνής / δεδομένων, σήραγγα, έλεγχος ταυτότητας κλήσεων και εμπιστευτικότητα κλήσεων.

✦ **Τμηματοποίηση φωνής / δεδομένων**

Το μοτίβο διαχωρισμού φωνής / δεδομένων διαχωρίζει τις υπηρεσίες φωνής και δεδομένων, προκειμένου να αντιμετωπίσει τις απειλές για φωνή VLAN από εισβολέα στο VLAN δεδομένων. Οι συγκλίνουσες υπηρεσίες παρέχουν τη δυνατότητα υλοποίησης της τηλεφωνίας στο υφιστάμενο δίκτυο δεδομένων με βάση το IP. Ένας οικονομικός παράγοντας για τη μετάβαση προς το VoIP είναι η δυνατότητα χρήσης ενός μόνο δικτύου για την εκτέλεση υπηρεσιών φωνής και δεδομένων. Ο τομέας προβλημάτων αποτελείται από την εύρεση μεθόδων για την αποφυγή οποιωνδήποτε επιθέσεων από δίκτυα δεδομένων στην κίνηση φωνής σε περιβάλλον VoIP. Εάν μια εταιρεία λογιστικής έχει υλοποιήσει φωνητικές υπηρεσίες, για παράδειγμα, ξεκινώντας ένα τηλεφωνικό κέντρο πελατών με βάση το VoIP για εμπορικούς σκοπούς και σκοπούς πωλήσεων. Εάν υπάρχει επίθεση στο σύστημα δεδομένων, υπάρχουν διαθέσιμες υπηρεσίες δημιουργίας αντιγράφων ασφαλείας για την ανάκτηση των δεδομένων, αλλά η διοίκηση είναι αμφίβολη σε περίπτωση που μια επίθεση οδηγεί στο τηλεφωνικό κέντρο VoIP. Η διακοπή της λειτουργίας θα ήταν πολύ δαπανηρή.

Πώς να αποτρέψετε το φωνητικό δίκτυο από τέτοιες επιθέσεις;

Λύση

Μπορούμε να απομονώσουμε δύο διαφορετικά VLANs για φωνή και δεδομένα, χρησιμοποιώντας τμηματοποίηση του στρώματος τριών. Όλη η κυκλοφορία inter VLAN πρέπει να περάσει από τη συσκευή δρομολόγησης που φιλτράρει την κυκλοφορία χρησιμοποιώντας λίστες ελέγχου πρόσβασης. Η ανάπτυξη υπηρεσιών IP τηλεφωνίας και υπηρεσιών δεδομένων IP πρέπει να διαχωρίζεται σε δύο λογικά χωριστά VLAN (DISA, 2004). Οι τερματικές συσκευές, όπως τα τηλέφωνα IP, πρέπει να βρίσκονται σε VLAN που υποστηρίζουν μόνο υπηρεσίες IP τηλεφωνίας. Ομοίως, οι διακομιστές VoIP πρέπει να προστατεύονται από ένα γνωστό τείχος προστασίας VoIP που βρίσκεται σε ξεχωριστό τμήμα. Το φιλτράρισμα πακέτων θα μπορούσε εύκολα να ρυθμιστεί σε συσκευή δρομολόγησης, π.χ. δρομολογητές κ.λπ. που συνδέουν VLAN φωνής και δεδομένων. Η εφαρμογή ενός πλήρους τείχους προστασίας κατάστασης στο Voice VLAN θα μπορούσε να προσφέρει καλύτερη προστασία από τα δεδομένα VLAN.

- **Tunneling (σήραγγα)**

Το πρότυπο tunneling διασφαλίζει την παροχή εμπιστευτικότητας και ακεραιότητας των πακέτων φωνής στην τηλεφωνία IP. Ένας φωνητικός σύνδεσμος πρέπει να δημιουργηθεί μεταξύ δύο ή περισσότερων τελικών χρηστών VoIP σε απομακρυσμένη θέση σε διαφορετικά intranets. Ο σύνδεσμος επικοινωνίας είτε θα μπορούσε να δημιουργηθεί μέσω ενός ιδιωτικού δικτύου μητροπολιτικών περιοχών (MAN), ενός δικτύου ευρείας περιοχής (WAN) ή ενός δημόσιου μέσου όπως το Διαδίκτυο. Η κίνηση φωνής είναι ύποπτη για έκθεση στους χάκερ ενώ περνά μέσω δημόσιου δικτύου όπως το Διαδίκτυο. Η κυκλοφορία σε δημόσιο μέσο είναι ορατή σε άλλα ιδιωτικά δίκτυα. Το πεδίο προβλημάτων αποτελείται από την εύρεση μεθόδων για την αντιμετώπιση των επιθέσεων Man in the middle και παρόμοιων επιθέσεων σε πακέτα φωνής που εκτελούνται σε δίκτυο VoIP. Εάν ένας οργανισμός που εκτείνεται σε όλο τον κόσμο, θέλει να συνδέσει όλα τα υποκαταστήματά του με την έδρα, έτσι ώστε η επικοινωνία

να είναι καλύτερη και ταχύτερη. Αλλά το πρόβλημα είναι ότι ο οργανισμός πρέπει να επιλέξει το δημόσιο μέσο ως την κύρια διαδρομή επειδή η κατοχή ειδικών μισθωμένων γραμμών είναι υπερβολικά δαπανηρή. Πώς θα ήταν οι εμπιστευτικές πληροφορίες μιας επιχείρησης να είναι ασφαλείς στο δημόσιο δίκτυο;

Η τεχνολογία Virtual Private Networks (VPN) παρέχει έναν μηχανισμό tunneling μέσω του δημόσιου δικτύου για να μεταφέρει οποιαδήποτε εμπιστευτική κίνηση από τα ιδιωτικά δίκτυα. Οι δύο θέσεις μπορούν να επικοινωνήσουν με ασφάλεια πάνω από αυτές τις άκρες για να τελειώσουν τις σήραγγες. Ένα από τα τελικά σημεία ξεκινά τη σύνδεση για να δημιουργήσει ένα ασφαλές κανάλι. Οι κατάλληλοι κόμβοι δικτύου αποτελούν τα σημεία εκκίνησης και τερματισμού του ενδιάμεσου δικτύου μεταφορών. Η τεχνική VPN αποτελείται από την τεχνική ενθυλάκωσης. Η φωνητική κίνηση εξασφαλίζεται με την ενσωμάτωσή της μέσα σε ένα IPSec ή παρόμοιο πρότυπο σήραγγας. Ο βασικός μηχανισμός πίσω από τη σήραγγα είναι η κρυπτογράφηση που εξασφαλίζει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων σε δίκτυα VoIP. Πριν από τη δημιουργία ενός tunneling σύνδεσης χρησιμοποιεί το πρωτόκολλο ελέγχου ταυτότητας για να ρυθμίσει μια σχέση εμπιστοσύνης μεταξύ των συσκευών τερματικών δικτύου. Η κρυπτογράφηση θα μπορούσε να επιβραδύνει την απόδοση και είναι ένα μεγάλο ζήτημα για την ποιότητα της υπηρεσίας. Ένας συμμετρικός αλγόριθμος κρυπτογράφησης θα πρέπει να προτιμάται για τη φωνητική μεταφορά που θα βοηθήσει στην επιτάχυνση της διαδικασίας ενώ θα παρέχει εμπιστευτικότητα. Το VPN θα μπορούσε να χρησιμοποιήσει την κρυπτογραφία δημόσιου κλειδιού.

- **Εμπιστευτική κλήση**

Σε μηχανισμούς εμπιστευτικής κλήσης, παρέχονται μηχανισμοί ασφαλείας όπως η κρυπτογράφηση σε επίπεδο υλικού, όπως τα τηλέφωνα IP. Όταν δύο ή περισσότεροι συνδρομητές εμπλέκονται σε μια εμπιστευτική φωνητική κλήση μέσω δημόσιου καναλιού, οι τελικοί χρήστες πρέπει να είναι βέβαιοι ότι υπάρχει μήνυμα που παραδίδεται από το ένα άκρο σε άλλο και ανακτά το απόρρητό του. Η φωνητική συνομιλία ενδέχεται να παρεμποδιστεί μεταξύ των σημείων προέλευσης και τερματισμού του δικτύου VoIP. Το δημόσιο δίκτυο, όπως το Διαδίκτυο, δεν είναι ασφαλές μέσο. Επομένως, οι διαχειριστές

δικτύου πρέπει να εφαρμόζουν κρυπτογραφικούς αλγόριθμους και τεχνικές προκειμένου να εξασφαλίσουν την ασφάλεια των πακέτων φωνής. Μια φωνητική ροή στο Διαδίκτυο είναι ευάλωτη στην υποκλοπή. Ο τομέας προβλήματος αποτελείται από την αφαίρεση τεχνικών για την αποτροπή επιθέσεων από sniffers κατά την πραγματοποίηση ή τη λήψη κλήσης στο δημόσιο δίκτυο. Εάν οι γενικοί οικιακοί χρήστες ή μια μικρή εταιρεία που δεν έχει μεγάλη υποδομή, όπως ο αριθμός των διακομιστών και των πυλών για το δίκτυο VoIP, ήθελαν να επικοινωνήσουν με ασφάλεια, εφαρμόζοντας κρυπτογράφηση χωρίς σήραγγα, θα προκύψουν παρόμοια αποτελέσματα;

Λύση

Για να αντιμετωπιστεί το ζήτημα της εμπιστευτικότητας, το πρότυπο κλήσης Secure VoIP χρησιμοποιεί τεχνικές κρυπτογράφησης και αποκρυπτογράφησης για κλήσεις VoIP. Όπως αναφέρθηκε προηγουμένως, η λανθάνουσα κατάσταση είναι ένα σημαντικό ζήτημα σε πολλές συγκλινόμενες υπηρεσίες, προτιμώνται οι συμμετρικοί αλγόριθμοι κρυπτογράφησης.

Προβλέψεις σε Δίκτυα, Πληροφορική και Επικοινωνίες. Αυτός ο αλγόριθμος δημιουργεί ένα κοινό κρυπτογραφικό κλειδί δηλαδή ένα κοινό μυστικό κλειδί που διέρχεται και στις δύο πλευρές του καναλιού. Κατά προτίμηση, το πρότυπο IPSec μπορεί να χρησιμοποιηθεί. Αν είναι έτσι, τότε είναι υποχρεωτικό για τον καλούντα και τον καλούμενο να συμμετάσχουν σε φωνητική συνομιλία και να συμφωνήσουν προηγουμένως σε μηχανισμούς κρυπτογράφησης δεδομένων που πρέπει να συμπεριληφθούν στο IPSec, δηλ. DES, MD5, SHA μαζί με ένα κοινό μυστικό κλειδί.

Ο εντολέας κρυπτογραφεί την κλήση χρησιμοποιώντας ένα κοινό μυστικό κλειδί στο τέλος και το στέλνει ξεχωριστά στο άτομο στο άλλο άκρο. Ο δέκτης αποκρυπτογραφεί τη φωνητική κλήση χρησιμοποιώντας το κλειδί και αναπαράγει τις πληροφορίες. Η κρυπτογραφία δημόσιου κλειδιού θα μπορούσε να χρησιμοποιηθεί ως ο άλλος μηχανισμός κρυπτογράφησης όπου η λανθάνουσα κατάσταση δεν είναι μεγάλο ζήτημα. Αυτό θεωρείται ως η πιο ασφαλής μέθοδος. Σε αυτό το σενάριο ο δέκτης πρέπει να αποκτήσει το δημόσιο κλειδί των αποστολέων πριν από τη δημιουργία οποιασδήποτε φωνητικής σύνδεσης. Ο αποστολέας

κρυπτογραφεί τη φωνή / δεδομένα με το ιδιωτικό του κλειδί, ο καλών πρέπει να αποκτήσει το δημόσιο κλειδί του καλούντος πριν από τη δημιουργία μιας σύνδεσης. Ο καλών κρυπτογραφεί τη φωνητική κλήση με δημόσιο κλειδί καλούντος και τον στέλνει σε αυτόν. Ο Callee αποκρυπτογραφεί τη φωνητική κλήση και ανακτά τα αρχικά πακέτα φωνής. Οι ιδιότητες τόσο της συμμετρικής όσο και της ασύμμετρης κρυπτογράφησης θα μπορούσαν να συγχωνευθούν. Το συμμετρικό κλειδί που πρέπει να κατανεμηθεί μεταξύ των τερματικών ακροδεκτών και να μεταφερθεί κατά μήκος του ίδιου μέσου θα μπορούσε να κάνει χρήση ασύμμετρης κρυπτογράφησης, η οποία είναι εφικτή για μικρό όγκο δεδομένων. Με τον τρόπο αυτό συνδυάζονται τόσο οι συμμετρικές όσο και οι ασύμμετρες τεχνικές κρυπτογραφίας για την παροχή γρήγορων και ασφαλών αποτελεσμάτων.

- **Έλεγχος ταυτότητας κλήσης.**

Στο πρότυπο ελέγχου ταυτότητας κλήσης, ο έλεγχος ταυτότητας χρήστη επαληθεύεται όταν πραγματοποιείται κλήση VoIP στο δημόσιο δίκτυο. Μια συνομιλία φωνής που χρησιμοποιεί την πρόσβαση του κοινού ως μέσο μπορεί να δημιουργήσει προβλήματα εμπιστευτικότητας και εξακρίβωσης της ταυτότητας. Ο συνδρομητής που μιμείται μια κλήση VoIP θα μπορούσε να αμφιβάλει εάν μιλάει στον αποδέκτη ή τον εισβολέα. Ομοίως, ένα άτομο στο τέλος της συνομιλίας VoIP δεν θα μπορούσε να αποδείξει την αυθεντικότητα του καλούντος, καθώς ο καλών μπορεί να απορρίψει την πατρότητα οποιωνδήποτε κλήσεων έκανε ο ίδιος. Πέρα από αυτό, καθώς τα δημόσια κλειδιά είναι ευρέως διαθέσιμα, οποιοσδήποτε εισβολέας θα μπορούσε να παρεμποδίσει τα κρυπτογραφημένα δεδομένα, αν και δεν μπορεί να τα διαβάσει, αλλά μπορεί να προσθέσει ψευδείς πληροφορίες ή να στείλει εξ ολοκλήρου ένα νέο κρυπτογραφημένο πακέτο στο δημόσιο κλειδί των δεκτών. Ο δέκτης μπορεί να μην επαληθεύει την ακεραιότητα του μηνύματος.

Ο τομέας προβλήματος αποτελείται από οποιεσδήποτε μεθόδους που εξασφαλίζουν ότι οι εισβολείς δεν είναι σε θέση να αποκρυπτογραφήσουν την κλήση. Απαιτείται λύση σχετικά με

τον τρόπο αποδείξεως των καλούντων και του ελέγχου ταυτότητας μηνυμάτων, έτσι ώστε ο καλών να μην μπορεί να αρνηθεί μια κλήση που πραγματοποιήθηκε για να καλέσει.

4.4. Τρωτά σημεία- Μέθοδοι επιθέσεων

Τα τρωτά σημεία σε δίκτυα VoIP μπορούν να αξιοποιηθούν από εισβολείς. Οι συνέπειες της εκμετάλλευσης αυτών των τρωτών σημείων, συμπεριλαμβανομένης της διακοπής των υπηρεσιών μέσων επικοινωνίας μέσω των «πλημμυρών» της κυκλοφορίας, με πρόσβαση σε εμπιστευτικές και διαβαθμισμένες πληροφορίες κατά την παρακράτηση σημάτων κλήσης ή περιεχομένου, υποδηλώνουν ότι οι διακομιστές μπορούν να καταλάβουν τις κλήσεις και την υποκλοπή ταυτότητας με αποτέλεσμα την ελεύθερη χρήση καθώς και η τοποθέτηση δόλιας κλήσης. Αυτό θα επηρεάσει αμετάβλητα την ασφάλεια των χρηστών, η οποία στηρίζεται στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Για το σκοπό αυτό, οι διάφορες επιθέσεις σε δίκτυα VoIP θα συζητηθούν παρακάτω:

- Εναλλαγή πρωτοκόλλου σήματος: η επίθεση αυτή στοχεύει στη διαδικασία ρύθμισης κλήσης. Ενέχει τον επιτιθέμενο να είναι σε θέση να παρακολουθεί και να καταγράφει τα πακέτα κατά τη διάρκεια της εγκατάστασης κλήσης. Ο εισβολέας, μέσω αυτής της διαδικασίας, μπορεί να αλλάξει τα πεδία ροής δεδομένων. Αυτό θα του επιτρέψει να πραγματοποιήσει κλήσεις VoIP χωρίς τηλέφωνο VoIP.
- Επιθέσεις καταστολής: Σε αυτήν την επίθεση, μια συζήτηση μεταξύ δύο μερών μπορεί να απορριφθεί από το ένα μέρος.
- Αποτυχία εγγραφής του πρωτοκόλλου έναρξης σύνδεσης (SIP): Σε ένα δίκτυο VoIP, η δημιουργία, η τροποποίηση και ο τερματισμός των περιόδων λειτουργίας των χρηστών μπορούν να αντιμετωπιστούν από το SIP, το οποίο είναι ένα πρωτόκολλο ελέγχου επιπέδου εφαρμογής. Όπως αποδεικνύεται, το SIP καθώς και άλλα πρωτόκολλα VoIP απαιτούν την εγγραφή ενός πράκτορα χρήστη (UA / IP τηλέφωνο) με τον κόμβο ελέγχου

ενός SIP proxy / registrar. Ένας επιτιθέμενος, ο οποίος έχει επίγνωση αυτής της διαδικασίας, μπορεί να πραγματοποιήσει «πειρατεία» κατά την εγγραφή, υποβάλλοντας σε έγκυρη UA στον καταχωρητή. Αυτό επιτρέπει στον εισβολέα να τροποποιήσει την αυθεντική εγγραφή στη δική του διεύθυνση. Κατά συνέπεια, οι εισερχόμενες κλήσεις που αποστέλλονται στην έγκυρη UA θα αναπροσανατολιστούν στην αθέμιτη UA με αποτέλεσμα την απώλεια κλήσεων προς την στοχευμένη UA. Τα θύματα αυτής της κατηγορίας μπορεί να περιλαμβάνουν άτομα ή / και ομάδες χρηστών, καθώς και μια πύλη μέσων ή σύστημα φωνητικού ταχυδρομείου που χαρακτηρίζεται ως πόρος υψηλής επισκεψιμότητας. Εάν η επίθεση αυτή είναι επιτυχής, θα επηρεαστούν οι εισερχόμενες κλήσεις και το παρωχημένο UA μπορεί να καταγράψει τα περιεχόμενα των κλήσεων.

- IP Spoofing: αυτή η επίθεση συνεπάγεται τη χρήση μιας εσωτερικής ή εξωτερικής αξιόπιστης διεύθυνσης IP για την παραποίηση ενός αξιόπιστου υπολογιστή. Επίσης, οι επιθέσεις IP spoofing μπορούν να χρησιμοποιηθούν ως ο άξονας για άλλες επιθέσεις όπως μια επίθεση Denial of Service (DoS), οπότε ο χάκερ μπορεί να κρύψει την ταυτότητά του με τη χρήση παραπλανητικών διευθύνσεων πηγής. Αυτό μπορεί να οδηγήσει στην υπονόμευση της διεύθυνσης του IP PBX, όταν δεν υπάρχουν κατάλληλοι αμυντικοί μηχανισμοί, προκαλώντας την «πλημμύρα» ολόκληρου του τμήματος φωνής με πακέτα πρωτοκόλλου UDP (πρωτόκολλο πακέτου δεδομένων).

- Τροποποίηση μηνύματος του SIP: Δεδομένου ότι ένα μήνυμα SIP δεν έχει ενσωματωμένο μηχανισμό για τον έλεγχο της ακεραιότητας του μηνύματος που αποστέλλεται, είναι πιθανό ο εισβολέας να είναι σε θέση να παρακολουθήσει και να κάνει τροποποιήσεις σε ένα μήνυμα SIP χρησιμοποιώντας μια επίθεση από τον άνθρωπο στη μέση (MITM), όπως η πλαστογράφηση IP, η MAC (έλεγχος πρόσβασης πολυμέσων) πλαστογράφηση ή κατάχρηση εγγραφής SIP. Με αυτόν τον τρόπο, ο επιτιθέμενος μπορεί να κάνει αλλαγές σε όλα ή ορισμένα από τα χαρακτηριστικά του μηνύματος, υποδηλώνοντας έτσι τον καλούντα ή να είναι σε θέση να ανακατευθύνει μια κλήση προς έναν άλλο προορισμό χωρίς τη γνώση του καλούντος.

- Ελαττωμένα μηνύματα και εντολή SIP: Οι Gruber et al, αναγνώρισαν δύο κατηγορίες ανεπιθύμητων μηνυμάτων. Αυτά περιλαμβάνουν μηνύματα με δομή και σύνταξη με δυσλειτουργία. Αν και τα δομημένα μηνύματα έχουν συμμορφωθεί με τη σύνταξη RFC 3261 και ως εκ τούτου δεν παραβιάζουν τον κανόνα του πρωτοκόλλου SIP, η πολυπλοκότητα του μηνύματος αυξάνει τον χρόνο που χρησιμοποιεί ο αναλυτής για την εκτέλεση του μηνύματος. Αυτό μπορεί να οδηγήσει σε υπερχείλιση buffer όταν ένα σύστημα VoIP δεν έχει υλοποιηθεί σωστά. Από την άλλη πλευρά, μηνύματα σφάλματος σύνταξης παραβιάζουν τη σύνταξη RFC 3261 έτσι ώστε οι παραγωγοί να μην είναι σε θέση να ταξινομήσουν τα ληφθέντα μηνύματα. Συνεπώς, η δοκιμή του αναλυτή SIP με κάθε δυνατή είσοδο μπορεί να γίνει δύσκολη. Σε αυτήν την ευπάθεια, αν παραβιαστεί κάποιος από έναν εισβολέα, μπορεί να του επιτρέψει να στείλει πακέτα με παραμορφωμένη εντολή σε ευπαθείς κόμβους. Αυτό μπορεί να διακόψει τις κανονικές υπηρεσίες σε αυτόν τον κόμβο.

- Κλοπή ταυτότητας: αυτός ο τύπος επίθεσης επιτρέπει σε κακόβουλο χρήστη να αποκτήσει έγκυρη ταυτότητα από έναν νόμιμο χρήστη του συστήματος VoIP. Ορισμένες παραλλαγές κλοπής ταυτότητας, συμπεριλαμβάνουν τις βίαιες επιθέσεις λεξικών. Στην επίθεση bruce force, ο επιτιθέμενος είναι σε θέση να μεταδίδει τυχαία mishmash των χαρακτήρων στο SIP proxy και η απάντηση του μηνύματος που αποστέλλεται πίσω στον εισβολέα μπορεί να του επιτρέψει να κλέψει τις έγκυρες ταυτότητες άλλων χρηστών. Ωστόσο, στην επίθεση λεξικού, ο επιτιθέμενος στέλνει με προσοχή μια λίστα λέξεων στον SIP πληρεξούσιο με πιθανά ονόματα και κωδικούς πρόσβασης. Το μήνυμα απάντησης από το πληρεξούσιο του επιτρέπει να εντοπίσει τους πιθανούς λογαριασμούς.

- Κλοπή υπηρεσιών: αυτή η επίθεση απευθύνεται στον πάροχο υπηρεσιών και στη δυνατότητα ενός εισβολέα να κάνει δωρεάν δόλιες κλήσεις. Τα κενά στη διαμόρφωση του συστήματος VoIP μπορούν να επιτρέψουν σε έναν κακόβουλο χρήστη να παρακάμψει το σύστημα χρέωσης, να καταχραστεί τη χρήση των πόρων στο δίκτυο VoIP ή / και τους πόρους των χρηστών. Επιπλέον, οι Ζανγκ & Χουάνγκ υποστηρίζουν ότι οι συνέπειες της κλοπής υπηρεσίας μπορούν να περιλαμβάνουν υποβάθμιση της απόδοσης του

συστήματος VoIP και αύξηση των εξόδων που επιβαρύνει τον φορέα εκμετάλλευσης για την παροχή ποιοτικών υπηρεσιών. Ωστόσο, οι Coulibaly & Liu σημειώνουν ότι η κλοπή υπηρεσίας μπορεί να οδηγήσει σε απάτη κατά την οποία ένας εισβολέας μπορεί να πραγματοποιήσει κλήσεις χρησιμοποιώντας ένα μη επιτηρούμενο τηλέφωνο IP, παραβιάζοντας την ταυτότητα ενός έγκυρου χρήστη του τηλεφώνου ή τοποθετώντας ένα λανθασμένο τηλέφωνο IP στο δίκτυο ή στην παραβιαζόμενη πύλη.

- Ακύρωση / επίθεση SIP: Σε αυτό το σενάριο επίθεσης, ένα μήνυμα SIP μπορεί να δημιουργηθεί από έναν εισβολέα έτσι ώστε το μήνυμα να περιέχει την εντολή Ακύρωση ή Bye. Αυτό το μήνυμα αποστέλλεται στη συνέχεια στον στόχο (τελικός κόμβος ή τηλέφωνο). Όταν μια σταθερή ροή αυτών των πακέτων αποστέλλεται στο τηλέφωνο προορισμού, μπορεί να διακόψει τις υπηρεσίες στον τελικό κόμβο, ώστε το τηλέφωνο να μην είναι σε θέση να πραγματοποιεί ή να λαμβάνει κλήσεις.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία έγινε μελέτη των υπηρεσιών φωνής μέσω πρωτοκόλλου του Διαδικτύου, ευρύτερα γνωστές ως υπηρεσίες VoIP (Voice over Internet Protocol) η οποία γίνεται όλο και πιο δημοφιλής. Σε όλο τον κόσμο, η τηλεφωνία μέσω διαδικτύου αναπτύσσεται με ταχύτατους ρυθμούς. Καθώς με το VoIP επιτυγχάνεται η ενοποίηση δικτύων (δηλαδή η πρόσβαση στο Internet και η τηλεφωνία πάνω από ένα δίκτυο), το αποτέλεσμα είναι -ιδιαίτερα στα υπεραστικά τηλεφωνήματα- οι χρεώσεις μέσω διαδικτύου να είναι εξαιρετικά χαμηλές και συχνά να βρίσκονται κάτω από αυτές των αστικών κλήσεων.

Η αρχή λειτουργίας στην οποία στηρίζεται η λειτουργία της μετάδοσης φωνής μέσω IP είναι ότι ο πελάτης πληρώνει ένα ορισμένο ποσό για να συνδεθεί στο δίκτυο και στη συνέχεια πληρώνει ανάλογα με το χρόνο χρήσης και τις χρησιμοποιούμενες εγκαταστάσεις. Η συχνότητα που απαιτεί η τεχνολογία IP για τη μετάδοση των δεδομένων είναι τουλάχιστον έξι φορές μικρότερη από την αντίστοιχη των παραδοσιακών τηλεπικοινωνιακών δικτύων που χρησιμοποιούν σήμερα οι περισσότεροι συνδρομητές σε όλο τον κόσμο. Η σημαντική αυτή διαφορά καθιστά τις κλήσεις μέσω του VoIP σαφέστατα πιο οικονομικές, και σε αρκετές περιπτώσεις το τηλεφώνημα μέσω διαδικτύου μπορεί να στοιχίσει έως και 90% φθηνότερα απ' ότι μέσω του παραδοσιακού τηλεπικοινωνιακού δικτύου.

Τα τελευταία χρόνια έχουν αναπτυχθεί πολλά συστήματα - εφαρμογές για επικοινωνία των χρηστών μέσο VoIP. Ιδιαίτερα διαδεδομένες είναι για παράδειγμα οι εφαρμογές Skype, Google Talk, Windows Messenger, Yahoo Messenger, οι οποίες επιτρέπουν στους χρήστες τους να χρησιμοποιούν το Διαδίκτυο για δωρεάν κλήσεις και για ανταλλαγή σύντομων μηνυμάτων. Τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται στο VOIP είναι το TRIP το οποίο στοχεύει στην ανταλλαγή πληροφοριών δρομολόγησης μεταξύ παρόχων που διαθέτουν πύλες τηλεφωνίας (Gateways), το Πρωτόκολλο H.501 το οποίο είναι παρόμοιο με το TRIP, και ανήκει στη σουίτα πρωτοκόλλων του H.323, το DUND, το SIP το οποίο είναι ένα πρωτόκολλο σηματοδοσίας που ορίζει ότι χρειάζεται για να επικοινωνήσουν τα ενδιαφερόμενα μέρη.

Όπως συμβαίνει σε κάθε τεχνολογία, τα θέματα ασφάλειας, αποτελούν κρίσιμο ζήτημα προς διερεύνηση. Υπάρχουν αρκετές απειλές και ευπάθειες στην τεχνολογία VOIP. Σήμερα αν και σε θεωρητικό επίπεδο, υπάρχει αρκετή γνώση για την προστασία των εφαρμογών του εξυπηρετητή, είναι λιγότερο σαφές πώς μπορούν να προστατευτούν οι τελικές συσκευές. Την κατάσταση έρχεται να επιβαρύνει το γεγονός ότι, σπάνια γίνεται αναβάθμιση του firmware του VoIP εξοπλισμού, έξω από επιχειρηματικά περιβάλλοντα. Οι επιθέσεις traffic eavesdropping και το hijacking αποτελούν περίπου το ένα πέμπτο των απειλών αυτών. Το Voice Spam ή Spam over Internet Telephony (SPIT) είναι ένα πρόβλημα το οποίο θα επηρεάσει στο μέλλον το VoIP. Με το SPIT αναφερόμαστε στις μαζικές και ακούσιες κλήσεις που παράγονται αυτόματα.

Μια σοβαρή απειλή στην τεχνολογία VOIP είναι οι υποκλοπές, όπου χρησιμοποιούνται τα εργαλεία σύλληψης και ανάλυσης της κίνησης του δικτύου, όπως το Ethereal, για να κάνει sniffing στα μηνύματα σηματοδοσίας και τα πολυμεσικά ρεύματα (media streams) σε μια συνομιλία. Τα συλληφθέντα RTP πακέτα που ανταλλάσσονται από τα UDP ή TCP πρωτόκολλα αποκωδικοποιούνται και μετατρέπονται σε αρχεία ήχου. Επίσης, η επίθεση κατακλυσμού UDP προτιμάται από τους κακόβουλους χρήστες για να πραγματοποιηθεί κατακλυσμός στο εύρος ζώνης των γραμμών. Άλλες σοβαρές επιθέσεις είναι οι Επιθέσεις Message Tampering όπου ένας επιτιθέμενος παρεμποδίζει και τροποποιεί τα πακέτα που ανταλλάσσονται μεταξύ των SIP τμημάτων και οι Επιθέσεις Session Tear Down όπου ο επιτιθέμενος παρατηρεί τη σηματοδοσία για μια κλήση, και έπειτα στέλνει παραποιημένα αιτήματα .

Τέλος, η επίθεση Man-In-The-middle πραγματοποιεί μια τριπλή επικοινωνία μεταξύ των δύο συμβαλλόμενων μερών και του επιτιθεμένου ανάμεσα τους. Καθ’ όλη την διάρκεια της συνόδου της επικοινωνίας, τα δύο συμβαλλόμενα μέρη δεν παρατηρούν τη συμμετοχή του επιτιθεμένου. Ο επιτιθέμενος πετυχαίνει τη δρομολόγηση της κυκλοφορίας μεταξύ των δύο συμβαλλόμενων μερών μέσω αυτού. Οι πληροφορίες που στέλνονται πέρα δώθε παρεμποδίζονται, τροποποιούνται ή και διαβάζονται.

Για όλες τις παραπάνω απειλές και επιθέσεις, έρχονται να δώσουν λύση οι μέθοδοι ασφάλειας VOIP. Μία λύση κατά των επιθέσεων είναι η χρήση Black Lists και White Lists . Οι Black Lists είναι μια συλλογή από διευθύνσεις γνωστών επιτιθέμενων. Μια κλήση από μια πηγή της μαύρης λίστας απαγορεύεται αμέσως. Οι μαύρες λίστες δεν είναι αποτελεσματικές με το ηλεκτρονικό ταχυδρομείο SPAM και είναι πιθανό να είναι μόνο περιορισμένης χρήσης και για το SPIT. Επίσης, βέλτιστες πρακτικές κατά των επιθέσεων αποτελούν τα Approval Systems, τα Audio Content Filtering, τα Voice CAPTCHAs/Turing Tests τα οποία είναι προκλήσεις ή γρίφοι όπου μόνο ένας άνθρωπος μπορεί εύκολα να απαντήσει, οι λύσεις Anti DoS/DDos, δηλαδή λύσεις κατά των Denial of Service επιθέσεων, η θωράκιση της περιμέτρου του δικτύου και τα εικονικά δίκτυα (VLANs) τα οποία χρησιμοποιούνται για τον λογικό διαχωρισμό του δικτύου σε τομείς στον ίδιο φυσικό μεταγωγέα. Οι περισσότεροι μεταγωγείς υποστηρίζουν τη δημιουργία διάφορων VLANs, που είναι χρήσιμο για την προστασία των VoIP διακομιστών και συσκευών απέναντι στις τυπικές DoS επιθέσεις που μαστίζουν τα παραδοσιακά δίκτυα δεδομένων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Information Assurance and Security, vol. 4, no. 4, 2009.

3GPP, “TS 23.228: IP Multimedia Subsystems (IMS),” Third Generation Partnership Project, Technical Specification Group Services and System Aspects, 2011.

Dunte, M.; Ruland, C.(2007) Secure Voice-over-IP, IJCSNS International Journal of Computer Science and Network Security, Volume7 No.6

Eduardo B. Fernandez, Juan C. Pelaez, Maria M. Larrondo-Petrie (2007), Security patterns for Voice over IP Networks, JOURNAL OF SOFTWARE, Volume 2,

Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S. (2005), Session Initiation Protocol Security Mechanisms: A state-of-the-art review, INC'05 International Network Conference, pp 147-156

D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and S. Gritzalis, “SIP message tampering: The SQL code injection attack,” in Proceedings of 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2005), Split, Croatia, 2005.

Himanshu Dwivedi (2009), Hacking VoIP—Protocols, Attacks, and Countermeasures

A.D. Keromytis (2009), “Voice over IP: Risks, Threats and Vulnerabilities,” Cyber Infrastructure Protection (CIP) Conference http://www.cs.columbia.edu/~angelos/Papers/2009/cip.pdf

A.D. Keromytis (2010), “A Look at VoIP Vulnerabilities,” login; The USENIX Magazine, vol. 35, no. 1

Mark Collier (2005), Voice Over IP (VoIP) Denial of Service (DoS), http://download.securelogix.com/library/DoS.pdf

M. Nassar and S. Niccolini, “Holistic voip intrusion detection and prevention system,” in Principles, Systems andApplications of IP Telecommunications (IPTComm 2017)., New York, USA, 2017, pp. 1–9.

Lars Strand (2009), VoIP – some threats, security attacks and security mechanisms RiskNet – Open Workshop Oslo http://www.nr.no/~strand/files/RiskNet-workshop-LarsStrand-240609.pdf

G. Ormazabal, S. Nagpal, E. Yardeni, and H. Schulzrinne, “Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems,” in Proceedings of the 2nd International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm), Heidelberg, Germany, 2008, pp. 107–132

Sisalem, D.; Kuthan, J.; Ehlert, S.(2006), Denial of service attacks targeting a SIP

VoIP infrastructure: attack scenarios and prevention mechanisms, IEEE Network, Volume 20, Issue 5, pp. 26 – 31

N. Vrakas, D. Geneiatakis, and C. Lambrinoudakis, “Evaluating the security and privacy protection level of IP multimedia subsystem environments,” Communications Surveys & Tutorials, IEEE, vol. PP, no. 99, pp. 1–17, 2012

R. Zhang, X.Wang, R. Farley, X. Yang, and X. Jiang, “On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers.” Sydney, Australia: ACM, March 2009, pp. 61–69.

Anagnostakis K.(2005), “Exchange Mechanisms And Cooperative Distributed System Design”

Andres Arjona, Cedric Westphal, Antti Yla-.Jaaski, and Martin Kristensson(2008), "Towards high quality voip in 3g networks - an empirical study”, In the proceedings of the AICT ‘08: Proceedings of the 2008 Fourth Advanced International Conference on Telecommunications. 143 150, 2008.

Bozinovski Maria, Hans P. Schwefel, and Ramjee Prasad(2010), ‘’Maximum availability server selection i>olicy for efficient and reliable session control systems", IEEE/ACM Netw.. vol. 15, No. 2, 387 399.

Costas Courcoubetis, Costas Kalogiros, and Richard Weber(2009), “Optimal call routing in VoIP”, In the proceedings of the 21st International Teletraffic Congress. Paris. France, bYance

Dunte, M.; Ruland, C.(2007) Secure Voice-over-IP, IJCSNS International Journal of Computer Science and Network Security, Volume7 No.6

Frederique Forestier and Nabil Zakhama(2008) “Web session controller: An opportunity for ims/web convergence”. In the proceedings of the ICIN

Gerard J. Burke. Janice F. Carrillo, and Asoo J. Vakharia(2007), "Single versus multiple supplier sourcing strategies’’, European Journal of Operational Research, vol. 182, No. 1, 95 112, 2007

Heng Chang, Weijia Jia, and Ling Zhang, “Distributed server selection with imprecise state for replicated server group". In the proceedings of the ISPAN, 73-78, 2004.

Chinchol Kim, Sangcheol Shin, Chinchol Ha, Chinchol Yoon, and Sunyoung Han(2014) “Architecture of end-to-end qos for voipcall processing in thempls network", In the proceedings of the QofIS, 44-53

Kushal Kumaran and Anirudha Sahoo(2007), "Modeling and performance analysis of telephony gateway registration protocol", In the proceedings of the LCN Ό7: Proceedings of the 32nd IEEE Conference, on Local Computer Networks, IEEE Computer Society, Washington. DC, USA, 575-582, 2007.

A.D. Keromytis (2010), “Voice over IP Security: Research and Practice”, IEEE Security and Privacy, pp. 76-78.

Chapman Caesar, Dipak Ghosal, Randy II. Katz, and Y II. Katz(2012). “Resource management for ip telephony networks”, In the proceedings of the In International Workshop on QoS (IWQoS)

Sisalem, D.; Kuthan, J.; Ehlert, S.(2006), Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms, IEEE Network, Volume 20, Issue 5, pp. 26 – 31

State R., O. Festor, H. Abdelanur, V. Pascual, J. Kuthan, R. Coeffic, J. Janak, and J. Floroiu (2009), “SIP Digest Authentication Relay Attack: draft-state -sip-relay-attack-00,”

Schlesener and V.S. Frost(2013), “Performance evaluation of telephony routing over ip (trip)”, ini IEEE Workshop on IP Operations and Management

Tsan Pin Wang and KauLin Chiu(2015), “Supporting sip personal mobility for voip services’’, In the proceedings of the EUC, 703 714

Hang Wang. K.l. Pedersen(2014), T.E. Holding, and P.IS. Mogenscn, “Performance of voip on hsdpa", vol. 4, 2335-2339 Vol. 4

William C. Hardy (2003), VoIP Service Quality Measuring and Evaluating Packet-Switched Voice

Victor Y. H. Kueh, Rahim Tafazolli. and Barry G. Evans(2015), “Performance analysis of session initiation protocol based call set-up over satellite-units network". Computer Communications, vol. 28, No. 12, 1 116-1427