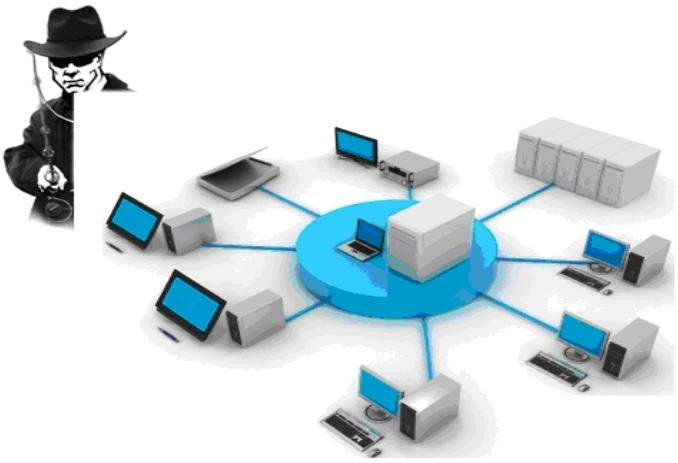
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΔΙΔΑΚΤΙΚΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΣΤΑ IP ΔΙΚΤΥΑ



ΜΠΟΥΜΠΟΥΛΗ ΝΑΥΣΙΚΑ

ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ:
ΚΑΤΣΙΚΑΣ ΣΩΚΡΑΤΗΣ

ΑΘΗΝΑ 2010

ΠΕΡΙΕΧΟΜΕΝΑ

Ευχαριστίες

Για την εκπόνηση της Μεταπτυχιακής Διπλωματικής Εργασίας, θα ήθελα να ευχαριστήσω ιδιαίτερα, τον καθηγητή, κύριο Κάτσικα Σωκράτη, για την αμέριστη βοήθεια του, για το χρόνο που αφιέρωσε σε αυτήν κάνοντας εύστοχες παρατηρήσεις, καθώς και για την πολύ καλή συνεργασία που είχαμε.

Δεν θα μπορούσα, όμως, να παραλείψω να ευχαριστήσω την οικογένειά μου και όλους όσους συνέβαλαν έμμεσα ή άμεσα, είτε προσφέροντας χρήσιμη βοήθεια και υλικό, είτε ψυχολογική στήριξη.

ΕΙΣΑΓΩΓΗ

Στα χρόνια πριν από την εξάπλωση της χρήσης των ηλεκτρονικών υπολογιστών ως εργαλεία επεξεργασίας της πληροφορίας, η διασφάλιση της μυστικότητας, ακεραιότητας και διαθεσιμότητας των σημαντικών πληροφοριών ενός οργανισμού γινόταν μέσω της φυσικής προστασίας, καθώς και μέσω κάποιων διαδικασιών και κανονισμών ασφάλειας. Για παράδειγμα, τα ευαίσθητα έγγραφα κλείνονταν σε ντουλάπες ή χρηματοκιβώτια στιβαρής κατασκευής τα οποία προστατεύονταν από κλειδαριές, ενώ μόνον εξουσιοδοτημένο προσωπικό το οποίο επιλεγόταν αυστηρά, είχε πρόσβαση σε αυτά. Τις τελευταίες δεκαετίες, δύο γεγονότα έχουν αλλάξει δραστικά τις ανάγκες των οργανισμών σε σχέση με την ασφάλεια των πληροφοριών.

Το πρώτο γεγονός είναι η εισαγωγή των υπολογιστών ως εργαλεία αποθήκευσης και επεξεργασίας της πληροφορίας. Η προστασία της πληροφορίας ανάγεται πλέον στην προστασία των αρχείων των υπολογιστών στα οποία είναι αποθηκευμένη η πληροφορία, στον έλεγχο της πρόσβασης στα αρχεία αυτά, καθώς και στην προστασία των προγραμμάτων εκείνων που μπορούν να απειλήσουν την ασφάλεια των αρχείων αυτών. Ο όρος που χρησιμοποιείται για να περιγράψει το σύνολο των εργαλείων και διαδικασιών που έχουν σχεδιασθεί για την προστασία των ηλεκτρονικών δεδομένων είναι "ασφάλεια υπολογιστών" (computer security).

Το δεύτερο γεγονός το οποίο επηρέασε δραστικά τις ανάγκες σε ασφάλεια της πληροφορίας είναι η εισαγωγή των κατανεμημένων συστημάτων και η χρήση δικτύων και τηλεπικοινωνιακών συστημάτων για την μεταφορά δεδομένων μεταξύ υπολογιστών. Ο όρος "ασφάλεια δικτύων" (network security) αναφέρεται στα μέτρα προστασίας των δεδομένων κατά την μεταφορά τους μέσω του δικτύου διασύνδεσης.

Στα πλαίσια της διαχείρισης ενός δικτύου, η διαχείριση ασφάλειας αναφέρεται στην παροχή ασφάλειας σε όλα τα στοιχεία του δικτύου, δηλαδή σε ασφάλεια υπολογιστών και ασφάλεια δικτύου.

Η ιλιγγιώδης ανάπτυξη του διαδικτύου (Ίντερνετ) και κατ' επέκταση η ανάπτυξη του πρωτοκόλλου Internet Protocol (IP) που το υποστηρίζει οριοθετεί νέες εξελίξεις στην αγορά των τηλεπικοινωνιών. Ποιά η δυναμική του πρωτοκόλλου Ίντερνετ (IP) και ποιές οι εφαρμογές του;

Είναι πλέον αναμφισβήτητο ότι το μεγαλύτερο δίκτυο μεταφοράς δεδομένων στον κόσμο είναι το Internet. Με βάση στατιστικές μελέτες, φαίνεται ότι τη χρονιά 2001 θα υπάρχουν περισσότεροι από 100 εκατομμύρια δικτυωμένοι ηλεκτρονικοί υπολογιστές σε περισσότερα από ένα εκατομμύριο δίκτυα, κάνοντας χρήση του διαδικτύου. Το γεγονός αυτό αναβαθμίζει τη θέση του πρωτοκόλλου IP μέσω του οποίου υλοποιείται το διαδίκτυο. Οι παραδοσιακοί τηλεπικοινωνιακοί οργανισμοί καλούνται να προσαρμοστούν στις νέες εξελίξεις και να είναι έτοιμοι να εκμεταλλευτούν τη νέα δυναμική και ανάπτυξη της τεχνολογίας αυτής.

Κεφάλαιο 1ο

Αρχιτεκτονική IP Τηλεφωνίας

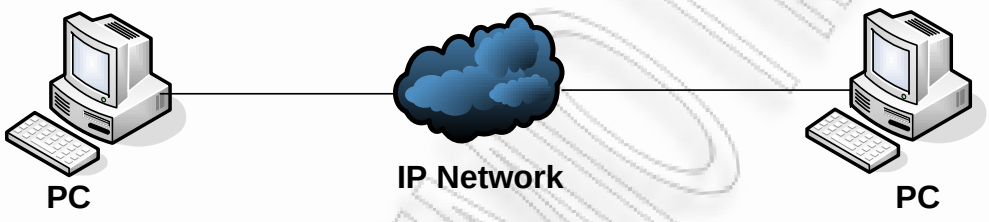
1.1 Γενικά

Ο όρος VoIP αναφέρεται στη μεταφορά φωνής πάνω από δίκτυα που βασίζονται στην τεχνολογία του Internet και πιο συγκεκριμένα στο πρωτόκολλο IP. Το πρωτόκολλο πάνω στο οποίο βασίζεται το Internet δημιουργήθηκε για να υλοποιήσει δίκτυα μεταφοράς δεδομένων. Αυτό σημαίνει ότι ένα έγγραφο που μεταφέρεται μέσω Internet διαχωρίζεται σε μικρά πακέτα δεδομένων και αποστέλλεται μέσω του δικτύου. Όταν το έγγραφο φτάσει στον προορισμό του, τα πακέτα ενώνονται δημιουργώντας ξανά το αρχικό μήνυμα, ώστε αυτό να δοθεί ενιαίο στον παραλήπτη του. Η ίδια λογική εφαρμόζεται και στην περίπτωση που τα δεδομένα που μεταφέρονται αντιστοιχούν σε κάποια φωνητική συνομιλία. Πιο αναλυτικά, φωνή ψηφιοποιείται, διαχωρίζεται σε πακέτα δεδομένων, μεταφέρεται από το δίκτυο μέσω

του IP πρωτοκόλλου και στον προορισμό ανασυντίθεται ώστε να φτάσει στο συνομιλητή. Η VoIP σύνδεση μπορεί να κατηγοριοποιηθεί με βάση τον τύπο των συσκευών που πραγματοποιούν ένα τηλεφώνημα στο διαδίκτυο σε σύνδεση **PC σε PC**, **PC σε τηλέφωνο και τηλέφωνο σε PC, Τηλέφωνο σε Τηλέφωνο.**

Ο όρος PC, μπορεί να χρησιμοποιηθεί για οποιαδήποτε συσκευή ικανή να στείλει φωνή μέσω ενός δικτύου πληροφοριών. Με άλλα λόγια δεν έχει υποχρεωτικά όλα τα χαρακτηριστικά ενός υπολογιστή.

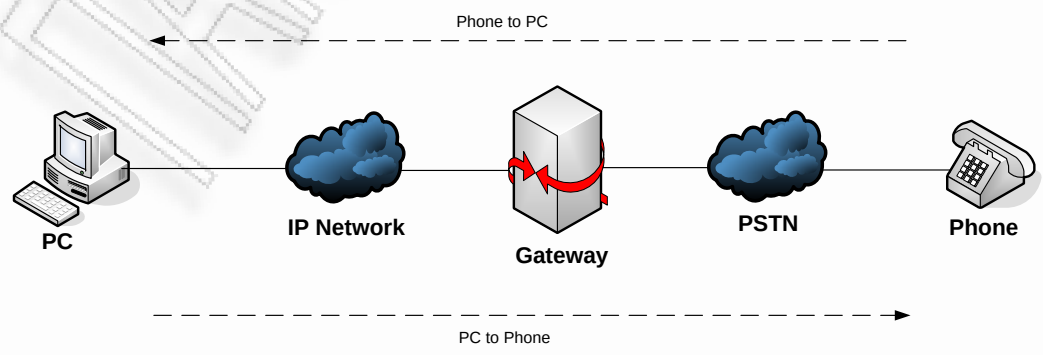
1. PC σε PC



Σχήμα 1

Η σύνδεση αυτή είναι κυρίως για χρήστες οι οποίοι έχουν ήδη πρόσβαση στο διαδίκτυο. Σε αυτή τη περίπτωση υπάρχουν πλεονεκτήματα που μπορούν να προκύψουν από άλλες υπηρεσίες του διαδικτύου, όπως το World Wide Web, το email και τα μηνύματα μέσω Internet.

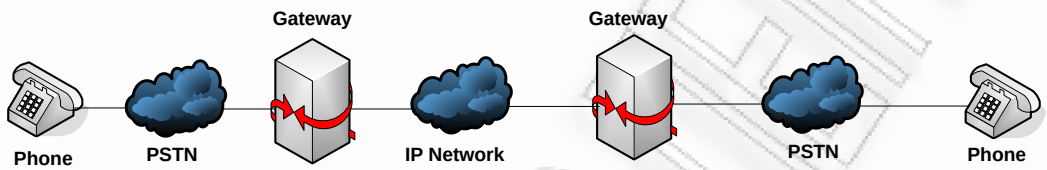
2. PC σε τηλέφωνο και τηλέφωνο σε PC



Σχήμα 2

Δίνεται η δυνατότητα πραγματοποίησης κλήσεων από IP δίκτυο με την βοήθεια μιας πύλης (gateway) προς το εξωτερικό δίκτυο PSTN. Αντίστοιχα και ένας χρήστης του PSTN δικτύου μπορεί να πραγματοποιήσει μια κλήση προς το IP δίκτυο , μέσω της πύλης η οποία είναι υπεύθυνη για την δημιουργία και την ολοκλήρωση μιας κλήσης.

3. Τηλέφωνο σε Τηλέφωνο



Σχήμα 3

Παρέχει την δυνατότητα σε χρήστες του PSTN δικτύου να πραγματοποιήσουνε κλήσεις μεταξύ τους με την χρήση του IP δικτύου μέσω των πυλών (gateways)

1.2 Λειτουργίες VoIP

Είναι πολύ σημαντικό τα μέρη ενός συστήματος VoIP να έχουν τα ίδια χαρακτηριστικά γνωρίσματα με το PSTN δίκτυο, όπως:

- Σηματοδότηση
- Υπηρεσίες βάσεων δεδομένων
- Σύνδεση και αποσύνδεση κλήσης (έλεγχος φορέων)
- Διαδικασίες κωδικοποιητών/αποκωδικοποιητών

1.2.1 Σηματοδότηση

Η σηματοδότηση σε ένα VoIP δίκτυο είναι τόσο κρίσιμη, όσο και στο γνωστό σε όλους μας παραδοσιακό τηλεφωνικό δίκτυο, καθώς ενεργοποιεί και συντονίζει την διαδικασία ολοκλήρωσης μιας κλήσης.

Σε ένα VoIP δίκτυο, η σηματοδότηση ολοκληρώνεται από την ανταλλαγή μηνυμάτων, των οποίων η μορφή καλύπτεται από ένα μεγάλο αριθμό προτύπων πρωτοκόλλων.

1.2.2 Υπηρεσίες Βάσεων Δεδομένων

Οι υπηρεσίες βάσεων δεδομένων είναι ένας τρόπος να βρεθεί ένα ακραίο σημείο (endpoint) και να μεταφραστεί η διευθυνσιοδότηση που χρησιμοποιούν δύο δίκτυα (συνήθως ετερογενή). Για παράδειγμα, τα δίκτυα PSTN χρησιμοποιούν τηλεφωνικούς αριθμούς για να προσδιορίσουν τα ακραία σημεία, ενώ ένα VoIP δίκτυο μπορεί να χρησιμοποιήσει μια διεύθυνση IP (η ανάθεση διευθύνσεων μπόρεσε να ολοκληρωθεί με τη χρήση του DNS) και τους αριθμούς θυρών (ports) για να προσδιορίσει ένα ακραίο σημείο. Αυτές οι χαρτογραφήσεις και μεταφράσεις περιέχονται σε μία βάση δεδομένων ελέγχου κλήσης.

Οι υπηρεσίες που παρέχονται είναι αρκετές, όπως για παράδειγμα, η δυνατότητα εξερχόμενων κλήσεων από τους χρήστες του τηλεφωνικού δικτύου. Πιο αναλυτικά στο κάθε χρήστη μπορεί να δοθεί διαφορετική δυνατότητα πραγματοποίησης εξερχόμενων κλήσεων , όπως Αστική, Υπεραστική ή Διεθνή ή ακόμα και την απαγόρευση κλήσεων προς συγκεκριμένους αριθμούς του PSTN δικτύου.

1.2.3 Σύνδεση και Αποσύνδεση Κλήσης (έλεγχος φορέων)

Η σύνδεση μίας κλήσης μεταξύ δύο ακραίων σημείων πραγματοποιείται με το άνοιγμα περιόδων επικοινωνίας. Στο δίκτυο PSTN, το δημόσιο ή ιδιωτικό switch

συνδέει τα λογικά DS-0 κανάλια μέσω του δικτύου για να ολοκληρώσει τις κλήσεις. Σε μια VoIP εφαρμογή, αυτή η σύνδεση είναι ένα ρεύμα πολυμέσων (audio,video, ή και τα δύο) που μεταφέρεται σε πραγματικό χρόνο. Αυτή η σύνδεση είναι το κανάλι φορέων και αντιπροσωπεύει το audio ή το video που παραδίδεται. Όταν η επικοινωνία ολοκληρωθεί, οι περίοδοι IP επικοινωνίας ελευθερώνονται και εκδίδονται προαιρετικά τα στοιχεία συμπεριφοράς του δικτύου.

1.2.4 Λειτουργίες Κωδικοποιητή/ Αποκωδικοποιητή

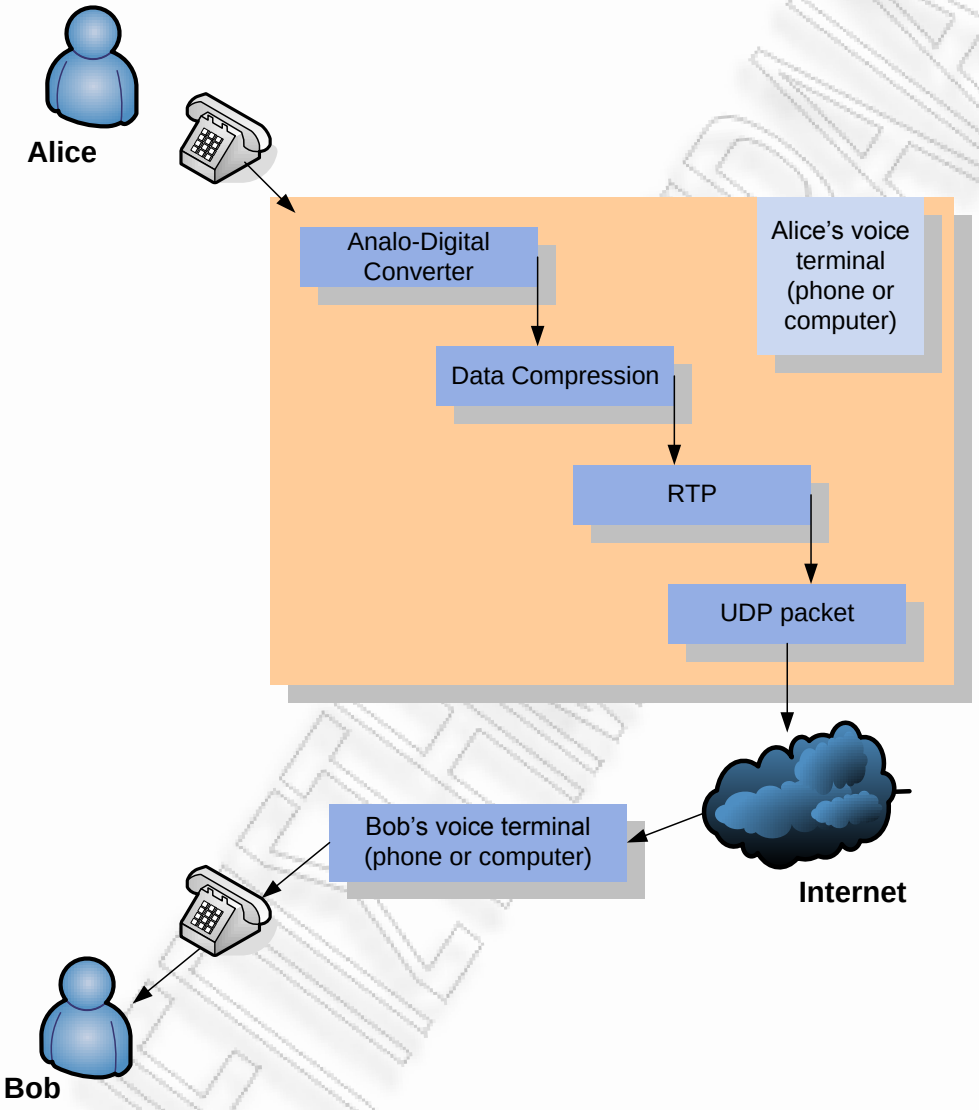
Η διαδικασία μετατροπής των αναλογικών σημάτων σε ψηφιακές πληροφορίες γίνεται με έναν κωδικοποιητή - αποκωδικοποιητή (CODEC). Υπάρχουν πολλοί τρόποι που ένα αναλογικό σήμα φωνής μπορεί να μετασχηματιστεί , οι οποίοι ορίζονται από διάφορα πρότυπα. Οι περισσότερες από τις μετατροπές γίνονται βάσει της παλμοκωδικής διαμόρφωσης (PCM).

1.3 Επισκόπηση στο Χειρισμό Δεδομένων

Η μετάδοση της φωνής πραγματοποιείται, αφού πρώτα έχει πραγματοποιηθεί μια κλήση. Σε ένα συνηθισμένο τηλεφωνικό σύστημα αυτή η διαδικασία περιλαμβάνει το σχηματισμό των ψηφίων του αριθμού που πρόκειται να κληθεί, τα οποία στη συνέχεια υποβάλλονται σε επεξεργασία από το τηλεφωνικό σύστημα, ώστε να πραγματοποιηθεί η κλήση.

Ο χρήστης του VoIP συστήματος πρέπει είτε να πληκτρολογήσει τον αριθμό κλήσης, είτε να επιλέξει τη χρήση ενός Universal Resource Indicator (URI), με τη χρήση του οποίου όμως, μπορεί να προκύψει μια σύνθετη σειρά ανταλλαγής πακέτων, η οποία βασίζεται σε ένα πρωτόκολλο σηματοδότησης VoIP. Το πρόβλημα είναι ότι τα συστήματα ηλεκτρονικών υπολογιστών διακρίνονται χρησιμοποιώντας την IP διεύθυνση τους. Ο χρήστης όμως για να πραγματοποιήσει την κλήση, εισάγει έναν συνηθισμένο αριθμό τηλεφώνου ή ένα URI. Έτσι, ο αριθμός τηλεφώνου ή το

URI θα πρέπει να συνδεθούν με μια IP διεύθυνση, ώστε να ολοκληρωθεί η διαδικασία.



Σχήμα 4: **Voice Data Processing σε ένα VoIP Σύστημα**

Το σχήμα 4 επεξηγεί τη βασική ροή των δεδομένων φωνής μέσα σε ένα σύστημα VoIP. Μόλις ενεργοποιηθεί η κλήση, θα πρέπει να μεταδοθεί χωρίζοντας το σήμα φωνής σε ένα ρεύμα (stream) από πακέτα. Αρχικά μέσω του μετατροπέα (analogue-digital converter) γίνεται η μετατροπή του αναλογικού σήματος φωνής σε ψηφιακό, και στη συνέχεια, επειδή η ψηφιοποιημένη φωνή απαιτεί έναν μεγάλο αριθμό από bits, χρησιμοποιείται ένας αλγόριθμος συμπίεσης για να μειώσει τον όγκο των

δεδομένων που διαβιβάζονται. Τέλος, τα δείγματα φωνής εισάγονται σε πακέτα δεδομένων, ώστε να μεταφερθούν στο διαδίκτυο.

Το πρωτόκολλο για τα πακέτα φωνής είναι το Real-time Transport Protocol (RTP) (RFC 3550). Τα RTP πακέτα έχουν ειδικό πεδίο κεφαλίδας, όπου εκεί φυλάσσονται τα δεδομένα που απαιτούνται για να συγκεντρωθούν εκ νέου, σωστά τα πακέτα σε ένα σήμα φωνής στο άλλο τερματικό. Τα πακέτα φωνής όμως, θα μεταφερθούν ως ωφέλιμο φορτίο από UDP πρωτόκολλα που χρησιμοποιούνται και για τη συνηθισμένη μετάδοση δεδομένων. Με άλλα λόγια, τα πακέτα RTP μεταφέρονται σαν δεδομένα από UDP διαγράμματα, τα οποία στη συνέχεια μπορούν να υποβληθούν σε επεξεργασία από τους συνήθεις κόμβους δικτύων σε όλο το Διαδίκτυο. Στο άλλο τερματικό, η διαδικασία είναι αντίστροφη: τα πακέτα διαχωρίζονται και τίθενται στην κατάλληλη σειρά. Στη συνέχεια, τα ψηφιοποιημένα δεδομένα φωνής εξάγονται από τα πακέτα τα οποία βέβαια είναι ασυμπίεστα. Τέλος, η ψηφιοποιημένη φωνή υποβάλλεται σε επεξεργασία από έναν ψηφιακό σε αναλογικό μετατροπέα (digital-to-analog converter), ώστε να το μετατρέψει σε αναλογικό σήμα για τον ομιλητή.

1.4 Οι Απειλές στην IP Τηλεφωνία

Οι απειλές στα συστήματα επικοινωνιών IP είναι παρόμοιες με τις απειλές των παραδοσιακών συστημάτων τηλεφωνίας, καθώς και με τις απειλές δικτύων δεδομένων.

Οι απειλές αυτές περιλαμβάνουν την *διάσπαση*, η οποία είναι μια επίθεση που αποβάλει ή περιορίζει την δυνατότητα χρησιμοποίησης τηλεφώνων και υπηρεσιών φωνής, το eavesdropping με την οποία εκμαιεύονται εμπιστευτικές ή ιδιωτικές πληροφορίες, η ακατάλληλη χρήση όπου πηγές τηλεφωνίας χρησιμοποιούνται για μη επιχειρηματικούς σκοπούς και η κλοπή υπηρεσιών, στην οποία, οι υπηρεσίες που πληρώνονται από την εταιρεία χρησιμοποιούνται από άλλους.

Καθώς η IP τηλεφωνία χρησιμοποιεί το υπάρχον IP δίκτυο, οι επιθέσεις σε αυτό το δίκτυο δεδομένων είναι πιθανόν να έχουνε επιπτώσεις και στις υπηρεσίες φωνής.

Οι πιο συνηθισμένες απειλές είναι:

Toll Fraud

Αυτή η απειλή αναφέρεται στους εσωτερικούς ή εξωτερικούς χρήστες οι οποίοι χρησιμοποιούν το εταιρικό τηλεφωνικό σύστημα για να πραγματοποιήσουν τις αναρμόδιες κλήσεις. Είναι μια απειλή που μπορεί να πραγματοποιηθεί και σε TDM, αλλά και σε IP δίκτυα.

Denial of Service

Οι επιθέσεις αυτού του είδους έχουν ως σκοπό την μείωση ή την εξάλειψη της ικανότητας ενός συστήματος να προσφέρει τις υπηρεσίες του στους νόμιμους χρήστες. Χαρακτηριστικότερες είναι οι TCP SYN Flooding επιθέσεις, οι επιθέσεις με το γνωστό πρόγραμμα Ping, και οι επιθέσεις με τη χρήση του UDP. Συνήθως, η δυσλειτουργία διατηρείται για ένα αρκετά μεγάλο χρονικό διάστημα μετά το πέρας της επίθεσης.

Επιθέσεις Μεταμφίεσης (Spoofing)

Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, "μεταμφιέζεται" ώστε να αποκτήσει εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Οι χαρακτηριστικότερες επιθέσεις του είδους είναι το IP Spoofing, το DNS (Domain Name System) Spoofing και το ARP (Address Resolution Protocol) spoofing.

IP Spoofing

Ο όρος IP spoofing αναφέρεται στην δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης, ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή.

DNS (Domain Name System) Spoofing

Ο όρος DNS spoofing αναφέρεται στην δημιουργία ενός DNS ο οποίος παραπέμπει σε μια άλλη IP διεύθυνση, από εκείνη που είχε ζητηθεί αρχικά από τον χρήστη.

ARP (Address Resolution Protocol) spoofing

Το ARP spoofing ή ARP poisoning είναι ένας τύπος παραβίασης σε δίκτυο υπολογιστών το οποίο βασίζεται στο πρωτόκολλο ARP.

Ο κακόβουλος χρήστης μπορεί, μεταδίδοντας λανθασμένα πακέτα ARP, να μπερδέψει άλλους host ώστε να στείλουν τα πλαίσια δεδομένων τους σε άλλον υπολογιστή χωρίς να το αντιληφθούν. Μπορεί τότε να παρακολουθήσει την επικοινωνία μεταξύ

- δυο host
- ενός host και ενός υποδικτύου
- ενός host και του Διαδικτύου
- οποιοδήποτε συνδυασμό των παραπάνω παραβιάσεων
- Έχει επίσης την δυνατότητα να αποκλείσει έναν host από ένα δίκτυο

Eavesdropping or Man-in-the-Middle Exploits

Σε τέτοιου είδους επιθέσεις, ένας εσωτερικός χρήστης αντιγράφει την IP διεύθυνση ενός router ή PC, ώστε να κατασκοπεύσει την κίνηση της φωνής και των δεδομένων κατά την διάρκεια μιας συζήτησης. Στην συνέχεια ο χρήστης αντιγράφει γρήγορα τις πληροφορίες και δρομολογεί την κίνηση της φωνής στον προορισμό της ώστε κανείς να μην καταλάβει την υποκλοπή.

Σε όλες τις περιπτώσεις, το τελικό αποτέλεσμα είναι το ίδιο: Το δίκτυο συμβιβάζεται και το εμπιστευτικό στοιχείο τίθεται σε κίνδυνο — προφανώς, μια απαράδεκτη κατάσταση.

Κεφάλαιο 2ο

Αρχές Ασφάλειας στην IP Τηλεφωνία

Λαμβάνοντας υπόψη τους κινδύνους, είναι επιτακτικό να γίνεται μελέτη και εκτίμηση της υποδομής ασφάλειας των εταιρειών, πριν από την εφαρμογή οποιασδήποτε λύσης IP τηλεφωνίας.

Μερικά από τα θεμελιώδη αξιώματα που θα πρέπει να λαμβάνονται υπόψη όταν θέλουμε να προσφέρουμε ασφάλεια σε ένα IP τηλεφωνικό δίκτυο είναι :

- Μια δοκιμασμένη πολιτική ασφαλείας
- Συχνές αξιολογήσεις της ασφάλειας , οι οποίες θα είναι και προγραμματισμένες αλλά και τυχαίες, είναι πολύ σημαντικό να

πραγματοποιούνται για να είναι δυνατή η προστασία απέναντι σε νέες επιθέσεις.

- Η ασφάλεια στην IP τηλεφωνία θα πρέπει να διαχωρίζεται σε επίπεδα ώστε οποιαδήποτε απειλή να μην επηρεάζει ολόκληρο το δίκτυο.
- Η ασφάλεια θα πρέπει να εξετάζει γνωστές και άγνωστες απειλές, καθώς οι εισβολείς συνεχώς εξελίσσουν την επίθεσή τους.
- Μια καλή ασφάλεια IP τηλεφωνίας είναι πάντα εξαρτώμενη από μια καλή ασφάλεια των δεδομένων.
- Η ασφάλεια θα πρέπει να ελέγχει και να απομονώνει τα πάντα και στην συνέχεια επιλεκτικά να επιτρέπει μόνο την επιθυμητή πληροφορία, χρησιμοποιώντας όσες περισσότερες διευκρινίσεις είναι δυνατόν.

2.1 Ζητήματα Ποιότητας Υπηρεσιών (Quality of Service-QoS)

Η υπηρεσία Quality of Service (QoS), παίζει σημαντικό ρόλο στη λειτουργία ενός δικτύου VOIP. Παρόλο που το VOIP είναι πιο οικονομικό και παρέχει κομψότητα στα δίκτυα, εάν δεν μπορέσει να προσφέρει τουλάχιστον την ίδια ποιότητα κλήσης και φωνής με ένα παραδοσιακό τηλεφωνικό δίκτυο, τότε η αξία του θα μειωθεί. Η εφαρμογή των διάφορων μέτρων ασφάλειας, μπορεί να υποβιβάσει το QoS. Αυτό μπορεί να συμβεί είτε από την καθυστέρηση, είτε από το μπλοκάρισμα των κλήσεων που προκαλείται από firewalls, από λανθάνουσα κατάσταση και από το jitter.

Τα ζητήματα ποιότητας ασφαλείας, είναι βασικά στην ασφάλεια του VOIP. Εάν η ποιότητα των υπηρεσιών (QoS) ήταν δεδομένη, τότε τα περισσότερα μέτρα ασφαλείας που εφαρμόζονται στα σημερινά δίκτυα δεδομένων θα μπορούσαν να χρησιμοποιηθούν και στα δίκτυα VOIP. Λόγω όμως της χαμηλής ανοχής τους στη διάσπαση και στην απώλεια πακέτων, πολλά μέτρα ασφαλείας που εφαρμόζονται στα παραδοσιακά δίκτυα δεδομένων δεν ισχύουν ακριβώς με την υπάρχουσα μορφή τους.

Τα κυριότερα ζητήματα QoS που συνδέονται με δίκτυα VOIP και επηρεάζεται η ασφάλεια είναι τα ακόλουθα:

2.1.1 Λανθάνουσα κατάσταση

Η λανθάνουσα κατάσταση σε ένα VOIP δίκτυο αναφέρεται στο χρόνο που χρειάζεται η μετάδοση φωνής από την πηγή της στον προορισμό της. Το ιδανικό είναι να κρατήσουμε τη λανθάνουσα κατάσταση όσο το δυνατόν χαμηλότερη. Το ITU-T Recommendation G.114 επιβάλλει μία σειρά από χρονικούς περιορισμούς για τη μονόδρομη λανθάνουσα κατάσταση. Το ανώτατο όριο εύρους είναι 150 ms για μονόδρομη κυκλοφορία.

Οι κλήσεις μέσω VOIP πρέπει να επιτύχουν εύρος 150 ms ώστε να μιμηθούν επιτυχώς το QoS που παρέχουν τα σημερινά τηλέφωνα. Ο χρονικός περιορισμός αφήνει πολύ μικρό περιθώριο λάθους στην παράδοση πακέτων. Επιπλέον, τοποθετεί έναν αυθεντικό περιορισμό στην ποσότητα ασφαλείας που μπορεί να προστεθεί σε ένα VOIP δίκτυο.

Η καθυστέρηση δεν περιορίζεται στα τερματικά του συστήματος. Κάθε hop μέσα στο δίκτυο εισάγει μια νέα καθυστέρηση αναμονής και ενδεχομένως και μια καθυστέρηση επεξεργασίας, εάν πρόκειται για κάποιο σημείο ελέγχου ασφαλείας (δηλ. firewall ή σημείο κρυπτογράφησης/αποκρυπτογράφησης). Επίσης, τα μεγάλα πακέτα τείνουν να προκαλούν συμφόρηση στο εύρος ζώνης και να αυξάνουν τη λανθάνουσα κατάσταση. Λαμβάνοντας υπ' όψη τα παραπάνω, το VOIP λειτουργεί καλύτερα με μικρά πακέτα αφού έτσι διατηρείται η λανθάνουσα κατάσταση σε χαμηλά επίπεδα.

2.1.2 Το Jitter

Το Jitter αναφέρεται στις ανομοιόμορφες καθυστερήσεις πακέτων. Συχνά προκαλείται από καταστάσεις χαμηλού εύρους ζώνης σε δίκτυα VOIP και μπορεί να επηρεάσει αρκετά την ποιότητα μετάδοσης της πληροφορίας. Αυτή η ανομοιομορφία στις καθυστερήσεις μπορεί να είναι καταστρεπτικότερη για το QoS από ότι οι ίδιες οι καθυστερήσεις. Το Jitter μπορεί να αναγκάσει τα πακέτα να φτάσουν σε μία ακολουθία και να υποβληθούν σε επεξεργασία .

Ένα πρωτόκολλο που χρησιμοποιείται για να μεταφέρει τη φωνή είναι το RTP. Είναι βασισμένο στο UDP και γι αυτό τα πακέτα εκτός ακολουθίας δεν συγκεντρώνονται εκ νέου στο επίπεδο πρωτοκόλλου. Ωστόσο, το RTP επιτρέπει στις εφαρμογές να ξανακάνουν την παραγγελία χρησιμοποιώντας τις ακολουθίες sequence number και timestamp.

Ένας τρόπος για τον έλεγχο του jitter στα τερματικά του VOIP είναι η χρήση ενός απομονωτή (buffer). Ένας τέτοιος όμως απομονωτής θα πρέπει να απελευθερώνει πακέτα φωνής τουλάχιστον κάθε 150 ms (συνήθως πολύ πιο γρήγορα, λαμβάνοντας υπ' όψη και την καθυστέρηση μεταφοράς), έτσι οι ανομοιομορφίες στις καθυστερήσεις θα πρέπει να είναι οριακές.

Στο ζήτημα της εφαρμογής όμως των απομονωτών, υπάρχει αβεβαιότητα στο κατά πόσο ένα πακέτο που λείπει, απλά καθυστερεί να φτάσει για μεγάλο χρονικό διάστημα ή στην ουσία έχει χαθεί. Εάν το jitter δεν είναι ομαλό, τότε το σύστημα δεν μπορεί να χρησιμοποιήσει τους προηγούμενους χρόνους καθυστέρησης ως δείκτες για τη θέση ενός πακέτου που λείπει. Αυτό αφήνει το σύστημα εκτεθειμένο στη συγκεκριμένη συμπεριφορά εφαρμογής σχετικά με ένα τέτοιο πακέτο.

Επίσης, το Jitter μπορεί να ελεγχθεί σε όλο το δίκτυο VOIP με τη χρησιμοποίηση routers, firewalls και άλλες δικτυακές συσκευές που υποστηρίζουν QoS. Αυτές οι συσκευές επεξεργάζονται και περνούν πιο σύντομα τα πακέτα VOIP επείγουσας κυκλοφορίας απ΄ότι τα λιγότερο επείγοντα πακέτα δεδομένων.

Μία άλλη μέθοδος για την μείωση της καθυστέρησης, είναι να μειώσουμε το jitter με το να κάνουμε όσο το δυνατόν πιο αποδοτική χρήση του εύρους ζώνης. Αυτή η μέθοδος αντιτίθεται με μερικά μέτρα ασφαλείας στο VOIP. Οι απαιτήσεις επεξεργασίας του IPsec μπορεί να αυξήσουν τη λανθάνουσα κατάσταση, περιορίζοντας κατά συνέπεια το αποτελεσματικό εύρος ζώνης και συμβάλλοντας στην αύξηση του jitter.

Το αποτελεσματικό εύρος ζώνης περιορίζεται όταν τα πακέτα επεκτείνονται με νέες κεφαλίδες. Στην κανονική κυκλοφορία IP, αυτό το πρόβλημα είναι αμελητέο δεδομένου ότι η αλλαγή στο μέγεθος του πακέτου είναι πολύ μικρή σε σχέση με το ίδιο το μέγεθος των πακέτων.

Επειδή όμως το VOIP χρησιμοποιεί πολύ μικρά πακέτα, ακόμη και μια ελάχιστη αύξηση θα είναι σημαντική. Αυτό συμβαίνει επειδή η αύξηση θα εξαπλώνεται σε όλα τα πακέτα και έτσι το VOIP θα στέλνει πάρα πολλά τέτοια μικρά πακέτα. Καθώς το παράθυρο παράδοσης για ένα πακέτο VOIP είναι πολύ μικρό, αυτό έχει σαν αποτέλεσμα να είναι ακόμα πιο μικρή η αποδεκτή καθυστέρηση των πακέτων. Έτσι, αν και ενδιαφερόμαστε για την ασφάλεια, η απώτατη προσοχή θα πρέπει να δοθεί στη βεβαίωση, ότι οι καθυστερήσεις στις παραδόσεις πακέτων που προκαλούνται από τις συσκευές ασφαλείας παραμένουν ομοιόμορφες σε όλο το ρεύμα κυκλοφορίας (bitstream). Η εφαρμογή των συσκευών που υποστηρίζουν το QoS και η βελτίωση της αποδοτικότητας του εύρους ζώνης με τη συμπίεση των κεφαλίδων, επιτρέπει την πιο ομαλή καθυστέρηση των πακέτων σε ένα ασφαλές δίκτυο VOIP.

2.1.3 Απώλεια Πακέτων

Το VOIP είναι εξαιρετικά αδιάλλακτο ως προς την απώλεια πακέτων. Η απώλεια πακέτων μπορεί να προκύψει από αυξημένη λανθάνουσα κατάσταση σε μια ομάδα πακέτων που φτάνει καθυστερημένα και πρέπει να απορριφθεί υπέρ των νεότερων πακέτων. Επίσης μπορεί να ευθύνεται και το jitter αφού όταν φτάσει ένα πακέτο και τα περιβάλλοντα πακέτα του έχουν επεξεργαστεί από τον απομονωτή, το λαμβανόμενο πακέτο καθίσταται άχρηστο.

Τα επιπλέον ζητήματα που υπάρχουν σχετικά με την απώλεια πακέτων, εκτός από τα ζητήματα απώλειας πακέτων που συνδέθηκαν ήδη με τα δίκτυα δεδομένων, έχουν να κάνουν με το όταν ένα πακέτο δεν παραδίδεται καθόλου. Το πρόβλημα αυτό οφείλεται στην εμπιστοσύνη του VOIP στο πρωτόκολλο RTP, που χρησιμοποιεί το αναξιόπιστο UDP για τη μεταφορά, και έτσι δεν εγγυάται την παράδοση πακέτων.

Εντούτοις, οι χρονικοί περιορισμοί δεν επιτρέπουν να χρησιμοποιηθεί ένα αξιόπιστο πρωτόκολλο όπως το TCP, καθώς ώσπου να αναφερθεί ότι ένα πακέτο λείπει, να αναμεταδοθεί, και να παραληφθεί, οι χρονικοί περιορισμοί για QoS μπορεί να έχουν λήξει.

Το θετικό είναι ότι τα πακέτα VOIP είναι πολύ μικρά και περιέχουν ένα ωφέλιμο φορτίο μόνο 10-50 bytes, που είναι περίπου 12.5-62.5 ms, με τις περισσότερες εφαρμογές να τείνουν προς την συντομότερη ακολουθία. Η απώλεια ενός τέτοιου μικρού ποσού δεν είναι ευδιάκριτη ή τουλάχιστον ικανή παραπόνων για έναν χρήστη του VOIP.

Το αρνητικό όμως είναι ότι αυτά τα πακέτα συνήθως δεν χάνονται μεμονωμένα. Η συμφόρηση εύρους ζώνης και άλλες τέτοιες αιτίες της απώλειας πακέτων, τείνουν να έχουν επιπτώσεις σε όλα τα πακέτα που παραδίδονται γύρω από το ίδιο χρονικό διάστημα.

Έτσι, αν και η απώλεια ενός πακέτου είναι αρκετά ανακόλουθη, πιθανολογούμε ότι με την απώλεια ενός πακέτου συνεπάγεται η απώλεια διάφορων άλλων, πράγμα που υποβιβάζει σοβαρά την ποιότητα της υπηρεσίας σε ένα δίκτυο VOIP.

Σε μια σύγκριση της ποιότητας του VOIP έναντι του παραδοσιακού switched δικτύου, παρατηρείται ότι ακόμη και ένα αρκετά μικρό ποσοστό χαμένων πακέτων θα μπορούσε να ωθήσει το QoS του δικτύου σε χαμηλότερο επίπεδο απ' ότι αναμένουν οι χρήστες στις παραδοσιακές τους τηλεφωνικές γραμμές.

Σε κάθε κωδικοποιητή-αποκωδικοποιητή που έχει μελετηθεί, υπήρξε έντονη δυσαρέσκεια των χρηστών όταν η λανθάνουσα κατάσταση έφτανε τα 150 ms. Βέβαια ακόμη και με λανθάνουσα κατάσταση λιγότερο από 150 ms, μια απώλεια πακέτων 5% ανάγκαζε την κυκλοφορία στο VOIP που κωδικοποιήθηκε με G.711 (διεθνή πρότυπα για την κωδικοποίηση του τηλεφωνικού ήχου σε ένα ρεύμα (stream) 64 kbps) να μειωθεί κάτω από τα επίπεδα QoS του PSTN, ακόμη και με ένα σχέδιο απόκρυψης απώλειας πακέτων. Ομοίως, οι απώλειες 1% και 2% που κωδικοποιήθηκαν με G.723.1 (για πολύ χαμηλό ρυθμό συμπίεσης ποσοστού bits) και

G.729A (για τη συμπίεση φωνής σε ένα ρεύμα (stream) 8kbps) αντίστοιχα ήταν αρκετές ώστε να μειωθεί η ποιότητα στα δίκτυα κάτω από αυτό το κατώτατο όριο. Με απώλειες 3 % και 4 % αντίστοιχα, η απόδοση αυτών των δικτύων οδήγησε σε μεγάλο αριθμό δυσαρεστημένων χρηστών.

Συνεπώς τα "ανεκτά" ποσοστά απώλειας είναι μέσα σε 1-3% και η ποιότητα γίνεται ανυπόφορη όταν χάνονται περισσότερο από 3% των πακέτων φωνής. Επίσης τα μεγαλύτερα ποσοστά συμπίεσης ωφέλιμων φορτίων οδηγούν σε μια υψηλότερη ευαισθησία στην απώλεια πακέτων. Αυτό αποκαθίσταται με την εφαρμογή σχεδίων διορθώσεων λάθους και απόκρυψης απώλειας πακέτων, με αποτέλεσμα ένα δίκτυο VOIP να είναι λιγότερο ευαίσθητο στην απώλεια πακέτων.

Στα παραπάνω βέβαια, δε λαμβάνονται υπ' όψη τα ποικίλα μεγέθη πακέτων και διάφορες άλλες ιδιότητες που μπορούν να έχουν επιπτώσεις στη σχέση μεταξύ της απώλειας πακέτων και του QoS.

Παρά την αδυναμία χρησιμοποίησης ενός εγγυημένου πρωτοκόλλου παράδοσης όπως το TCP, υπάρχουν μερικές λύσεις για το πρόβλημα απώλειας πακέτων. Δεν μπορεί κανείς να εγγυηθεί ότι όλα τα πακέτα παραδίδονται, αλλά εάν το εύρος ζώνης είναι διαθέσιμο, η αποστολή των περιττών πληροφοριών μπορεί να ακυρώσει την πιθανότητα της απώλειας. Τέτοιο εύρος ζώνης δεν είναι πάντα προσιτό και οι περιττές πληροφορίες θα πρέπει να υποβληθούν σε επεξεργασία, εισάγοντας ακόμη περισσότερη λανθάνουσα κατάσταση στο σύστημα και ενδεχομένως ακόμα μεγαλύτερη απώλεια πακέτων.

Οι νεότεροι κωδικοποιητές-αποκωδικοποιητές όπως το Internet Low Bit-rate Codec (iLBC) ολοένα και αναπτύσσονται ως προς την ποιότητα φωνής και ως προς την υπολογιστική πολυπλοκότητα G.729A και παρέχουν αυξημένη ανοχή στην απώλεια πακέτων.

2.1.4 Εύρος Ζώνης και Αποτελεσματικό Εύρος Ζώνης

Σε οποιοδήποτε δίκτυο, η προφανής πρώτη ανησυχία είναι εάν το δίκτυο είναι διαθέσιμο για χρήση. Δεδομένου ότι ένα δίκτυο μπορεί να χωριστεί σε κόμβους και σε συνδέσεις μεταξύ των κόμβων όπου η κυκλοφορία ρέει, η αναζήτηση για ένα διαθέσιμο δίκτυο έχει να κάνει με τη διαθεσιμότητα κάθε κόμβου και τη διαθεσιμότητα κάθε πορείας μεταξύ των κόμβων.

Η συμφόρηση εύρους ζώνης μπορεί να προκαλέσει την απώλεια πακέτων και ένα πλήθος άλλων προβλημάτων στο QoS. Κατά συνέπεια, η κατάλληλη προφύλαξη και η σωστή κατανομή εύρους ζώνης είναι ουσιαστικές για την ποιότητα VOIP. Ένα από τα πλεονεκτήματα του VOIP, είναι ότι τα δεδομένα και η φωνή μοιράζονται τα ίδια καλώδια. Ταυτοχρόνως όμως, μπορεί να είναι πρόβλημα για τους χρήστες, αφού θα πρέπει να διαθέτουν το απαραίτητο εύρος ζώνης και για τα δύο δίκτυα σε ένα σύστημα που σχεδιάστηκε κανονικά για ένα. Η συμφόρηση του δικτύου αναγκάζει τα πακέτα να περιμένουν τη σειρά τους σε ουρά, γεγονός το οποίο συμβάλλει μετέπειτα στην αύξηση της λανθάνουσας κατάστασης του συστήματος. Επίσης το χαμηλό εύρος ζώνης μπορεί να συμβάλει στις ανομοιόμορφες καθυστερήσεις (jitter).

Εξαιτίας αυτών των ζητημάτων, οι υποδομές των δικτύων VOIP θα πρέπει να παρέχουν το υψηλότερο πιθανό ποσοστό εύρους ζώνης. Στο τοπικό δίκτυο LAN, αυτό σημαίνει ότι είναι απαραίτητη η ύπαρξη σύγχρονων switches που τρέχουν στα 100M bit/sec και μαζί με άλλες αρχιτεκτονικές βελτιώσεις θα μειωθούν τα προβλήματα μέσα στο LAN.

Εάν η λανθάνουσα κατάσταση δικτύων παραμένει κάτω από 100 msec, τότε το μέγιστο jitter δε θα είναι ποτέ περισσότερο από 40 msec και κατά συνέπεια δεν θα υπάρχει απώλεια πακέτων. Με εξασφαλισμένες αυτές τις ιδιότητες, μπορεί να υπολογιστεί το απαραίτητο εύρος ζώνης στο τοπικό δίκτυο LAN για τη χειρότερη περίπτωση, χρησιμοποιώντας τις στατιστικές που συνδέονται με τη χειρότερη περίπτωση συμφόρησης εύρους ζώνης κωδικοποιητή-αποκωδικοποιητή. Αυτό είναι

εύκολο για τις κλήσεις στο τοπικό LAN, αλλά η χρήση ενός WAN περιπλέκει τα θέματα.

Η χρήση εύρους ζώνης ποικίλλει σημαντικά σε ένα WAN. Έτσι απαιτείται μία πιο σύνθετη μεθοδολογία, ώστε να υπολογιστεί η απαραίτητη χρήση εύρους ζώνης. Παρακάτω ακολουθεί μια ανάλυση του συνολικού εύρους ζώνης που απαιτείται, όσον αφορά την ποσότητα κυκλοφορίας και το ποσοστό ροής του.

Οι μέθοδοι για τον περιορισμό του εύρους ζώνης στο VOIP περιλαμβάνουν την κεφαλίδα συμπίεσης στο RTP και το Voice Activity Detection (VAD). Η συμπίεση στο RTP συμπυκνώνει την κυκλοφορία ρευμάτων τόσο, ώστε να χρησιμοποιείται λιγότερο εύρος ζώνης. Βέβαια, ένα ανεπαρκές σχέδιο συμπίεσης μπορεί να προκαλέσει λανθάνουσα κατάσταση ή κακή ποιότητα της φωνής, προκαλώντας έτσι μια γενική μείωση του QoS. Το VAD αποτρέπει τη μετάδοση των κενών πακέτων φωνής (δηλ. όταν δεν μιλά ένας χρήστης, η συσκευή του δεν στέλνει τον λευκό θόρυβο). Πάντως, εξ ορισμού το VAD επηρεάζει το jitter προκαλώντας στο σύστημα ανώμαλη παραγωγή πακέτων.

Οι απαιτήσεις εύρους ζώνης που τίθενται, σχεδιάζονται για ένα βασικό σύστημα VOIP. Η προσθήκη περιορισμών ασφαλείας, αυξάνει σημαντικά τη χρήση εύρους ζώνης, προκαλώντας την αύξηση της λανθάνουσας κατάστασης και του jitter και με αυτόν τον τρόπο υποβιβάζεται το γενικό QoS του δικτύου. Επιπλέον, αυτές οι απαιτήσεις δεν λαμβάνουν υπ' όψη την ετερογενή ροή των δεδομένων πέρα από το δίκτυο. Δεδομένου ότι τα ρεύματα φωνής και δεδομένων μοιράζονται το ίδιο πεπερασμένο εύρος ζώνης και τα ρεύματα δεδομένων τείνουν να περιέχουν πολύ μεγαλύτερα πακέτα από ότι του VOIP, τα σημαντικά ποσά δεδομένων μπορούν να προκαλέσουν πρόβλημα στο δίκτυο και να αποτρέψουν την κυκλοφορία φωνής να φτάσει έγκαιρα στον προορισμό της.

Για αυτόν τον λόγο, οι περισσότερες νέες συσκευές hardware επεκτάθηκαν στο να υποστηρίζουν το QoS σε δίκτυα VOIP. Αυτές οι συσκευές, όπως οι routers και τα firewalls, χρησιμοποιούν IP πρωτόκολλα του Type of Service (ToS) για να στείλουν την κυκλοφορία του VOIP κατευθείαν, πριν από κυκλοφορία των δεδομένων που δεν

επείγουν χρονικά. Οι τηλεφωνικές συσκευές VOIP συχνά περιλαμβάνουν τα χαρακτηριστικά γνωρίσματα του QoS.

Εκτός από το διαθέσιμο εύρος ζώνης του συστήματος που επηρεάζεται από την εισαγωγή μέτρων ασφαλείας, υποτιμάται σημαντικά και το αποτελεσματικό εύρος ζώνης. Το αποτελεσματικό εύρος ζώνης καθορίζεται ως "το ποσοστό του εύρους ζώνης με τα πραγματικά στοιχεία σε συνάρτηση με το συνολικό εύρος ζώνης που χρησιμοποιείται". Η εισαγωγή του IPsec ή άλλων μορφών κρυπτογράφησης οδηγεί σε μια πολύ μεγαλύτερη κεφαλίδα στην αναλογία ωφέλιμου φορτίου για κάθε πακέτο και αυτό μειώνει το αποτελεσματικό εύρος ζώνης, δεδομένου ότι ο ίδιος αριθμός πακέτων (αλλά μεγαλύτερου μεγέθους) χρησιμοποιείται για να μεταφέρει το ίδιο ποσό στοιχείων. Οι συνέπειες της μείωσης του αποτελεσματικού εύρους ζώνης, έχει ως αποτέλεσμα τη μείωση του ρυθμού απόδοσης και την αύξηση της λανθάνουσας κατάστασης.

2.1.5 Η Ανάγκη για την Ταχύτητα

Το κλειδί για την αποκατάσταση των ζητημάτων του QoS, όπως η λανθάνουσα κατάσταση και η συμφόρηση του εύρους ζώνης, είναι η ταχύτητα. Εξ ορισμού, μεγαλύτερος ρυθμός απόδοσης, σημαίνει μείωση της λανθάνουσας κατάστασης και κατά συνέπεια μείωση των πιθανοτήτων της βαριάς μορφής συμφόρησης του εύρους ζώνης. Η λανθάνουσα κατάσταση που συχνά συνδέεται με τους στόχους στα δίκτυα δεδομένων δεν θα επιτευχθεί.

Για τη βελτίωση της απόδοσης της παραγωγής λανθάνουσας κατάστασης χρησιμοποιούμε firewall/NAT και κρυπτογράφηση / αποκρυπτογράφηση της κυκλοφορίας. Παραδοσιακά είναι δύο από τους πιο αποτελεσματικούς τρόπους των διαχειριστών για την προστασία των δικτύων τους. Είναι όμως και δύο από τους μέγιστους συνεισφέροντες στη συμφόρηση δικτύων και την καθυστέρηση του ρυθμού απόδοσης.

Η παρεμβολή των παραδοσιακών αντιπυρικών ζωνών και προϊόντων κρυπτογράφησης σε ένα δίκτυο VOIP δεν είναι εφικτή, ιδιαίτερα όταν

ενσωματώνεται στα υπάρχοντα δίκτυα δεδομένων. Αντ' αυτού, οι λύσεις αυτές θα πρέπει να προσαρμοστούν στην υποστήριξη της ασφάλειας. Στη συνέχεια θα αναφερθούμε στη σύγκρουση μεταξύ των απαιτήσεων ταχύτητας του QoS και στην επιβράδυνση που συνεπάγεται με αυτά τα παραδοσιακά μέτρα ασφαλείας.

2.1.6 Διακοπή Ρεύματος και Εφεδρικά Συστήματα

Τα συμβατικά τηλέφωνα λειτουργούν με 48 volts που παρέχονται από την ίδια τη τηλεφωνική γραμμή και για αυτό το λόγο συνεχίζουν να λειτουργούν ακόμη και κατά τη διάρκεια μιας διακοπής ρεύματος. Οι περισσότεροι χρήστες χρησιμοποιούν PBX συστήματα μαζί με τα συμβατικά τηλέφωνά τους. Αυτό σημαίνει ότι απαιτούνται εφεδρικά συστήματα τροφοδοσίας, έτσι ώστε να συνεχίζουν να λειτουργούν και κατά τη διάρκεια μιας διακοπής ρεύματος. Αυτά τα εφεδρικά συστήματα θα συνεχίσουν να είναι απαραίτητα και με το VOIP και σε πολλές περιπτώσεις θα πρέπει να επεκταθούν.

Μία λύση είναι η ύπαρξη ενός οργανισμού που θα έχει ένα μη διακοπτόμενο συστήματα τροφοδοσίας για το δίκτυο δεδομένων και τους υπολογιστές χρηστών. Έτσι θα μπορεί να παρέχει ένα μεγάλο μέρος της τροφοδοσίας που απαιτείται για να συνεχίσει η επικοινωνία κατά τη διάρκεια οποιασδήποτε διακοπής ρεύματος. Αυτό όμως απαιτεί μια προσεκτική αξιολόγηση και να εξασφαλιστεί ότι η εφεδρική τροφοδοσία που θα διατίθεται, θα είναι επαρκής και για το VOIP αλλά και για κάθε υπολογιστή.

Στο κόστος θα πρέπει να συμπεριληφθεί η ηλεκτρική δύναμη ώστε να φορτίζονται οι μπαταρίες UPS, οι περιοδικές δαπάνες συντήρησης για τα εφεδρικά συστήματα ηλεκτρικής παραγωγής και η αντικατάσταση των μπαταριών. Εάν για έκτακτη ανάγκη χρειάζεται εφεδρική δύναμη για περισσότερο από μερικές ώρες, θα απαιτηθεί η χρήση ηλεκτρικών γεννητριών. Οι δαπάνες για τις γεννήτριες περιλαμβάνουν τις εγκαταστάσεις καυσίμων και αποθήκευσής τους και το κόστος της διάθεσης καυσίμων μετά τη λήξη του χρόνου αποθήκευσης.

2.1.7 Επιπτώσεις της Ποιότητα των Υπηρεσιών λόγω της Ασφάλειας

Οι αυστηρές απαιτήσεις απόδοσης του VOIP έχουν σημαντικές επιπτώσεις στην ασφάλεια, ιδιαίτερα σε ζητήματα denial of service (DoS). Τα συνήθη προβλήματα του VOIP (δηλ. υπερχείλιση των ειδικά επεξεργασμένων μηνυμάτων SIP) μπορούν να οδηγήσουν σε DoS πολλών VOIP συσκευών. Για παράδειγμα, τα τερματικά τηλέφωνα SIP μπορεί να παγώσουν και να καταστραφούν κατά την προσπάθεια να επεξεργαστούν ένα υψηλό ποσοστό κυκλοφορίας πακέτων SIP.

Επίσης οι proxy servers μπορούν να μη λειτουργήσουν σωστά με σήματα κατώτερα του 1Mb/sec. Γενικά, το ποσοστό πακέτων που συσσωρεύονται μπορεί να ασκήσει περισσότερη επίδραση από ότι το εύρος ζώνης δηλ. ένα υψηλό ποσοστό πακέτων να οδηγήσει σε ένα DoS ακόμα κι αν το εύρος ζώνης που καταναλώνεται είναι χαμηλό.

2.2 Μέθοδοι Ασφάλειας στην IP Τηλεφωνία

Οι διαχειριστές μπορούν να δημιουργήσουν τα σωστά θεμέλια για την ασφάλεια στην IP τηλεφωνία με το να ελέγξουν τα παρακάτω :

- Υποδομή δικτύου
- Εξοπλισμό IP τηλεφωνίας
- Διαδικασίες αυθεντικοποίησης και κρυπτογράφησης στην IP τηλεφωνία

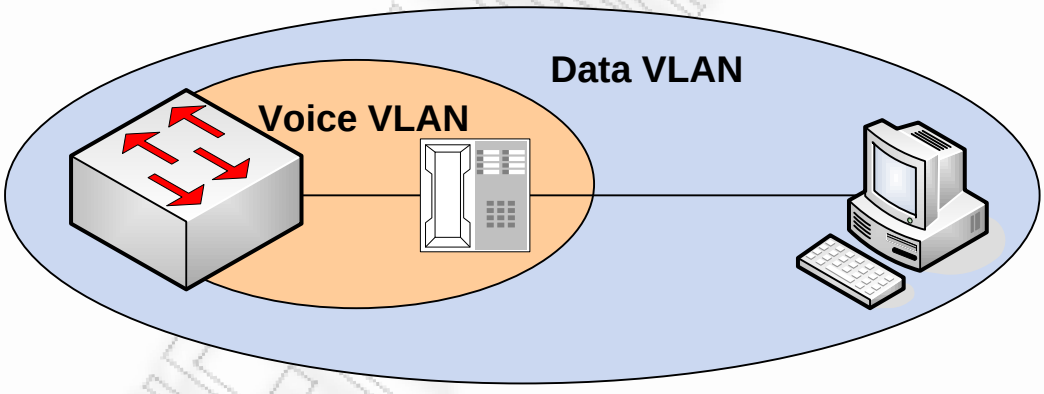
2.2.1 Ασφάλεια στην Υποδομή Δικτύου

Για την ασφάλεια στις υπηρεσίες δεδομένων, φωνής και video απαιτείται ο συνδυασμός των παραδοσιακών τεχνολογιών με τις νέες τεχνολογίες των δικτύων υπηρεσιών φωνής.

1. Διαχωρισμός Δεδομένων - Φωνής σε εικονικά δίκτυα (VLANs)

Για την χρήση τους θα πρέπει να υπάρχει υποστήριξη VLAN από τις δικτυακές συσκευές του δικτύου. Τα πλεονεκτήματά τους είναι η μείωση της κίνησης στο δίκτυο, η αύξηση της ασφάλειας και η μείωση σε απαιτήσεις υλικού.

Παρόλο που στην IP τηλεφωνία και η φωνή, αλλά και τα δεδομένα, χρησιμοποιούν το ίδιο φυσικό δίκτυο, θα πρέπει να διαχωριστεί η κίνηση της φωνής από εκείνης των δεδομένων, με την δημιουργία vlan. Αυτό παρέχει καλύτερη διαφάνεια και διαχείριση στην κίνηση της φωνής , καθώς επίσης και τη δυνατότητα να δώσει προτεραιότητα στην καθυστέρηση της κυκλοφορίας της φωνής χρησιμοποιώντας την ποιότητα της υπηρεσίας (QoS). Επιπλέον ο διαχωρισμός αυτός , μειώνει την πιθανότητα επίθεσης στο δίκτυο της φωνής, καθώς δεν μπορεί να διακριθεί η επικοινωνία μέσω φωνής σε διαφορετικά vlan.



Σχήμα 5

2. Χρήση εξελιγμένων firewalls

Τα firewalls έχουν την δυνατότητα να εμποδίσουν ιούς (viruses), worms, trojan horses και άλλες επιθέσεις στο τηλεφωνικό δίκτυο. Δίνει την δυνατότητα στον υπολογιστή να μας ειδοποιήσει ότι δέχεται κάποια επίθεση. Μπορούν να μας παρουσιάσουν αναλυτικά στατιστικά στοιχεία σχετικά με την κίνηση από και προς

τον υπολογιστή μας, καθώς και να εμποδίσουν κάποιο πρόγραμμα τύπου dialer από το να πραγματοποιήσει τηλεφωνικές κλήσεις χωρίς τη θέλησή μας.

3. Ασφάλεια Διαχείρισης και Διοίκησης

Στα στοιχεία που αποτελούν ένα τηλεφωνικό δίκτυο όπως δρομολογητές (routers), switches και firewalls, θα πρέπει να χρησιμοποιηθούν *transport security (TLS) ή Secure Shell (SSH) κρυπτογράφηση, για την αποφυγή πρόσβασης στην* διαμόρφωση των πληροφοριών ώστε να μην δημιουργηθούν διάφορα προβλήματα στο δίκτυο.

4. Ασφάλεια Απομακρυσμένων Γραφείων

Η απομακρυσμένη υποστήριξη στην IP τηλεφωνία πρέπει να τηρεί τους κανόνες ασφαλείας ώστε να παρέχει ακεραιότητα δεδομένων. Η ασφάλεια στις συνδέσεις μεταξύ headquarters και απομακρυσμένων γραφείων μπορεί να δημιουργηθεί, χρησιμοποιώντας τεχνολογίες ασφάλειας δικτύων όπως *voice- and video-enabled VPN (V3PN).*

Το *V3PN* διασφαλίζει τη σύνδεση η οποία παρέχεται από τα site-to-site IPSec VPNs να μεταφέρει φωνή, video και δεδομένα σε ένα IP δίκτυο. Αυτό παρέχει μια αποδοτική, ελαστική συνδεσιμότητα η οποία ενεργοποιεί τις τελευταίες εφαρμογές δικτύου, όπως είναι η IP Τηλεφωνία. Οι πολλές δυνατότητες του V3PN προάγουν αποκεντρωμένα περιβάλλοντα γραφείων, όπως remote-office/homeoffice συνδεσιμότητα με επέκταση PBX.

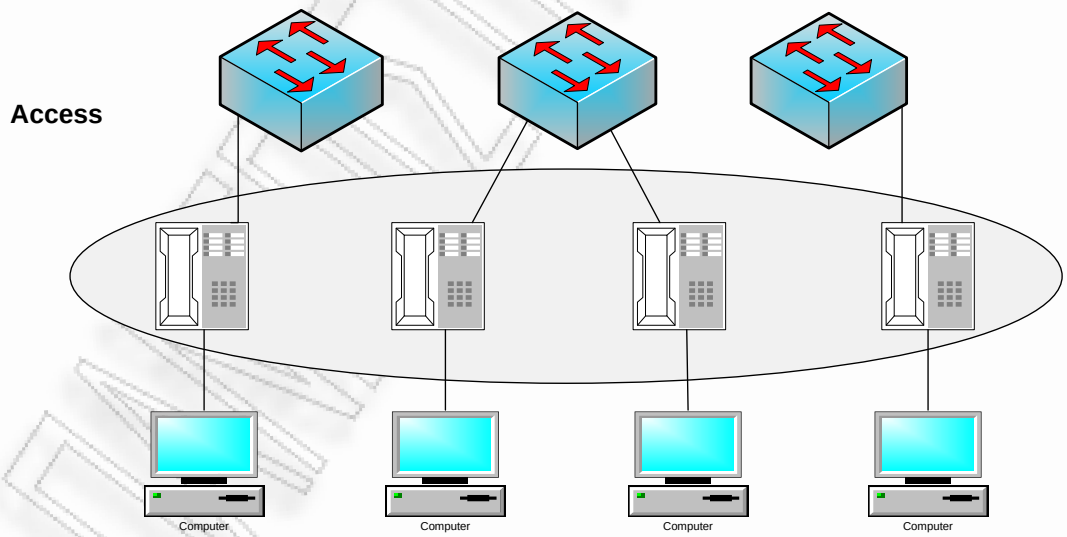
Ένας άλλος τρόπος για την ασφάλεια στην επικοινωνία φωνής, δεδομένων και video μεταξύ απομακρυσμένων γραφείων είναι η χρήση του *Dynamic Multipoint VPN (DMVPN).* Με την διαμόρφωση των πληροφοριών που αποθηκεύονται στο κεντρικό γραφείο, το *DMVPN* απλοποιεί την δημιουργία των VPNs μεταξύ των απομακρυσμένων γραφείων. Με αυτόν τον τρόπο, εμπιστευτικές μεταφορές δεδομένων, φωνής και video είναι ασφαλής, χωρίς καμία επιπλέον διαμόρφωση σε κάθε απομακρυσμένο γραφείο.

2.2.2 Ασφάλεια στον Εξοπλισμό της IP Τηλεφωνίας

Οι διαχειριστές σε ένα IP Τηλεφωνικό κέντρο, εκτός από την εξασφάλιση των καναλιών επικοινωνίας , θα πρέπει να εξασφαλίσουν και τα τερματικά σημεία (endpoints) της τηλεφωνίας. Όπως σε κάθε νέα συσκευή ή υπηρεσία στο δίκτυο, έτσι και ο εξοπλισμός της IP Τηλεφωνίας, μπορεί να αποτελέσει πηγή ή στόχο επιθέσεων και γι' αυτό πρέπει να ασφαλιστεί. Μέθοδοι ασφάλειας του εξοπλισμού αναφέρονται παρακάτω.

1. Ασφάλεια IP Τηλεφωνικών Συσκευών

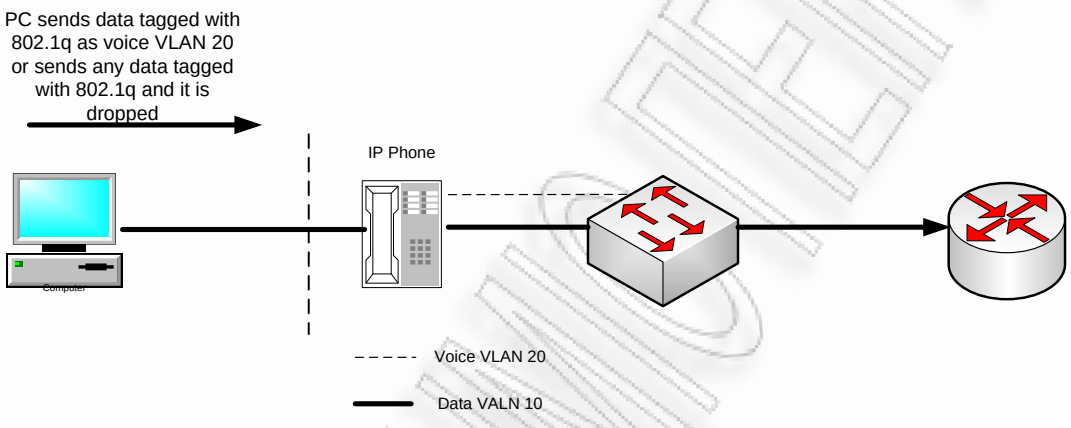
Οι IP τηλεφωνικές συσκευές έχουν την δυνατότητα να περιέχουν χαρακτηριστικά ασφαλείας καθώς και firmware images αλλά και αρχεία διαμόρφωσης. Αυτό εξασφαλίζει ότι οι Hackers δεν μπορούν να εισχωρήσουν στο firmware ή στα διαμορφωμένα αρχεία, για να υπονομεύσουν χαρακτηριστικά ασφάλειας. Επιπλέον προστατεύονται διάφορες ρυθμίσεις από τροποποιήσεις που θα μπορούσαν να υποστούν και οι οποίες θα επηρέαζαν την ασφάλεια του τηλεφωνικού κέντρου.



Σχήμα 6

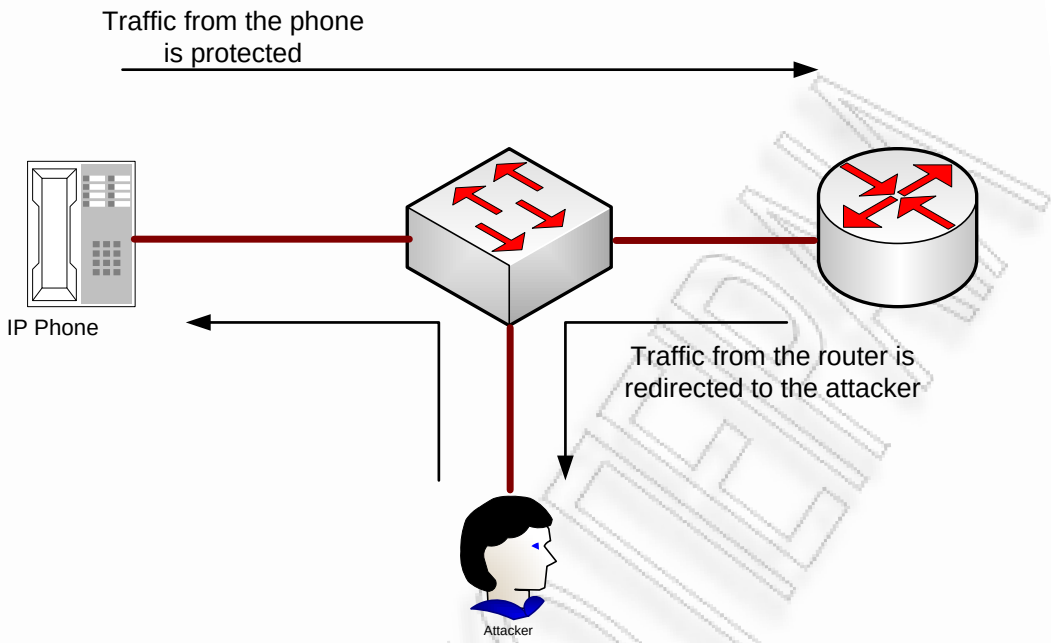
Οι περισσότερες IP τηλεφωνικές συσκευές έχουν ένα PC port, έτσι ώστε οι χρήστες να χρειάζονται μόνο ένα Ethernet καλώδιο για την λειτουργία της IP τηλεφωνικής

συσκευής και του υπολογιστή. Αυτές οι τηλεφωνικές συσκευές, δρομολογούν όλα τα πακέτα που λαμβάνονται από το switch στην πόρτα του PC. Επιπλέον η δυνατότητα απενεργοποίησης του voice VLAN στο PC port, επιτρέπει στον υπολογιστή που είναι συνδεδεμένος στην συγκεκριμένη θύρα να χρησιμοποιεί VLANs, αλλά όχι voice VLANs. Το PC port, μπορεί βέβαια να απενεργοποιηθεί γενικά, κάτι που αυξάνει την ασφάλεια στα τηλέφωνα που χρησιμοποιούνται στο lobby ή στα δωμάτια συνδιάσκεψης.



Σχήμα 7 ***Blocking Traffic to the Voice VLAN from the Phone PC Port***

Η πραγματικότητα είναι ότι μέσω δικτύου έχουμε διάφορες μορφές επιθέσεων, από ότι μέσω ενός συνδεδεμένου υπολογιστή. Γενικά τα περισσότερα IP τηλέφωνα δέχονται πακέτα Gratuitous ARP (GARP). Οι περισσότεροι διαχειριστές επιλέγουν να απενεργοποιούν το Gratuitous ARP.



Σχήμα 8 ***Gratuitous ARP Protects the Phone that Has It but Not Other Traffic***

2. Ασφάλεια στους υπολογιστές και στους Εξυπηρετητές (Servers)

Στη σημερινή εποχή, πολλές επιθέσεις δεν μπορούν να σταματήσουν μέσω των παραδοσιακών λύσεων, όπως με τη χρήση firewalls και signature-based antivirus εφαρμογών, νέες και άγνωστες επιθέσεις πραγματοποιούνται κάθε εβδομάδα και μπορούν να προκαλέσουν εξωπραγματική ζημιά πριν ένα αρχείο είναι διαθέσιμο.

Για την αντιμετώπιση αυτών των επιθέσεων, είναι απαραίτητη η χρήση ενός ειδικού λογισμικού, το λεγόμενο Agent λογισμικό. Δίνεται η δυνατότητα λοιπόν στους χρήστες (Agents) να εφαρμόσουν πολιτικές οι οποίες θα απωθήσουν ή θα περιορίσουν γνωστές ή και άγνωστες επιθέσεις, με το να ρυθμίζουν και να προσδιορίζουν τις δυνατότητες των hosts. Η προστασία αυτή λοιπόν είναι ιδιαίτερα επιθυμητή σε οποιοδήποτε δίκτυο, αλλά είναι κυρίως στο δίκτυο της IP Τηλεφωνίας, διότι σταματά επιθέσεις οι οποίες εάν μείνουν ανεξέλεγκτες, μπορούν να προκαλέσουν την διακοπή ολόκληρου του δικτύου και την υποκλοπή των κλήσεων φωνής.

3. Ασφάλεια του Λειτουργικού Διαχείρισης Κλήσεων

Οι διαχειριστές, όπως σε κάθε εφαρμογή θα πρέπει να απενεργοποιήσουν υπηρεσίες που δεν χρησιμοποιούνται. Για παράδειγμα, ο CallManager χρησιμοποιεί μια σειρά από υπηρεσίες οι οποίες περιλαμβάνουν DHCP, TFTP και το World Wide Web το οποίο παραμένει ενεργοποιημένο, όμως άλλες υπηρεσίες που δεν χρησιμοποιούνται θα πρέπει να απενεργοποιηθούν.

2.2.3 Αυθεντικοποίηση και Κρυπτογραφία στην IP Τηλεφωνία

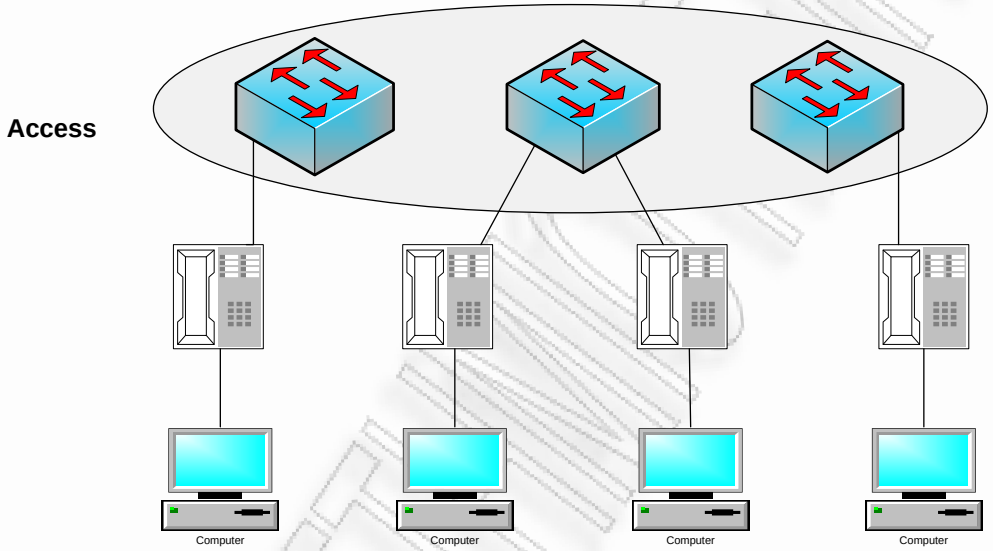
Μια από τις μεγαλύτερες απειλές στο δίκτυο είναι οι άγνωστες συσκευές. Για να αντιμετωπιστεί αυτό το πρόβλημα οι IP τηλεφωνικές συσκευές θα πρέπει να είναι συμβατές με το δίκτυο. Ορισμένες IP συσκευές περιέχουν κάποια ψηφιακά χαρακτηριστικά τα οποία τις αυθεντικοποιούν, μοναδικά, στο δίκτυο. Τα ψηφιακά αυτά στοιχεία μπορούν να μπουν στο firmware ή να προστεθούν από τους διαχειριστές στο δίκτυο.

Τα ιδιαίτερα αυτά χαρακτηριστικά χρησιμοποιούνται με διάφορους τρόπους για την αύξηση της ασφάλειας στο IP Τηλεφωνικό Δίκτυο. Πρώτον, το δίκτυο φωνής μπορεί να περιορίσει την πρόσβαση μόνο στα τηλέφωνα που έχουν γνωστές πιστοποιήσεις ή πιστοποιήσεις που δημιουργήθηκαν από μια έμπιστη αρχή πιστοποιήσεων CA. Δεύτερον, οι ίδιες IP τηλεφωνικές συσκευές μπορούν να διαμορφωθούν έτσι ώστε να εμπιστεύονται servers με συγκεκριμένα χαρακτηριστικά.

2.3 Ασφάλεια Πρόσβασης στο IP Τηλεφωνικό Δίκτυο

2.3.1 Ασφάλεια στο Switch

Υπάρχουν πολλά χαρακτηριστικά Ασφάλειας στη δομή ενός Switch που μπορούν να χρησιμοποιηθούν για την ασφάλεια του δικτύου δεδομένων.



Σχήμα 9 ***A Typical Access Layer Design to Which the Phones Attach***

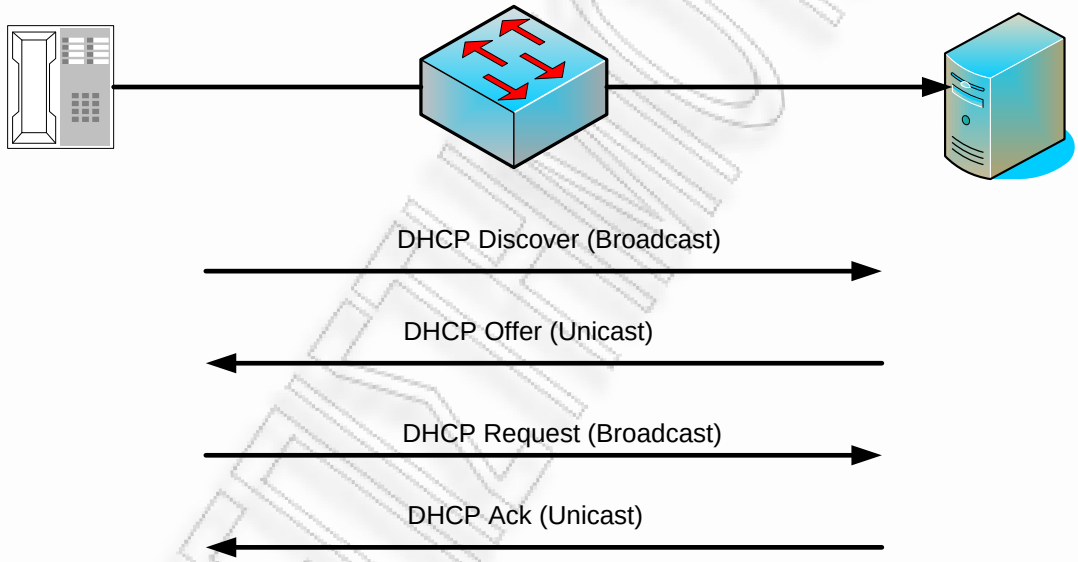
Μια συνηθισμένη επίθεση στο δίκτυο είναι η επίθεση *MAC content-addressable memory (CAM).* Αυτού του είδους η επίθεση πλημμυρίζει το switch με τόσες MAC διευθύνσεις με αποτέλεσμα το switch να μην μπορεί να διακρίνει σε ποια πόρτα συνδέεται μια συσκευή. Έτσι το switch διαχέει την πληροφορία η οποία προοριζότανε για την συσκευή σε ολόκληρο το VLAN. Αυτό δίνει την δυνατότητα στον εισβολέα να υπονομεύσει όλη την κίνηση των χρηστών μέσα στο VLAN. Για την αντιμετώπιση αυτής της επίθεσης μπορεί να χρησιμοποιηθεί είτε *port security είτε dynamic port security.*

Η ασφάλεια στο switch παρέχεται επίσης από τον κατάλληλο προγραμματισμό των ports. Θα πρέπει λοιπόν όλες οι πόρτες του switch να απενεργοποιηθούν, εκτός από εκείνες που χρησιμοποιούν οι συσκευές.

2.3.1.1 DHCP Snooping

Αντιμετώπιση Rogue DHCP Server Επιθέσεις

Πολλές υλοποιήσεις τηλεφωνικών κέντρων χρησιμοποιούν το **DHCP (** Dynamic Host Configuration Protocol) για να παρέχουν IP διευθύνσεις στα τηλέφωνα, γι' αυτό στα switch πρέπει να χρησιμοποιηθούν τα χαρακτηριστικά του *DHCP Snooping για να προστατευθούν τα μηνύματα DHCP*. Με την ενεργοποίηση του *DHCP Snooping* όλες οι πόρτες στο VLAN μετατρέπονται σε *μη-εμπιστευτικές πόρτες* με αποτέλεσμα να μην υπάρχει η δυνατότητα των *reserved DHCP responses.*

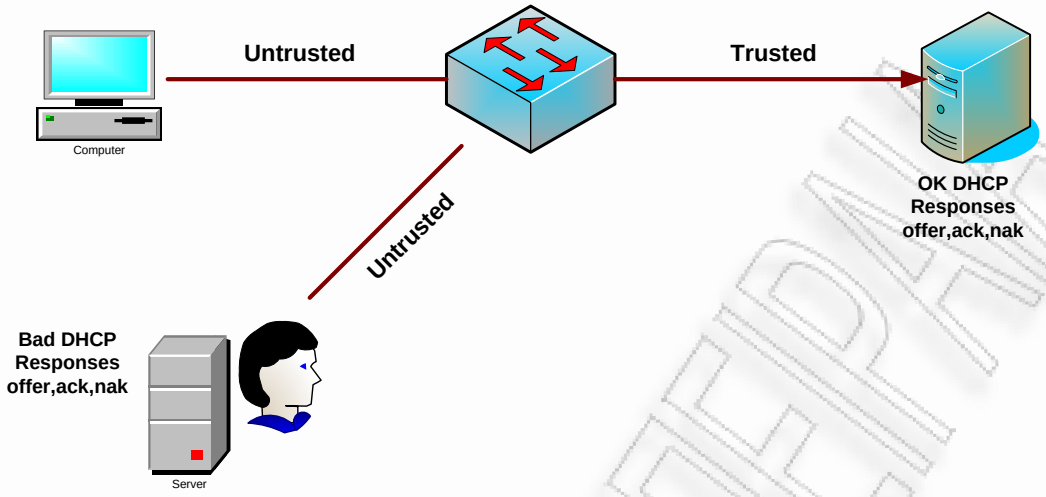


Σχήμα 10 ***Normal Operation of a DHCP Request***

Αντιμετώπιση DHCP Starvation Επιθέσεις

Η αντιμετώπιση αυτής της επίθεσης γίνεται με το να προγραμματίσουμε το switch με τον τρόπο που αναφέραμε παραπάνω ώστε να μειωθεί ο αριθμός των MAC διευθύνσεων.

Ενεργοποιώντας το DHCP Snooping οι μη-εμπιστευτικές πόρτες θα κάνουν μια σύγκριση των πηγών των MAC διευθύνσεων με την ωφέλιμη πληροφορία του DHCP και θα ακυρώσουν το αίτημα εάν δεν ταιριάζουνε.

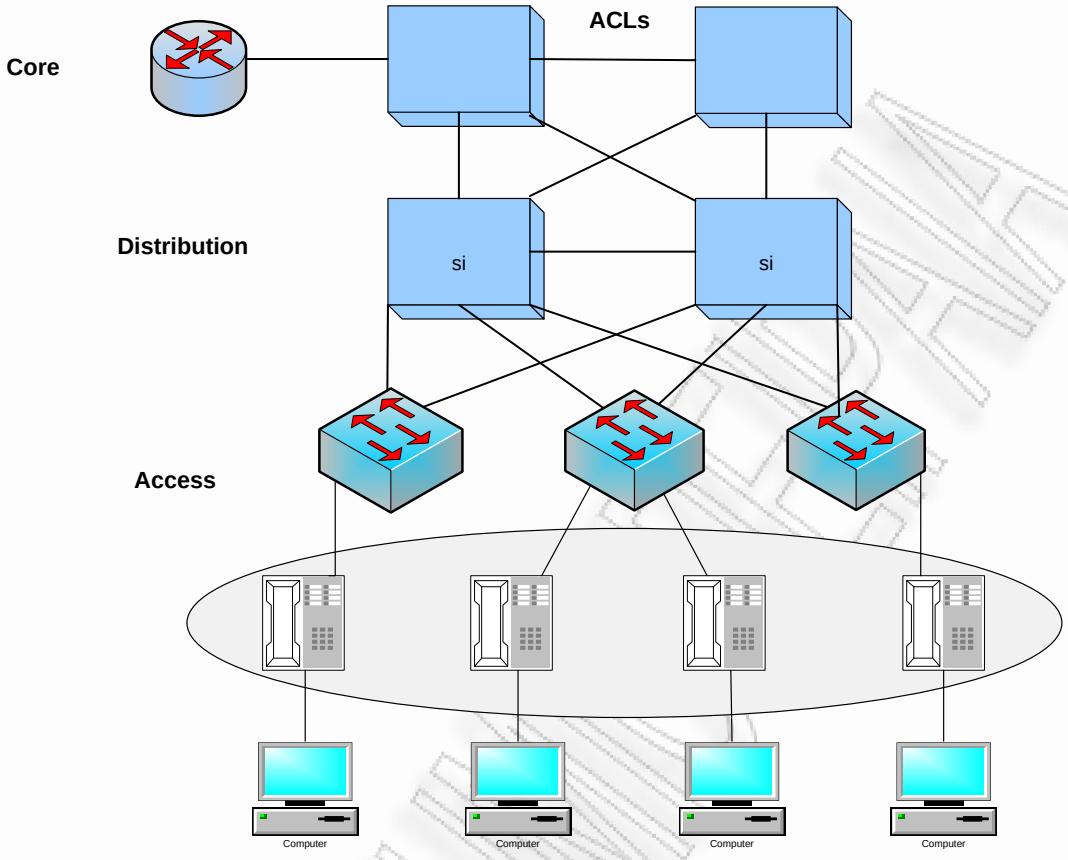


Σχήμα 11 ***Using DHCP Snooping to Prevent DHCP Starvation Attacks***

2.3.2 Ασφάλεια των Gateway and Media Resources

Οι πύλες(Gateways) και οι Media Resources αποτελούν τον απαραίτητο εξοπλισμό για την μετατροπή της IP τηλεφωνικής κλήση σε PSTN κλήση. Η ασφάλεια στις IP τηλεφωνικές πύλες – media resources παρέχεται πολύ πιο δύσκολα από ότι σε οποιαδήποτε άλλη συσκευή, επειδή μπορούν να εγκατασταθούν οπουδήποτε μέσα στο δίκτυο.

Για την προστασία του σήματος από και προς των *Gateways και Media Resources* , μπορεί να χρησιμοποιηθεί το ACL. Εάν το δίκτυο δεν παρέχει ασφάλεια ανάμεσα στις πύλες και όταν το ενοποιημένο λογισμικό επικοινωνίας (UCM) βρίσκει εφαρμογή (απομακρυσμένη περιοχή), τότε μπορούν να δημιουργηθούν IPsec tunnels στα *Gateways και Media Resources, για την προστασία του σήματος.* Στα περισσότερα δίκτυα υπάρχει ο συνδυασμός του IPsec και του ACL για την ασφάλεια αυτών των συσκευών.

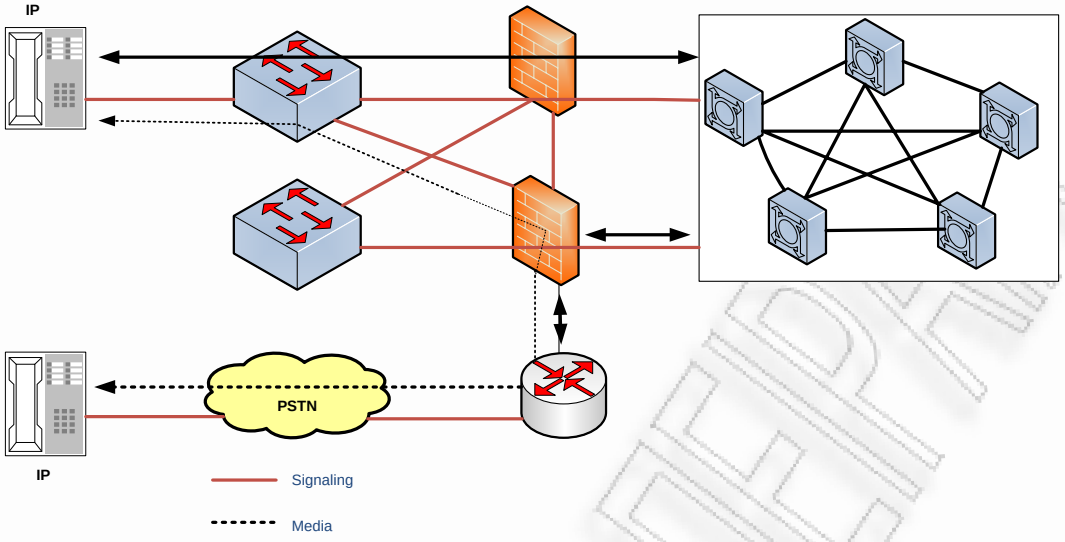


Σχήμα 12 ***Securing Gateways and Media Resources with IPSec, ACLs, and QoS***

2.3.2.1 Χρήση Firewalls στους Gateways

Η προτεινομένη λύση χρήσης firewalls σε Πύλες (Gateways) προσφέρει μια υψηλής ποιότητας ασφάλειας στο τηλεφωνικό δίκτυο. Υπάρχουν δύο τρόποι εγκατάστασης gateway με firewalls : μπροστά από το firewall και πίσω από αυτό.

Εάν η εγκατάσταση του gateway γίνει *πίσω από το firewall*, τότε οι η διέλευση των πληροφοριών των τηλεφωνικών συσκευών θα πρέπει να γίνει μέσω του firewall και απαιτείται CPU για να περάσουν όλα αυτά τα streams μέσα από το firewall. Με αυτό τον τρόπο το firewall αποκτά τον έλεγχο αυτών των streams και προστατεύει τον gateway από τις επιθέσεις denial-of-service.



Σχήμα 13 ***Gateway Placed Behind a Firewall***

Στην περίπτωση που η εγκατάσταση του gateway γίνει *μπροστά από το firewall*, τότε τα RTP streams που διοχετεύουν οι τηλεφωνικές συσκευές θα περάσουν στον έλεγχο του QoS του switch. Με αυτή την μέθοδο μειώνεται η παροχή ασφάλειας καθώς η πληροφορία δεν περνάει μέσα από το firewall.

Κεφάλαιο 3ο

Πρωτόκολλο H.323

Το H.323 ορίζεται από την Διεθνή Ένωση Τηλεπικοινωνιών (ITU) για audio/video επικοινωνία διαμέσου IP δικτύων. Στην πραγματικότητα καλύπτει διάφορα άλλα πρωτόκολλα όπως:

- H.225.0, το οποίο ορίζει τη σύνδεση.
- H.332, το οποίο χρησιμοποιείται για μεγάλες συνεδρίες.
- H.235, το οποίο παρέχει λειτουργίες ασφάλειας και αυθεντικότητας.
- H.245, το οποίο διαπραγματεύεται την χρήση του καναλιού.
- RAS, που χειρίζεται τα μηνύματα καταχώρισης, εισαγωγής, και κατάστασης (registration, admission, and status messages).

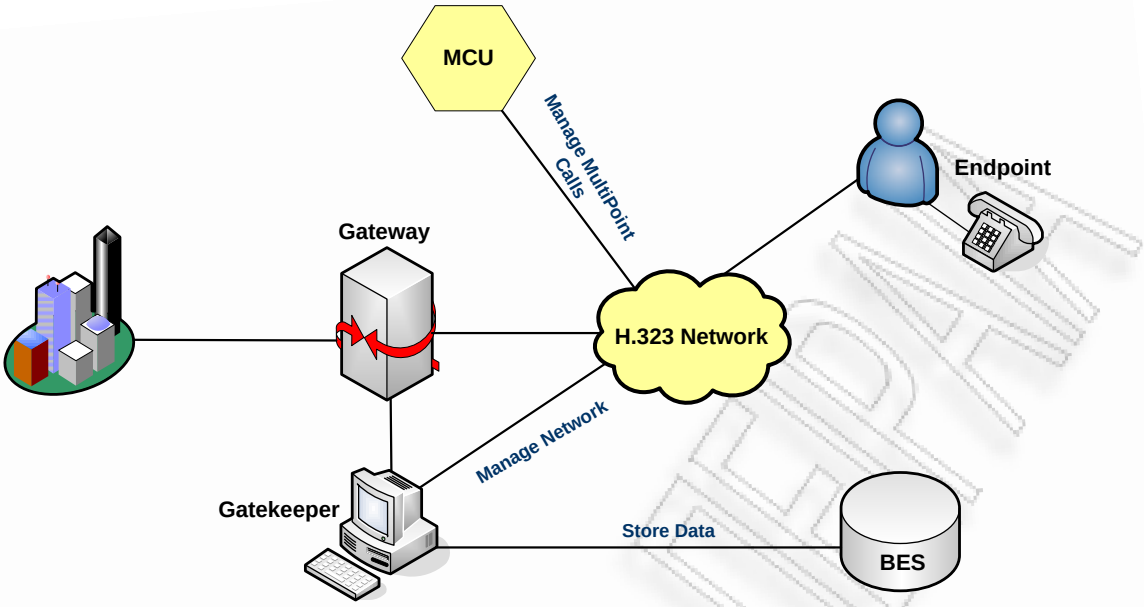
Κάθε ένα από αυτά τα πρωτόκολλα έχει έναν συγκεκριμένο ρόλο στη διαδικασία οργάνωσης μιάς κλήσης και όλα, εκτός από ένα, προορίζονται για δυναμικές θύρες. Το σχήμα 14 παρουσιάζει την αρχιτεκτονική H.323 και το σχήμα 15 παρέχει μια επισκόπηση της διαδικασίας οργάνωσης κλήσης με H.323.

3.1 Η Αρχιτεκτονική του H.323

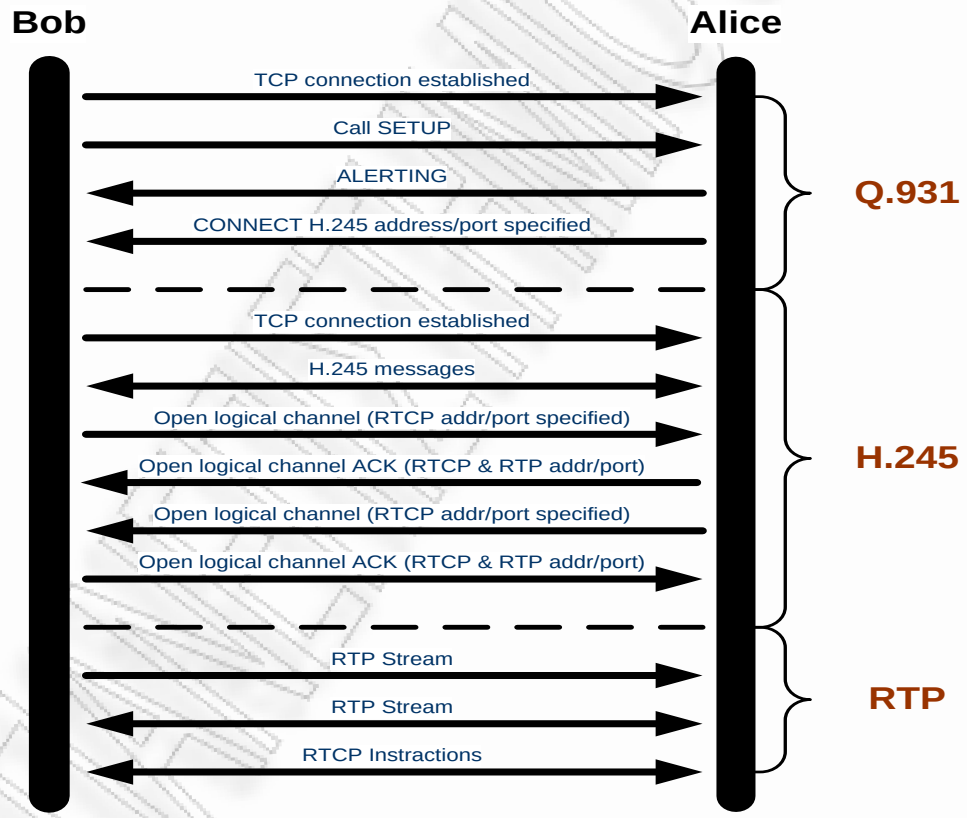
Ένα IP δίκτυο το οποίο θα χρησιμοποιεί το πρωτόκολλο H.323 μπορεί να αποτελείται από διάφορα τερματικά (endpoints), πύλες (gateways), ένα gatekeeper, μία μονάδα ελέγχου και Backup σύστημα. Ο gatekeeper αποτελεί συνήθως ένα από τα κύρια συστατικά στα συστήματα H.323, το οποίο παρέχει επίλυση διευθύνσεων και έλεγχο του εύρους ζώνης.

Η πύλη (gateway) χρησιμοποιείται για την πραγματοποίηση της κλήσης και την μετάδοση των πληροφοριών στο εξωτερικό δίκτυο όπου δεν είναι απαραίτητο να χρησιμοποιούνται συσκευές οι οποίες είναι συμβατές με το πρωτόκολλο H.323.

Το Multipoint Control Unit είναι ένα προαιρετικό στοιχείο που διευκολύνει την τηλεφωνική συνδιάσκεψη και άλλες επικοινωνίες ανάμεσα σε στους χρήστες του τηλεφωνικού δικτύου.



Σχήμα 14 **Αρχιτεκτονική του H.323**



Σχήμα 15 **Διαδικασία οργάνωσης κλήσης του H.323**

Γενικά, υπάρχουν διάφοροι τύποι H.323 κλήσεων που καθορίζονται στα H.323 πρότυπα:

- Δρομολόγηση κλήσεων από έναν gatekeeper μέσω ενός gatekeeper ο οποίος χρησιμοποιεί Η.245 σηματοδότηση
- Δρομολόγηση κλήσεων από έναν gatekeeper με άμεση χρήση Η.245 σηματοδότησης
- Άμεση δρομολόγηση κλήσεων μες gatekeeper
- Άμεση δρομολόγηση κλήσεων χωρίς gatekeeper

Η λειτουργία ενός VOIP Η.323 δικτύου ενεργοποιείται (ανάλογα με το πρότυπο κλήσης που χρησιμοποιείται) είτε από μία TCP, είτε από μία UDP σύνδεση (εάν το RAS είναι το σημείο αφετηρίας) μέσω ενός Η.225 σήματος. Στην περίπτωση της UDP σύνδεσης, αυτό το Η.225 σήμα, περιέχει το πρωτόκολλο Registration Admission Status (RAS), που διαπραγματεύεται με το gatekeeper και λαμβάνει τη διεύθυνση του ακραίου σημείου (endpoint) που προσπαθεί να έρθει σε επαφή.

Στη συνέχεια, ένα πρωτόκολλο όπως το "Q.931" (παραμένοντας στη σφαίρα του Η.225) χρησιμοποιείται για να καθιερώσει την ίδια κλήση και να διαπραγματευτεί τον έλεγχο της πληροφορίας για το Η.245 σήμα (αυτό γίνεται μέσω του TCP,το Q.931 στην πραγματικότητα ενθυλακώνει τα μηνύματα σηματοδότησης κλήσης του Η.225). Αυτή η διαδικασία, της "μετέπειτα οργάνωσης", έχει κοινό ρυθμό απόδοσης σε όλη την πρόοδο του Η.323, όπου ένα πρωτόκολλο διαπραγματεύεται τη διαμόρφωση του επόμενου πρωτοκόλλου που θα χρησιμοποιηθεί.

Καθώς το Η.225 διαπραγματεύεται απλά την καθιέρωση μιας σύνδεσης, το Η.245 καθιερώνει τα κανάλια που θα χρησιμοποιηθούν για τη μεταφορά των μέσων. Για άλλη μια φορά, αυτό γίνεται μέσω του TCP. Σε μια χρονικά-επείγουσα κατάσταση, το μήνυμα Η.245 μπορεί να ενσωματωθεί μέσα στο μήνυμα Η.225 (Η.245 tunneling), αλλά η ταχύτητα οργάνωσης μιας κλήσης συνήθως είναι ένα ζήτημα QoS, όπου οι προμηθευτές και οι πελάτες είναι πρόθυμοι να κάνουν παραχωρήσεις για την καλύτερη ποιότητα κλήσης.

Το H.245, πρέπει να καθιερώσει διάφορες ιδιότητες της VOIP κλήσης. Αυτές περιλαμβάνουν τους ακουστικούς κωδικοποιητές / αποκωδικο-ποιητές που θα χρησιμοποιηθούν και τα λογικά κανάλια για τη μεταφορά των μέσων. Επίσης το σήμα "OpenLogicalChannel" μεσολαβεί για τις RTP και RTCP θύρες. Πρέπει να καθιερωθούν συνολικά τέσσερις συνδέσεις, επειδή τα λογικά κανάλια (RTP και RTCP) είναι μόνο μίας κατεύθυνσης. Κάθε ζευγάρι μίας κατεύθυνσης, πρέπει επίσης να ανήκει σε κάποια θύρα. Αφότου το H.245 έχει καθιερώσει όλες τις ιδιότητες της VOIP κλήσης και των λογικών καναλιών, τότε μπορεί να αρχίσει η κλήση.

Η σύνθετη διαδικασία οργάνωσης του VOIP που περιγράψαμε προηγουμένως, είναι βασισμένη στο H.323. Η H.323 ακολουθία, συνδέει τα διάφορα πρωτόκολλα με τις πιο σύνθετες μορφές επικοινωνίας, συμπεριλαμβανομένου των H.332 (μεγάλες τηλεφωνικές συνδιασκέψεις), H.450.1, H.450.2 και H.450.3 (συμπληρωματικές υπηρεσίες), H.235 (ασφάλεια) και H.246 (διαλειτουργικότητα υπηρεσιών με switched κυκλώματα).

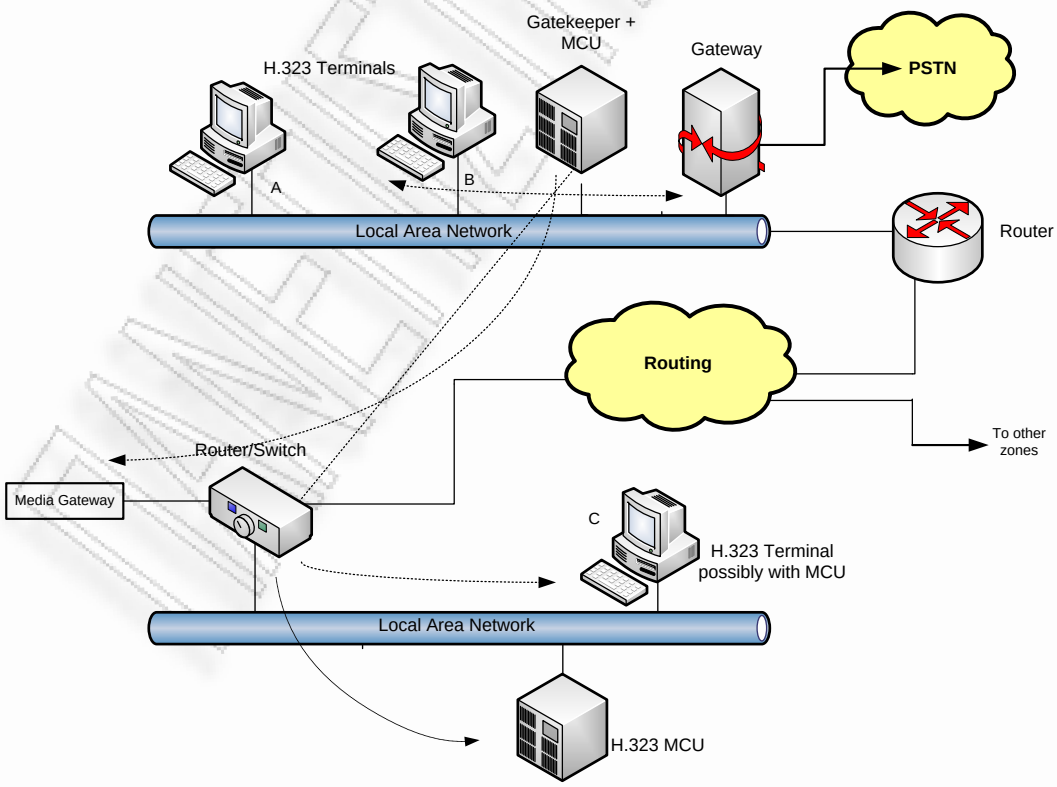
Η επικύρωση επίσης, μπορεί να εκτελεστεί σε κάθε σημείο στη διαδικασία οργάνωσης μιας κλήσης, χρησιμοποιώντας τα συμμετρικά κλειδιά ή κάποιο προγενέστερο “κοινό μυστικό”. Η χρήση αυτών των πρόσθετων πρωτοκόλλων ή και των μέτρων ασφαλείας, προσθέτει πολυπλοκότητα στη διαδικασίας οργάνωσης του H.323. Στη συνέχεια, θα δούμε ότι αυτή η πολυπλοκότητα είναι κυρίαρχη στο ασυμβίβαστο του H.323 με τις αντιπυρικές ζώνες και τα NATs. Αυτά τα ζητήματα αναφέρονται στην επόμενη παράγραφο.

3.2 Ορισμοί και Αναφορές

Ένα τερματικό H.323 είναι μια συσκευή που περιλαμβάνει ένα ακραίο σημείο σηματοδοσίας που υποστηρίζει έναν ή και περισσότερους χρήστες, οι οποίοι εισάγονται σε μία πραγματικού χρόνου επικοινωνία με ένα ή περισσότερα συμβαλλόμενα μέρη.

Στα ομοιογενή περιβάλλοντα H.323 τα υπόλοιπα συμβαλλόμενα μέρη θα είναι επίσης, χρήστες των τερματικών H.323, αλλά στη γενική περίπτωση ένα ή περισσότερα από τα συμβαλλόμενα μέρη σε μία κλήση μπορούν αν συμφωνήσουν με μία διαφορετική δικτυακή γειτονιά, όπως ένας χρήστης του SIP, PSTN ή ένα ακραίο σημείο με S/MGCP. Το πλήρες μοντέλο κλήσης H.323 εκτελείται μεταξύ δύο τερματικών, ενός τερματικού και ενός θυρωρού (gate keeper), ή ενός τερματικού και μιας πύλης. Ένας gate keeper είναι ο εγκέφαλος μιας ζώνης H.323. Μια ζώνη H.323 περιλαμβάνει όλες τις τελικές πύλες και της πολλαπλής διανομής μονάδες ελέγχου (MCUs) διοικούμενες από τον gate keeper. Σε κάθε ζώνη αντιστοιχεί μόνο ένας gate keeper.

Μια ζώνη είναι μια λογική ομαδοποίηση των συσκευών και μπορεί να περιέχει τα δεδομένα που μπορούν να είναι μέρος μίας αποκεντρωμένης τοπολογίας που συνδέεται με τα switches και τους routers. Με άλλα λόγια ακόμα μία ζώνη μπορεί να επεκταθεί σε μία ευρεία γεωγραφική περιοχή. Το σχήμα 16, εμφανίζει μία επέκταση της γενικής μορφής μιας ζώνης H.323 και τη συνδετικότητα μεταξύ των δεδομένων των gate keeper και των δικτύων σε δύο τμήματα μνήμης του LAN.



Σχήμα 16 **Στοιχεία H.323 δικτύων και εκτεταμένος καθορισμός ζώνης**

Σημειώνεται ότι τα switches και οι δρομολογητές είναι διαφανείς στα δεδομένα των H.323 δικτύων, δηλαδή δεν τους βλέπουν ή δεν τους διαχειρίζονται ως τμήμα διοικητικών λειτουργιών επεξεργασίας ή σηματοδότησης κλήσης. Μπορεί επίσης, να υπάρξουν περισσότερα από ένα MCU σε μία ζώνη, και η χρήση τους είναι μία από τις λειτουργίες που εκτελούνται από τον gate keeper. Στην περίπτωση ευρείας ζώνης εμφανίζεται η πρόσβαση του H.323 gate keeper σε ένα μόνιμο gateway/hub, μέσω της αλλαγής και της δρομολόγησης του εξοπλισμού.

Τέτοια θα ήταν η περίπτωση, για παράδειγμα εάν ένας ISP (Internet service provider) χρησιμοποιεί H.323 για να προσφέρει τη βασική ολοκλήρωση τηλεφωνικών υπηρεσιών καθώς επίσης και media stream στα απομακρυσμένα και γεωγραφικά διανεμημένα ακραία σημεία όπως οι κατοικημένες πύλες. Αυτό είναι μόνο μία σκέψη, και αυτός ο τύπος υπηρεσίας που συγχωνεύεται μεταξύ του LAN και του WAN εγείρει μεγάλα ζητήματα σχεδίασης και εφαρμογής.

Οι gatekeepers μπορούν να κάνουν σήμα σε άλλους gatekeepers, σε άλλες ζώνες για να προσεγγιστούν οι χρήστες σε άλλες δικτυακές γειτονιές με έναν τρόπο διαφανή στο συμβαλλόμενο μέρος που καλεί. Στα επιχειρηματικά σενάρια, αυτό θα ήταν χρήσιμο να υποστηρίξει τις διανεμημένες θέσεις μίας πολυεθνικής εταιρίας, ή οποιαδήποτε άλλη περίπτωση γεωγραφικής διανομής μεταξύ των τμημάτων μνήμης του LAN.

Οι πύλες έχουν πρόσβαση στο PSTN για να προσφέρουν τη συνδετικότητα κλήσης στους POTS πελάτες, αλλά οι πύλες προσφέρουν επίσης, τη πρόσβαση σε οποιοδήποτε διαφορετικό τύπο τοπικών τμημάτων μνήμης, όπως οι δικτυακές γειτονιές SIP και MGSP.

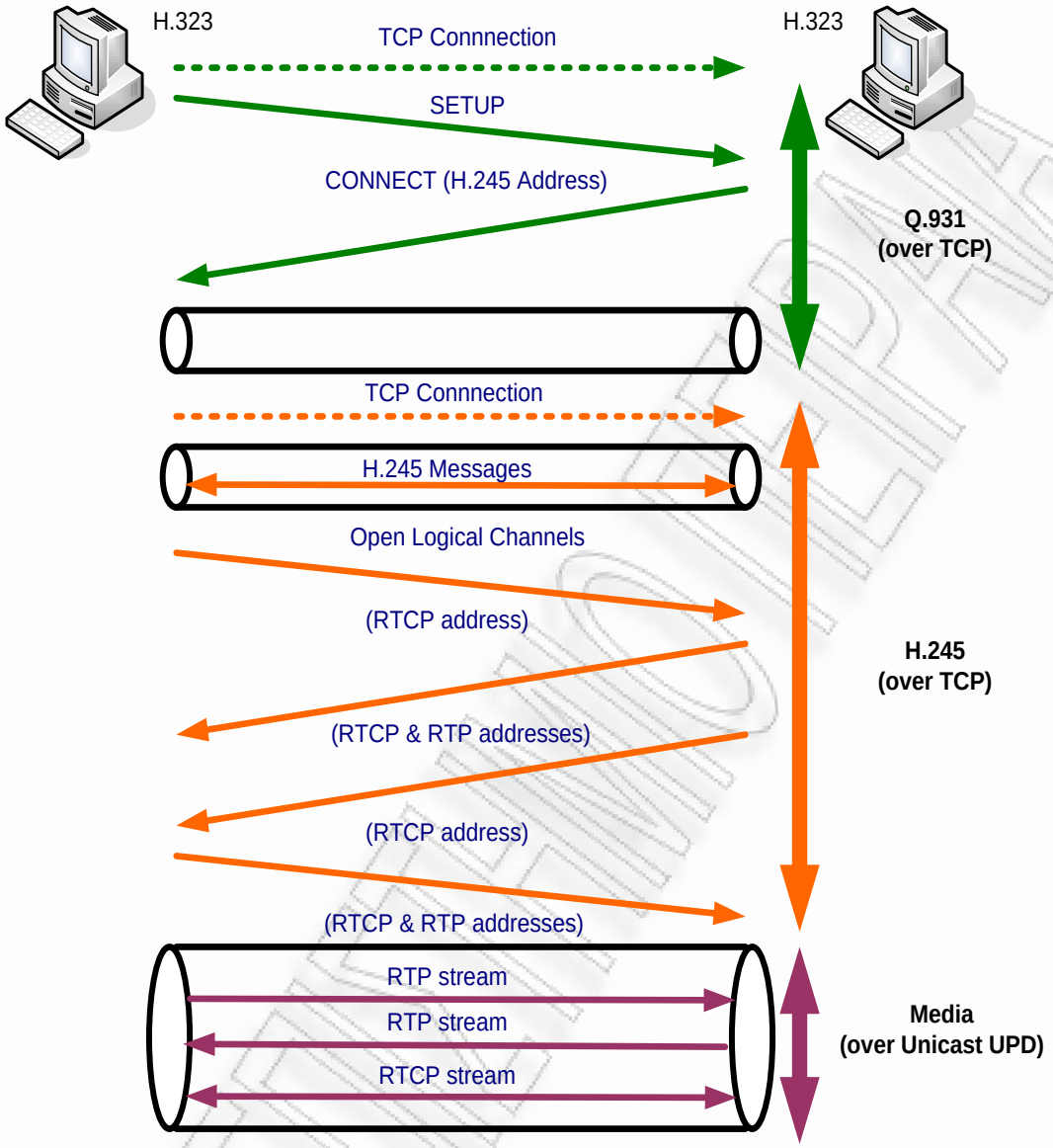
3.3 Πολλαπλές Συνδιασκέψεις / Συνεδριάσεις

Ένα από τα πολύ καλά χαρακτηριστικά του H.323 είναι η δυνατότητα που προσφέρει για την ύπαρξη πολλών διασυνδέσεων ταυτόχρονα. Δύναται να υλοποιήσει τρία διαφορετικά αρχιτεκτονικά μοντέλα:

- Συγκεντρωτικό μοντέλο (centralized model): απαιτεί την ύπαρξη μίας MSU στην οποία όλοι οι τερματικοί σταθμοί που επιθυμούν να συνδεθούν μεταξύ τους, εγκαθιστούν μία point – to – point επικοινωνία. Ο MS ελέγχει τις διασυνδέσεις χρησιμοποιώντας το H.245 ενώ παράλληλα, καθορίζει τις αρμοδιότητες κάθε τερματικού, ενώ ο MP φροντίζει για την ορθή διαχείριση του ρεύματος των πακέτων που ανταλλάσσονται παρέχοντας τις αναγκαίες υπηρεσίες mixing και switching, μπορεί να αναγνωρίσει την ύπαρξη διαφορετικών κωδικοποιητών/ αποκωδικοποιητών, να προσφέρει υπηρεσίες μετάβασης από τον ένα στον άλλον, αλλά και να προωθήσει multicast πληροφορία στους τελικούς πολλαπλούς προορισμούς της.

- Αποκεντρωμένο μοντέλο (de-centralized model): λειτουργεί κάνοντας χρήση της τεχνολογίας multicast, όπου τα συμβαλλόμενα σε διάφορες διασκέψεις τερματικά επικοινωνούν μεταξύ τους με αποστολή multicast πακέτων χωρίς να υποχρεώνονται στην προηγούμενη αποστολή αυτών στην MSU. Ο ρόλος πλέον της MSU καθορίζεται πλέον στην point – to – point πληροφορία ελέγχου (με τη μορφή των H.245 καναλιών), που αποστέλλεται στον MS για την ενημέρωση σχετικά με τον αριθμό των ενεργών ρευμάτων των πακέτων μεταξύ των τερματικών.

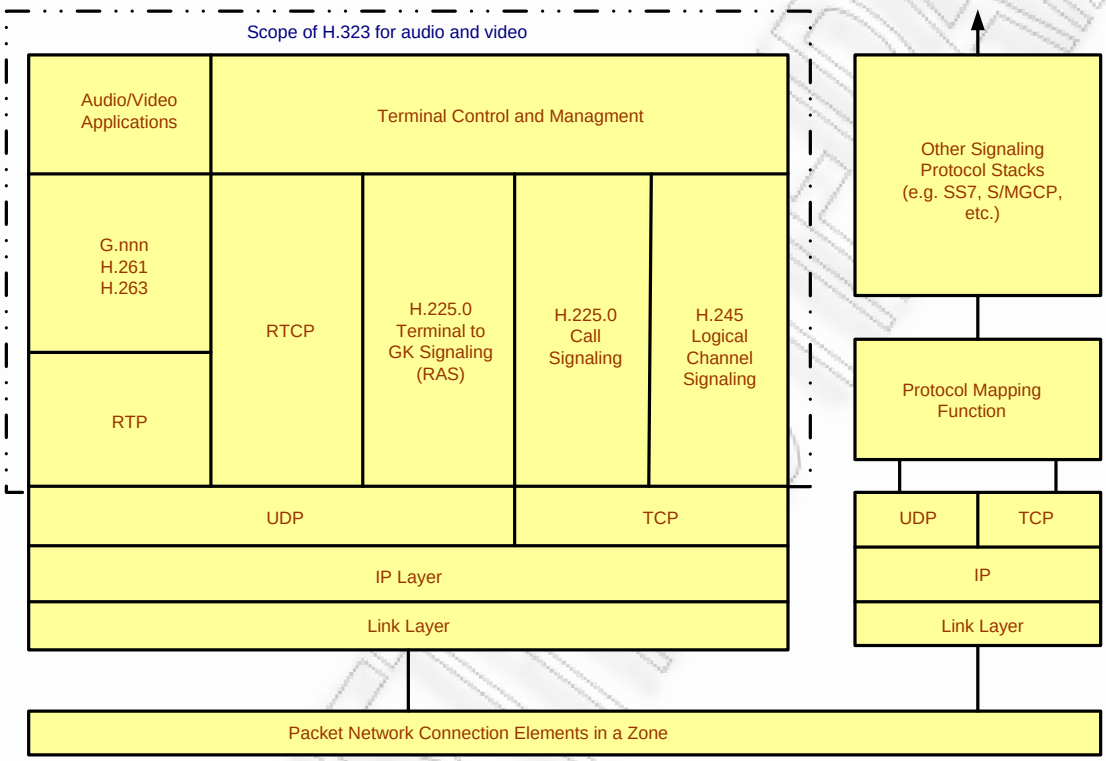
- Υβριδικό μοντέλο (hybrid model): χρησιμοποιεί συνδυασμό χαρακτηριστικών τόσο του συγκεντρωτικού, όσο και του αποκεντρωτικού μοντέλου προσφέροντας τη δυνατότητα μιας ενδιάμεσης λύσης, με ορισμένα από τα τερματικά να δρουν σαν μέλη ενός συγκεντρωτικού μοντέλου (με αποστολή πληροφορίας control+ data) στην MCU, και άλλα να χρησιμοποιούν multicast τεχνικές για την επικοινωνία τους χρησιμοποιώντας την MCU για πληροφορίες ελέγχου.



Σχήμα 17 **Πολλαπλές Διασκέψεις / Συνεδριάσεις**

3.4 Πρωτόκολλα H.323

Το πεδίο των προτύπων H.323 για τις ηχητικές, τις τηλεοπτικές και τις εφαρμογές fax εμφανίζεται στο σχήμα 18.



Σχήμα 18 **Σωρός του H.323 και αρχιτεκτονική Interworking πρωτοκόλλου**

Εκτός από το H.225.0 για τη σηματοδότηση κλήσης, το RAS, και το H.245 για τον έλεγχο μέσων, τα πρότυπα H.323 προσδιορίζουν επίσης, το RTP ως το πρωτόκολλο μεταφοράς μέσων. Το RTCP είναι το συνεργαζόμενο πρωτόκολλο ελέγχου με το RTP.

Η στοίβα πρωτοκόλλου χωρίζει το H.225.0 για να τρέξει πάνω από UDP για το RAS, και σε TCP για τη σηματοδότηση κλήσης. Το H.245 τρέχει μόνο άνω του TCP. Η φιλοσοφία του H.323 είναι η ευρωστία του ελέγχου κλήσης, στα μη γερά περιβάλλοντα. Αυτό έρχεται με κόστος μερικής υποβάθμισης απόδοσης στην οργάνωση των κλήσεων, και γενικά σύνθετες εφαρμογές για τους εγκεφάλους των τμημάτων μνήμης δικτύων, όπως τα GKs και τα GWs.

Το TCP προσφέρει μία σταθερή προσέγγιση στην κλήση σηματοδοσίας, αλλά περιέχει περιορισμούς απόδοσης που μπορούν αν είναι απαράδεκτοι για την WAN τηλεφωνία. Οι gate keepers πρέπει να κρατήσουν όλες τις συνδέσεις TCP ανοιχτές κατά τη διάρκεια των κλήσεων. Προσωρινά, τα ζητήματα με τα χαμηλότερα κανάλια σηματοδοσίας μπορεί να προκαλέσουν την απώλεια της σύνδεσης TCP, η οποία θα οδηγήσει στην απόρριψη της κλήσης.

Αυτό μπορεί να είναι αποδεκτό στην τηλεφωνία μη υψηλής ποιοτικής φωνής, αλλά δημιουργεί ζητήματα όταν ο στόχος είναι να επιτευχθεί η ποιότητα carrier (PSTN ποιότητα) στις διανεμημένες δικτυακές γειτονιές.

Μια υποστηριζόμενη αξίωση των πρωτοκόλλων του S/MGCP και του SIP είναι ένα πολύ απλουστευμένο μοντέλο κλήσης. Αυτό ισχύει σε πολλές περιπτώσεις, αλλά η απλότητα αυτή δε θα μείνει σίγουρα χωρίς επιπτώσεις.

Τα πρωτόκολλα H.323 χρησιμοποιούν το στρώμα IP χωρίς τις προειδοποιήσεις, δηλαδή καμία ιδιόκτητη επέκταση IP. Εντούτοις, για QoS δρομολόγηση, το H.323 συστήνει τη χρήση RSVP (πρωτόκολλο ReSerVation) που καθορίζεται στο RFC 2205, αλλά δεν απολαμβάνει την πανταχού παρούσα επέκταση στα περισσότερα δίκτυα.

Το πρωτόκολλο στρώματος συνδέσεων μπορεί να είναι το ATM, και η χρήση του ATM στις εφαρμογές σηματοδοσίας H.323 έχει αυξηθεί. Σε LANs το ονομαστικό πρωτόκολλο στρώματος συνδέσεων είναι το Ethernet, εντούτοις η ATM – βασισμένη τεχνολογία, όπως η εξομοίωση του τυπικού LAN – multiprotocol over ATM (MPOA), συν την ανάγκη να διανεμηθεί η H.323 σηματοδοσία στα απομακρυσμένα σημεία τέλους, έχει εξουσιοδοτήσει την ανάγκη για ένα WAN πρωτόκολλο στρώματος συνδέσεων για τη μεταφορά IP – βασισμένης σηματοδοσίας ελέγχου κλήσης.

Το ATM συνεργάζεται καλώς στη συγκεκριμένη διαδικασία, λόγω των διαφορετικών κλάσεων υπηρεσίας του, την αξιοπιστία, και τους μηχανισμούς QoS του που ενισχύουν το H.323 στην ποιότητα και την ευρωστία. Το φυσικό στρώμα στο

διάγραμμα είναι ένα εικονικό στρώμα και αποτελείται κανονικά από μία συλλογή των point - to- point και των broadcast τμημάτων μνήμης, μεταξύ των πολλαπλάσιων τύπων δικτύων.

Στο σχήμα 18, εμφανίζεται επιγραμματικά, μια στοίβα IP για το πρωτόκολλο που αλληλεπιδρά μεταξύ H.323 και SS7 ή του S/MGCP. Το μπροστινό τέλος της αλληλεπιδρώμενης στοίβας πρωτοκόλλου πρέπει να υποστηρίξει το H.225.0 για την οργάνωση κλήσης. Ακόμα κι αν τα χαμηλότερα στρώματα φαίνονται απλά, οι πολυπλοκότητες σε μια αλληλεπιδρώμενη εφαρμογή βρίσκονται στις λειτουργίες χαρτογράφησης για να επεκτείνουν κατάλληλα τη λειτουργία του ενός συνόλου πρωτοκόλλων στη δικτυακή γειτονιά του άλλου, στο μεγαλύτερο δυνατό βαθμό.

Για την SS7 αλληλεπίδραση, αναμένεται ότι το τμήμα μνήμης δικτύων της H.323 θα υιοθετήσει τα στοιχεία και τις διαδικασίες δικτύων για να ελέγξει τη σηματοδότηση και τους κορμούς του PSTN, όπως περιγράφουμε στο SS7 τμήμα, με έναν τρόπο διαφανή στο SS7 δίκτυο δηλαδή, το PSTN δε θα έχει τη γνώση της κλήσης σηματοδοσίας και των μηχανισμών μεταφοράς μέσων που υιοθετούνται στην PSTN σηματοδοσία που ελέγχεται από το Gateway.

3.5 Ζητήματα ασφάλειας του H.323

Οι αντιπυρικές ζώνες δημιουργούν ιδιαίτερα προβλήματα για τα δίκτυα VOIP που χρησιμοποιούν το H.323. Με εξαίρεση το H.225 που είναι σαν το Q.931, όλη η H.323 κυκλοφορία δρομολογείται μέσω των δυναμικών θυρών. Για το H.323 Fast Start και το H.245 tunneling χρησιμοποιείται μόνο ένα κανάλι (H.225 σηματοδότηση κλήσεως). Συνήθως, η σηματοδότηση κλήσεως εκτελείται μέσω της θύρας 1720.

Εάν επιπρόσθετα η επικοινωνία H.225 RAS γινόταν με το gatekeeper (UDP), αυτό θα γινόταν μέσω της θύρας 1719. Δηλαδή, κάθε διαδοχικό κανάλι στο πρωτόκολλο, δρομολογείται μέσω μίας δυναμικής θύρας, που καθορίζεται από τον προκάτοχό του. Αυτή η ειδική μέθοδος εξασφάλισης των καναλιών, δεν οδηγεί σωστά σε

διαμόρφωση στατικών αντιπυρικών ζωνών. Αυτό ισχύει ιδιαίτερα στην περίπτωση των άτακτων αντιπυρικών ζωνών που δεν μπορούν να κατανοήσουν την H.323 κυκλοφορία. Αυτά τα απλά φίλτρα πακέτων, δεν μπορούν να συσχετίσουν τις μεταδόσεις UDP και τις απαντήσεις. Αυτό απαιτεί διάνοιξη τρυπών στην αντιπυρική ζώνη, για να επιτρέψει στην H.323 κυκλοφορία, να διαπεράσει τη γέφυρα ασφαλείας σε οποιαδήποτε από τις προσωρινές θύρες που μπορεί να χρησιμοποιούνται.

Αυτή η πρακτική θα εμφάνιζε τις σοβαρές αδυναμίες στην ασφάλεια, επειδή μια τέτοια εφαρμογή θα πρέπει να ελευθερώσει 10.000 UDP θύρες και διάφορες H.323 συγκεκριμένες TCP θύρες ανοιχτές. Έτσι, υπάρχει μια ανάγκη για μια σταθερή αντιπυρική ζώνη που κατανοεί το VOIP και συγκεκριμένα το H.323. Μία τέτοια αντιπυρική ζώνη μπορεί να διαβάσει τα H.323 μηνύματα και να ανοίξει δυναμικά τις σωστές θύρες για κάθε κανάλι, καθώς το πρωτόκολλο εξελίσσεται μέσω της διαδικασίας οργάνωσης μιας κλήσης. Μια τέτοια αντιπυρική ζώνη, πρέπει να είναι μέρος μιας αρχιτεκτονικής ασφαλείας, ειδικά στα σενάρια όπου στο πρωτόκολλο εφαρμόζονται μέτρα ασφαλείας, π.χ. ακεραιότητα μηνυμάτων.

Ακόμη και με ένα ενήμερο VOIP στις αντιπυρικές ζώνες, η ανάλυση της H.323 κυκλοφορίας δεν είναι ένα τετριμμένο θέμα. Η H.323 κυκλοφορία, κωδικοποιείται με ένα δυαδικό σχήμα, βασισμένο στο ASN.1. Το ASN.1 δεν χρησιμοποιεί σταθερές αντισταθμίσεις για πληροφορίες διευθύνσεων και οι διάφορες περιπτώσεις μιας εφαρμογής μπορούν να διαπραγματευτούν διάφορες επιλογές, με συνέπεια τα διάφορα αντισταθμιστικά byte για τις ίδιες τις πληροφορίες. Αυτό το επίπεδο πολυπλοκότητας, δεν επιτρέπει τα απλά εργαλεία ανάλυσης ή τα απλά χειρόγραφα Perl, να αποκωδικοποιήσουν την κυκλοφορία. Στην πραγματικότητα, απαιτούνται ειδικές γεννήτριες κώδικα.

Μία τέτοια τεχνολογία δεν είναι διαθέσιμη στις παραδοσιακές φιλτραρισμένες αντιπυρικές ζώνες πακέτων ή ακόμα και στις απλές σταθερές αντιπυρικές ζώνες. Αν και αυτή η ανάλυση μπορεί να γίνει χρησιμοποιώντας τις σύγχρονες πύλες VOIP , απαιτείται σύνθετη ανάλυση για να διακρίνει το περιεχόμενο των κωδικοποιημένων ASN.1 πακέτων, εισάγοντας περαιτέρω λανθάνουσα κατάσταση σε ένα ευαίσθητο στην ταχύτητα σύστημα που είναι ήδη γεμάτο με καθυστερήσεις.

Το NAT επίσης, είναι ιδιαίτερα προβληματικό για τα συστήματα VOIP που χρησιμοποιούν το πρωτόκολλο οργάνωσης κλήσης H.323. Το NAT περιπλέκει τις H.323 επικοινωνίες, επειδή η εσωτερική διεύθυνση και η IP θύρα που διευκρινίζεται στις H.323 κεφαλίδες και στα H.323 μηνύματα δεν είναι οι ίδιοι πραγματικοί αριθμοί διευθύνσεων/θυρών που χρησιμοποιούνται εξωτερικά από ένα απομακρυσμένο τερματικό. Αυτό αποδιοργανώνει τη διαδικασία "επόμενης οργάνωσης" που χρησιμοποιείται από κάθε πρωτόκολλο μέσα στην H.323 ακολουθία (π.χ., H.225 που στήνει H.245).

Έτσι, δε χρειάζεται μόνο να κατανοηθεί η αντιπυρική ζώνη, αλλά είναι ουσιαστικό ότι η εφαρμογή VOIP λαμβάνοντας αυτές τις H.323 επικοινωνίες, λαμβάνει τους σωστούς μεταφρασμένους αριθμούς διευθύνσεων/θυρών. Κατά συνέπεια, εάν το H.323 πρόκειται να διαπεράσει μια πύλη NAT, η συσκευή NAT πρέπει να είναι σε θέση να μετατρέψει τις διευθύνσεις, σε ρεύμα ελέγχου. Έτσι με το NAT, όχι μόνο χρειάζεται να διαβαστεί η H.323 κυκλοφορία, αλλά πρέπει να τροποποιηθεί έτσι, ώστε οι σωστοί αριθμοί διευθύνσεων/θυρών να στέλνονται σε κάθε ένα από τα ακραία σημεία.

3.6 Σχεδιαγράμματα ασφάλειας H.235

Τα καθορισμένα σχεδιαγράμματα, παρέχουν τα διάφορα επίπεδα ασφαλείας και περιγράφουν ένα υποσύνολο πιθανών μηχανισμών ασφαλείας, που προσφέρονται από το H.235. Περιλαμβάνουν διάφορες επιλογές για την προστασία των επικοινωνιών, π.χ., με τη χρήση διαφόρων επιλογών του H.235.

3.7 Ζητήματα και Απόδοση Κρυπτογράφησης

Σε ένα σύστημα VOIP μπορεί να προστεθεί καθυστέρηση από τους κωδικοποιητές/αποκωδικοποιητές και από επιπρόσθετες επεξεργασίες, όπως η

κρυπτογράφηση. Οι κωδικοποιητές/ αποκωδικοποιητές προσθέτουν καθυστέρηση στην διάρκεια της κωδικοποίησης και της συμπίεσης των δεδομένων φωνής. Ο χρόνος επεξεργασίας αυξάνεται ανάλογα με το βαθμό συμπίεσης, επειδή απαιτούνται μεγαλύτεροι φραγμοί των δεδομένων φωνής για να παραχθούν υψηλότεροι βαθμοί συμπίεσης.

Η κρυπτογράφηση εξυπηρετεί δύο σκοπούς για το VOIP:

- προστασία μυστικότητας, με την κρυπτογράφηση των δεδομένων φωνής
- επικύρωση των μηνυμάτων, η οποία προστατεύει την προέλευση και την ακεραιότητα των πακέτων φωνής.

Η κρυπτογράφηση μπορεί να γίνει χρησιμοποιώντας είτε ένα ρεύμα (stream), είτε ένα φραγμό κρυπτογράφησης. Εάν χρησιμοποιείται ρεύμα κρυπτογράφησης, τότε θα εισάγεται πολύ λίγη καθυστέρηση, ιδιαίτερα, εάν το βασικό ρεύμα μπορεί να παραχθεί πριν ή έστω καθώς φτάνει το δεδομένο φωνής . Σε αυτήν την περίπτωση, θα υπάρξει μόνο ένα bit καθυστέρησης, καθώς εφαρμόζεται το ρεύμα κρυπτογράφησης. Οι φραγμοί κρυπτογράφησης μπορούν να απαιτήσουν έναν φραγμό καθυστέρησης, ο οποίος θα ποικίλει ανάλογα με τη χρησιμοποιούμενη μέθοδο, αλλά ακόμα θα απαιτούνται μικρά overhead .

Σημαντικές επίσης καθυστερήσεις εισάγονται από τον υπολογισμό του HMAC για την επικύρωση. Το HMAC χρησιμοποιείται με τις μυστικές λειτουργίες κλειδιών, όπως το MD5 ή το SHA-1. Το HMAC-MD5 παράγει ένα 128 bit (MAC message authentication code), ενώ το HMAC-SHA-1 παραγάγει ένα MAC 160 bit. Επειδή η λειτουργία HMAC πρέπει να περιμένει να φτάσει ένας πλήρης φραγμός δεδομένων πριν την επεξεργασία, αυτές οι διαδικασίες μπορούν να δημιουργήσουν σημαντικές καθυστερήσεις στη λανθάνουσα κατάσταση. Κατά την άφιξη, πρέπει να εφαρμοστούν οι αντίστροφες διαδικασίες, εισάγοντας περαιτέρω καθυστερήσεις στην απόδοση.

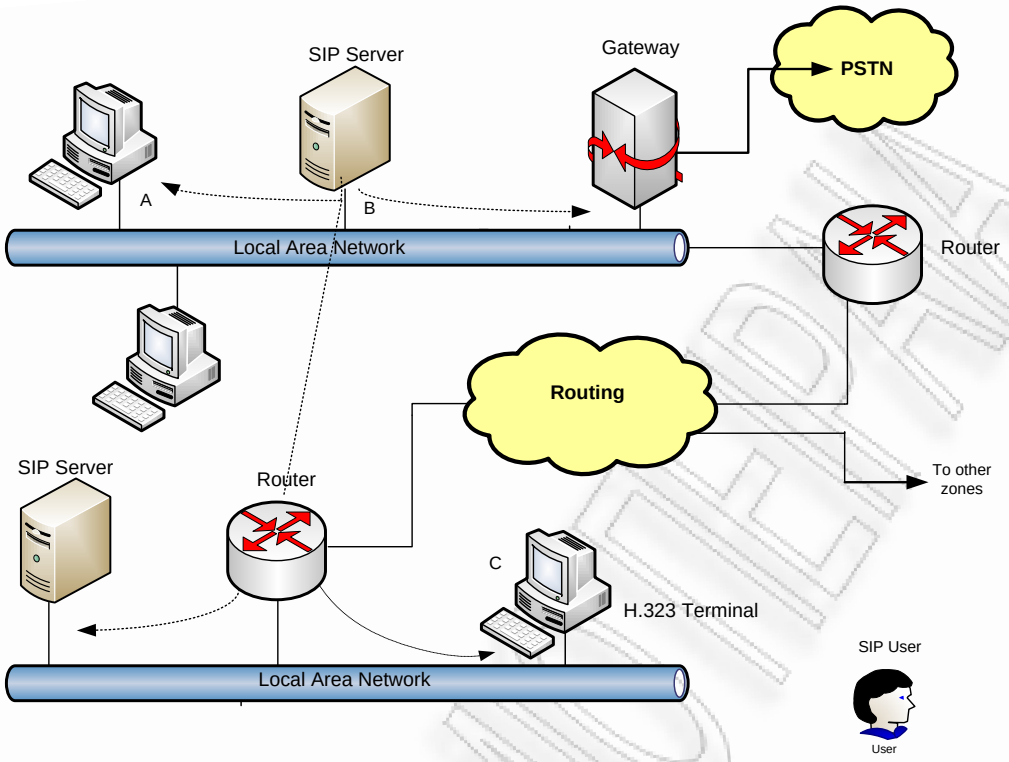
Στις περισσότερες εφαρμογές, η επικύρωση και η ακεραιότητα είναι εξίσου ή περισσότερο, σημαντική από την κρυπτογράφηση, αλλά με την επεξεργασία της φωνής για τους ομιλητές, κάποια επικύρωση είναι αυτόματα ενσωματωμένη και αυτό,

επειδή τα συμβαλλόμενα μέρη αναγνωρίζουν το πρόσωπο στο άλλο τερματικό της συνομιλίας. Ακόμα κι αν η συνομιλία είναι με έναν άγνωστο, η ανησυχία σχετικά με την επικύρωση της πηγής, ισχύει στο ξεκίνημα της κλήσης, παρά στην επικύρωση των πακέτων φωνής στη μέση μιας συνομιλίας. Ως αποτέλεσμα αυτών των εκτιμήσεων, μερικοί σχεδιαστές μπορεί να θεωρήσουν το HMAC λιγότερο σημαντικό για το ασφαλές VOIP, από ότι την κρυπτογράφηση της κλήσης και μπορεί να περιορίσουν τη χρήση του HMAC, εάν η απόδοση είναι πρόβλημα.

Κεφάλαιο 4ο

Πρωτόκολλο SIP

Το SIP (Session Initiation Protocol) είναι ένα πρωτόκολλο σηματοδοσίας που χρησιμοποιείται για τη δημιουργία συνόδων σε ένα IP δίκτυο. Η σύνοδος θα μπορούσε να είναι μια απλή αμφίδρομη τηλεφωνική κλήση ή θα μπορούσε να είναι μια συνδιάσκεψη συνόδου πολυμέσων. Η ικανότητα για τη δημιουργία αυτών των συνόδων σημαίνει ότι μια σειρά από καινοτόμες υπηρεσίες μπορούν να καταστούν δυνατές ,όπως voice-enriched e-commerce, web page click-to-dial, Instant Messaging with buddy lists και IP Centrex services.



Σχήμα 19

Το SIP δημιουργήθηκε από την Internet Engineering Task Force (IETF-συγκεκριμένα από την MMUSIC Working Group) ,το όργανο που είναι υπεύθυνο για τη διαχείριση και την ανάπτυξη των μηχανισμών που συνθέτουν το διαδίκτυο. Αρχικά δημοσιεύτηκε το 1996 ως RFC 2543 και αργότερα το 2002 εξελίχθηκε ως στο RFC 3261 . Τα τελευταία δύο χρόνια, η Voice over IP κοινότητα ενέκρινε το SIP, ως το κύριο πρωτόκολλο σηματοδοσίας και συνεχίζει να εξελίσσεται και επεκτείνεται όπως ωριμάζει η τεχνολογία ενώ συγχρόνως κερδίζει συνεχώς έδαφος στην αγορά.

Το SIP διακρίνεται λίγο πολύ από αυτή την φιλοσοφία. Έχοντας αναπτυχθεί αποκλειστικά ως ένας μηχανισμός για τη θέσπιση συνεδριών, δεν γνωρίζει τις λεπτομέρειες της συνεδρίας παρά μόνο αρχίζει, τερματίζει και τροποποιεί συνεδρίες. Αυτό η απλότητα σημαίνει ότι το SIP διακρίνεται από:

- Την επεκτασιμότητά του
- Και προσαρμόζεται εύκολα σε διαφορετικές αρχιτεκτονικές και σενάρια.

Το SIP είναι ένα request-response (αίτημα-απόκριση) πρωτόκολλο που μοιάζει με δύο άλλα πρωτόκολλα του διαδικτύου ,τα HTTP και SMTP, με συνέπεια να ταιριάζει άνετα δίπλα σε άλλες Internet εφαρμογές. Χρησιμοποιώντας το SIP, η τηλεφωνία γίνεται άλλη μια Web εφαρμογή και ενσωματώνεται εύκολα σε άλλες υπηρεσίες του Internet. Το SIP είναι μια απλή εργαλειοθήκη όπου οι πάροχοι υπηρεσιών μπορούν να χρησιμοποιήσουν για την οικοδόμηση υπηρεσιών φωνής και πολυμέσων. Τέλος για να καταστεί δυνατή η τηλεφωνική επικοινωνία, το SIP χρειάζεται να συνεργαστεί με άλλα πρωτόκολλα όπως:

- Για την εξασφάλιση μεταφοράς (RTP/RTCP).
- Για την συμφωνία των παραμέτρων της κλήσης(SDP).
- Για τον έλεγχο ταυτότητας των χρηστών (ακτίνα, διάμετρος).
- Να παρέχουν καταλόγους (LDAP),
- Να είναι σε θέση να εγγυάται ποιότητα φωνής (RSVP, YESSIR) και διασυνεργασίας με τη σημερινή του τηλεφωνικού δικτύου.

4.1 Αρχιτεκτονική SIP

Η αρχιτεκτονική ενός δικτύου SIP είναι διαφορετική από τη δομή του H.323. Ένα δίκτυο SIP αποτελείται από τα τερματικά, από ένα proxy ή redirect server ή και τα δύο μαζί, από έναν location server και ένα registrar. Το SIP είναι διαιρεμένο σε ένα σύνολο οντοτήτων (SIP Entities) από τις οποίες οι πιο κύριες είναι οι:

- User Agents (UA).
- SIP Εξυπηρετητές -SIP Servers

4.1.1 User Agents (UA)

Οι User Agents εκκινούν και τερματίζουν συνόδους ανταλλάζοντας αιτήσεις (requests) και απαντήσεις responses). Όπως υπονοείται από το όνομα, ένας User Agent παίρνει κάποια είσοδο από το χρήστη και λειτουργεί ως πράκτορας για λογαριασμό του χρήστη για την εγκατάσταση και τον τερματισμό διαλόγων με άλλους χρήστες. Κάθε UA πρέπει να διατηρεί πληροφορίες για την κατάσταση των κλήσεων, τις οποίες εκκινεί ή στις οποίες συμμετέχει. Οι πληροφορίες αυτές χρησιμοποιούνται και για την αποθήκευση των πληροφοριών για κάθε διάλογο, αλλά και για λόγους αξιοπιστίας.

Σύμφωνα με το RFC 3261 ο User Agent αποτελείται από έναν User Agent Client (UAC) και έναν User Agent Server (UAS).Ένας UAC μπορεί να δημιουργεί αιτήσεις οι οποίες προκύπτουν από έναν εξωτερικό παράγοντα (π.χ. το πάτημα από τον χρήστη ενός κουμπιού ή κάποιο σήμα στην τηλεφωνική γραμμή) και να επεξεργάζεται απαντήσεις. Ανάλογα ένας UAS είναι ικανός να λαμβάνει αιτήσεις και να δημιουργεί απαντήσεις οι οποίες μπορεί να προκύπτουν από τον χρήστη, το αποτέλεσμα της εκτέλεσης ενός προγράμματος ή μέσω ενός άλλου μηχανισμού. Η επεξεργασία της κάθε αίτησης γίνεται σε ατομικό επίπεδο και αν γίνει αποδεκτή τότε όλες οι αλλαγές κατάστασης που θα προκύψουν στον UAS πρέπει να εκτελεστούν αλλιώς καμία αλλαγή κατάστασης δεν πρέπει να γίνει.

4.1.2 Proxy Server

Ο Proxy Server, είναι υπεύθυνος για την δρομολόγηση των SIP αιτήσεων στους UAS και των SIP απαντήσεων στους UAC. Μία αίτηση μπορεί να περάσει από πολλούς Proxies μέχρι να φτάσει στον τελικό της στόχο. Κάθε Proxy παίρνει με τη σειρά του αποφάσεις για τη σωστή δρομολόγηση της αίτησης, μεταβάλλοντας την αίτηση προτού την προωθήσει. Οι απαντήσεις δρομολογούνται μέσω των ίδιων Proxies προς την αντίθετη κατεύθυνση αυτή τη φορά.

Είναι χρήσιμο να θεωρήσει κανείς τους Proxies ως δρομολογητές του SIP-επιπέδου, που προωθούν τις SIP αιτήσεις και απαντήσεις. Η λογική που χρησιμοποιούν είναι όμως πιο πολύπλοκη από μια απλή προώθηση μηνυμάτων, που βασίζεται σε έναν πίνακα δρομολόγησης. Οι προδιαγραφές του SIP επιτρέπουν στους Proxies να προβαίνουν σε ενέργειες, όπως είναι η εγκυρότητα των αιτήσεων , η ταυτοποίηση των χρηστών και ο εντοπισμός και χειρισμός ατερμόνων βρόχων. Η πολλαπλή χρησιμότητά τους επιτρέπει στο διαχειριστή του συστήματος να τους χρησιμοποιεί για διάφορους λόγους και σε διάφορες τοποθεσίες του δικτύου.

Ένας Proxy είναι σχεδιασμένος με τέτοιο τρόπο, ώστε η λειτουργία του να είναι όσο πιο διαφανή γίνεται στους UAs. Στους Proxy Servers επιτρέπεται να αλλάξουν οποιοδήποτε μήνυμα μόνο με κάποιους καθορισμένους και περιορισμένους τρόπους. Για παράδειγμα, δε μπορούν σε καμία περίπτωση να αλλάξουν το SDP σώμα ενός INVITE. Πλην κάποιων εξαιρέσεων , οι Proxies μπορούν να ξεκινήσουν αιτήσεις με δική τους πρωτοβουλία. Δε μπορούν όμως να τερματίσουν έναν ενεργό διάλογο στέλνοντας ένα BYE Request οι ίδιοι. Ένας Proxy Server διαχωρίζεται σε δύο κατηγορίες α) Stateful Proxy Server και β) Stateless proxy Server.

4.1.2 Redirect Servers

Ο Εξυπηρετητής Ανακατεύθυνσης (Redirect Server) λαμβάνει SIP αιτήσεις και δίνει μια απάντηση της κλάσης 3xx, κατευθύνοντας τον πελάτη να επικοινωνήσει με μια εναλλακτική ομάδα SIP διευθύνσεων. Οι εναλλακτικές διευθύνσεις υπάρχουν στο πεδίο Contact της επικεφαλίδας της απάντησης.

Η ανακατεύθυνση δίνει τη δυνατότητα στους Servers να επιστρέφουν πληροφορίες δρομολόγησης στους πελάτες, βοηθώντας στον εντοπισμό του στόχου, ενώ οι ίδιοι δε λαμβάνουν πλέον μέρος στη SIP συναλλαγή. Κατά συνέπεια, οι Redirect Servers δεν κρατάνε πληροφορίες για την κατάσταση των διαλόγων, αλλά μόνο για την πορεία ανεξάρτητων συναλλαγών που χειρίζονται οι ίδιοι. Η ανακατεύθυνση είναι μια απλή και γρήγορη διαδικασία, που επιτρέπει στους Redirect Servers να επιτυγχάνουν υψηλή απόδοση.

4.1.2 Registrar Servers

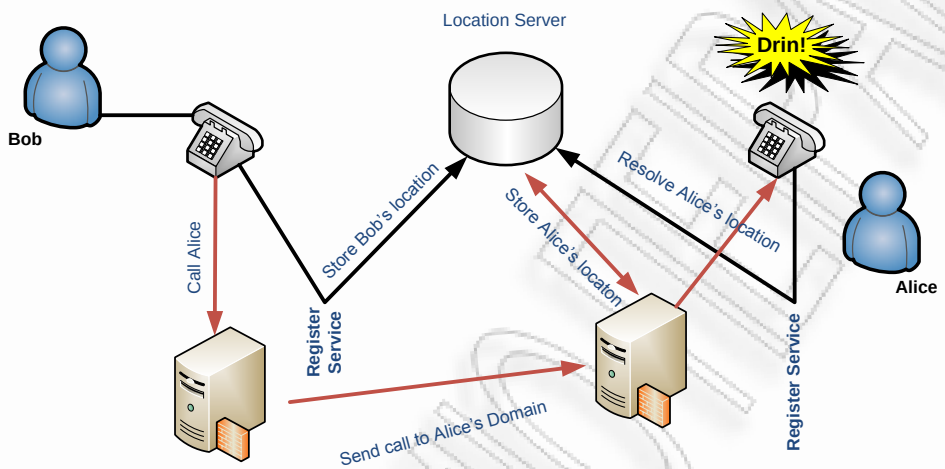
Ο Registrar ή Εξυπηρετητής Εγγραφών δέχεται αιτήσεις εγγραφής (REGISTER Requests) και τοποθετεί όσες πληροφορίες λαμβάνει στο Location Service για το domain που χειρίζεται. Κάθε Registrar χειρίζεται τα REGISTER Requests για ένα συγκεκριμένο domain ή σύνολο domains. Χρησιμοποιεί το Location Service (μια αφηρημένη βάση με τοποθεσίες) για την αποθήκευση και την ανάκτηση πληροφοριών για τη θέση των χρηστών. Ο Location Service μπορεί να τρέχει σε ένα απομακρυσμένο μηχάνημα και η επικοινωνία μαζί του να γίνεται με τη χρήση ενός κατάλληλου πρωτοκόλλου (π.χ. με το LDAP). Η επιλογή εξαρτάται από την εκάστοτε υλοποίηση. Μερικές υλοποιήσεις μπορούν να τοποθετήσουν το Location Service και το Registrar στο ίδιο μηχάνημα.

Ο Registrar μπορεί να ζητήσει ταυτοποίηση των εισερχόμενων αιτήσεων χρησιμοποιώντας την 401 (Unauthenticated) απάντηση, ενώ απορρίπτει την αίτηση, αν λάβει κάποιο μήνυμα με μέθοδο άλλη από τη REGISTER δίνοντας μια 501 (Not Implemented) απάντηση. Συνήθως ένας Registrar συνυπάρχει στο ίδιο σύστημα με έναν Proxy και έναν Redirect Server και η διαφοροποίηση υφίσταται μόνο λογικά και όχι φυσικά.

Εάν υποθέσουμε ότι ο Bob επιθυμεί να κάνει μια κλήση στην Alice, στέλνει ένα αίτημα (invite) στον proxy server περιλαμβάνοντας πληροφορίες SDP για την επικοινωνία, που διαβιβάζονται στον χρήστη Alice από τον proxy του Bob, ενδεχομένως μέσω του proxy της Alice. Τελικά, υποθέτοντας ότι η Alice θέλει να αποδεχθεί την κλήση του Bob και να μιλήσει σε αυτόν, θα στείλει ένα απαντητικό μήνυμα "OK" που θα περιέχει τις δικές της προτιμήσεις κλήσης σε SDP.

Κατόπιν ο Bob θα αποκριθεί με ένα μήνυμα επιβεβαίωσης "ACK". Το SIP επιτρέπει στο ACK να περιέχει SDP αντί του INVITE, έτσι ώστε ένα INVITE να μπορεί να φανεί χωρίς συγκεκριμένες πληροφορίες πρωτοκόλλου. Αφότου παραληφθεί το "ACK", η συνομιλία μπορεί να αρχίσει μέσω των θυρών RTP/RTCP που έχουν συμφωνήσει προηγουμένως.

Παρατηρείται ότι όλη η μετάδοση πληροφοριών μεταφέρθηκε μέσω μίας θύρας με μία απλή μορφή (κείμενο), χωρίς καμία περίπλοκη μετατροπή channel/ports που να έχει σχέση με το H.323. Επιπλέον, το SIP παρουσιάζει μία πληθώρα παροχών για αντιπυρικές ζώνες (firewalls) και NAT.



Σχήμα 20 ***Αρχιτεκτονική ενός SIP δικτύου***

4.2 Χαρακτηριστικά Γνωρίσματα Ασφαλείας στο SIP

Το RFC 3261 περιγράφει διάφορα χαρακτηριστικά γνωρίσματα ασφάλειας για το SIP. Το RFC 3261 δεν υποστηρίζει κάποια χαρακτηριστικά γνωρίσματα ασφάλειας, τα οποία είχαν υποστηριχθεί στο αρχικό RFC 2543, όπως η χρήση του PGP και του HTTP Basic Authentication.

4.2.1 Επικύρωση Δεδομένων Σηματοδότησης (Authentication of Signaling Data) που χρησιμοποιεί το HTTP Digest Authentication

Το Digest Authentication είναι βασισμένο στην εφαρμογή πρόσκληση – απόκριση, προσκαλώντας το απομακρυσμένο τερματικό χρησιμοποιώντας ένα nonce value. Το SIP Digest Authentication είναι βασισμένο στο Digest Authentication που καθορίζεται στο RFC 2617. Μια έγκυρη απάντηση περιέχει έναν συγκεντρωτικό έλεγχο (εξ ορισμού, το συγκεντρωτικό έλεγχο του MD5) στο user name, το password, το nonce value που έχει δοθεί, τη μεθόδου HTTP και το ζητούμενο URI. Κατ' αυτό τον τρόπο, ο κωδικός πρόσβασης ποτέ δε στέλνεται με σαφήνεια. Λόγω αυτής της αδυναμίας στην ασφάλειά του και προκειμένου να αποφευχθούν επιθέσεις με τον υποβιβασμό του απαιτούμενου επιπέδου ασφάλειας του Authentication, το HTTP Basic Authentication δεν συστήθηκε στο τρέχον σχέδιο RFC 3261.

42.2 Χρήση S/MIME στο SIP

Τα μηνύματα SIP αποτελούνται από MIME (Multipurpose Internet Mail Extensions) στοιχεία, τα οποία καθορίζουνε μηχανισμούς για την προστασία της ακεραιότητας και την κρυπτογράφηση του περιεχομένου του.

Το SIP μπορεί να χρησιμοποιήσει το S/MIME για να ενεργοποιήσει μηχανισμούς, όπως η διανομή δημοσίων κλειδιών, η επικύρωση και η προστασία της ακεραιότητας ή η εμπιστευτικότητα σηματοδότησης των δεδομένων του SIP. Το S/MIME μπορεί να θεωρηθεί ως αντικατάσταση του PGP ώστε να παρέχει τα μέσα για την προστασία της ακεραιότητας και την κρυπτογράφηση των μηνυμάτων SIP.

Στο δημοσίευμα RFC 3261, συστήνεται το S/MIME για να χρησιμοποιηθεί σε UAs (User Agent server). Επιπλέον, εάν το S/MIME χρησιμοποιείται στη διάνοιξη μηνυμάτων, συστήνεται η χρήση μιας σύνδεσης TCP λόγω του μεγέθους των μηνυμάτων. Αυτό συμβαίνει για να αποφευχθούν προβλήματα που μπορεί να προκύψουν από τον τεμαχισμό των UDP πακέτων.

Έτσι, οι ακόλουθες υπηρεσίες μπορούν να πραγματοποιηθούν με:

* επικύρωση και προστασία της ακεραιότητας των δεδομένων σηματοδότησης,
* εμπιστευτικότητα των δεδομένων σηματοδότησης.

4.2.3 Εμπιστευτικότητα των Media Data

Το ίδιο το SIP δεν εξετάζει την κρυπτογράφηση των media data. Ωστόσο, χρησιμοποιώντας την RTP κρυπτογράφηση, όπως ορίζεται στο δημοσίευμα RFC 1889, μπορεί να παρέχει την εμπιστευτικότητα για τα media data. Μια άλλη επιλογή για την ασφάλεια των media stream είναι η χρήση του SRTP (Secure Real-time Transport Protocol). Για τη διαχείριση κλειδιών μπορεί να χρησιμοποιηθεί το SDP (RFC 2327). Το SDP μπορεί να μεταβιβάσει τα κλειδιά επικοινωνίας (session keys) για τα media stream.

Αξίζει να σημειωθεί ότι η χρήση του SDP για τη ανταλλαγή κλειδιών δεν παρέχει καμία μέθοδο για να σταλεί ένα κρυπτογραφημένο media stream κλειδί. Επομένως, το αίτημα της σηματοδότησης θα πρέπει να κρυπτογραφηθεί, κατά προτίμηση με τη χρήση της κρυπτογράφησης End-to-End.

4.3 Χρήση IPsec στο SIP

Το πρωτόκολλο IPsec (Internet Protocol security) μπορεί να χρησιμοποιηθεί για την παροχή ασφάλειας σε SIP σηματοδότηση. Αυτός ο τύπος ασφάλειας ταιριάζει περισσότερο στην εξασφάλιση των χρηστών του SIP, για παράδειγμα σε ένα σενάριο SIP VPN (SIP χρήστες agents/proxies) ή μεταξύ των περιοχών διαχείρισης του SIP (administrative SIP domains).

Το πρωτόκολλο IPsec είναι συμβατό είτε με το UDP, το TCP είτε με το SCTP που είναι βασισμένα στη σηματοδότηση του SIP και χρησιμοποιείται για να παρέχει την

επικύρωση, την ακεραιότητα και την εμπιστευτικότητα για τα διαβιβάζοντα δεδομένα και υποστηρίζει σενάρια end-to-end εξίσου καλά όπως και σενάρια hop-by-hop.

Ένα αποδεκτό πρωτόκολλο για τη βασική διαχείριση κλειδιών είναι το Internet Key Exchange (IKE). Είναι ένα υβριδικό πρωτόκολλο βασισμένο στο Internet Security Association and Key Management Protocol (ISAKMP), στο Oakley Key Determination Protocol (RFC 2412) και στο Secure Key Exchange Mechanism για το Internet (SKEME).

Το πρωτόκολλο IKE παρέχει αυτοματοποιημένους κρυπτογραφημένους μηχανισμούς ανταλλαγής και διαχείρισης κλειδιών για το IPsec. Το πρωτόκολλο IKE χρησιμοποιείται για να διαπραγματεύεται τα security associations (SAs) με αυτόνομη χρήση της διαχείρισης των κλειδιών ανταλλαγής (αποκαλούμενες Phase 1) και για άλλες υπηρεσίες όπως το IPsec (αποκαλούμενο Phase 2). Το IKE χρησιμοποιείται ιδιαίτερα στην καθιέρωση των VPNs.

4.4 Επαυξημένη Ασφάλεια στο SIP

Αυτήν την περίοδο μέσα στο IETF διάφορα σχέδια σχετικά με την ασφάλεια συζητούνται, και επικρατεί μια άποψη, μιας γενικής λύσης ασφάλειας στα σενάρια του SIP. Διάφορα σχέδια έχουν παραχθεί σχετικά με την επικύρωση, την ακεραιότητα, και την εμπιστευτικότητα για το SIP. Οι ακόλουθες υποενότητες παρέχουν μια σύντομη επισκόπηση των σχεδίων του διαδικτύου, από όπου και μπορούμε να καταλάβουμε ότι επιζητείται αύξηση της ασφάλειας για τα κοινά σενάρια του SIP.

4.4.1 SIP Authenticated Identity Body (AIB)

Το SIP Authenticated Identity Body (AIB) καθορίζει ένα γενικό δείγμα επικύρωσης του SIP. Το δείγμα αυτό παρέχεται με την προσθήκη του S/MIME σε ένα αίτημα ή μια απάντηση του SIP, προκειμένου να παρασχεθεί η ακεραιότητα αναφοράς πέρα

από τις κεφαλίδες του. Αυτό είναι ένα ψηφιακά υπογεγραμμένο μήνυμα SIP (sip/message) ή τμήμα μηνυμάτων (sip/frag).

4.4.2 SIP Authenticated Identity Management (AIM)

Οι ήδη υπάρχοντες μηχανισμοί οι οποίοι χρησιμοποιούνται για την ανάδειξη της ταυτότητας στο SIP, συχνά δεν επιτρέπουν σε ένα διαχειριστικό σύστημα (administrative domain) να ελέγξει με ασφάλεια την ταυτότητα του δημιουργού ενός αιτήματος. Θα πρέπει λοιπόν να διανέμονται με κρυπτογραφικό τρόπο οι ασφαλείς επικυρωμένες ταυτότητες μέσα στα μηνύματα του SIP, συμπεριλαμβανομένου και μίας ένδειξης επικύρωσης (όπως MIME). Αυτή η ένδειξη προστίθεται μετά στο μήνυμα.

4.4.3 Η Απαίτηση του S/MIME AES στο SIP

Στο δημοσίευμα RFC 3261 ορίζεται το 3DES ως ο ελάχιστος απαραίτητος αλγόριθμος κρυπτογράφησης για τις εφαρμογές του S/MIME στο SIP. Αν και το 3DES είναι ακόμα ένας βιώσιμος αλγόριθμος, υπάρχει και ένας βελτιωμένος, ο AES, που είναι ουσιαστικά μία αντικατάσταση του DES και του 3DES. Το AES παρέχει υψηλότερο ρυθμό απόδοσης και χαμηλότερη υπολογιστική πολυπλοκότητα από ότι το 3DES. Επίσης μπορεί να εφαρμοστεί σε απαιτήσεις χαμηλότερης μνήμης, κάνοντάς το καταλληλότερο για τις κινητές ή ενσωματωμένες συσκευές, συμπεριλαμβανομένων και των τηλεφώνων συσκευών του VOIP.

4.4.4 Το Security Mechanism Agreement (SMA) στο SIP

Το SIP έχει διάφορους μηχανισμούς ασφάλειας. Μερικοί από αυτούς έχουν άμεσα ενσωματωθεί στο πρωτόκολλο SIP, όπως η επικύρωση του HTTP. Αυτοί οι μηχανισμοί έχουν εναλλακτικούς αλγορίθμους και παραμέτρους.

Η ιδέα αυτή προέρχεται από την 3η Generation Partnership Project (3GPP), μια συνεργασία επιχειρήσεων τηλεπικοινωνίας, και παρέχει έναν μηχανισμό με τον οποίο γίνεται η επιλογή του μηχανισμού ασφάλειας που θα χρησιμοποιηθεί μεταξύ δύο οντοτήτων. Το RFC 3261 δεν παρέχει κανέναν μηχανισμό συμφωνίας επιλογών. Επιπλέον, ακόμα κι αν μερικοί μηχανισμοί όπως τα OPTIONS χρησιμοποιήθηκαν για την ανάδειξη μηχανισμών συμφωνίας, η συμφωνία αυτή θα ήταν τρωτή στις επιθέσεις Bidding - Down (μια φάση επίθεσης man-in-the-middle, όπου ο επιτιθέμενος τροποποιεί τα μηνύματα για να πείσει τα επικοινωνούντα συμβαλλόμενα μέρη ότι και οι δύο πλευρές υποστηρίζουν μόνο τους αδύνατους αλγορίθμους).

Τρία πεδία κεφαλίδων καθορίζονται για τη διαπραγμάτευση των μηχανισμών ασφάλειας μέσα στο SIP, και συγκεκριμένα μεταξύ μιας οντότητας SIP User Agent και του επόμενου άλματος SIP server. Αυτά είναι προτεινόμενα πρότυπα (RFC 3329) από το IETF.

Πέντε μηχανισμοί υποστηρίζονται αυτήν την περίοδο:

- TLS
- Αφομοίωση του HTTP
- IPsec με IKE
- Χειροκίνητο κλείδωμα IPsec χωρίς IKE
- S/MIME

Κεφάλαιο 5ο

Media Gateways

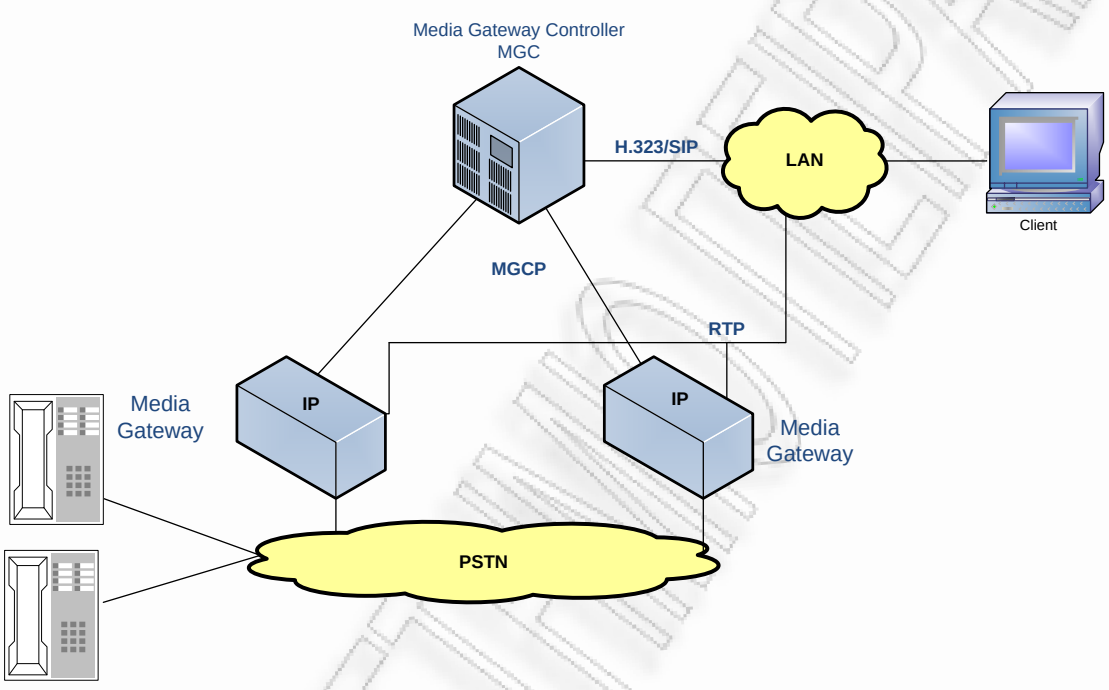
Οι Media Gateways αποτελούν ένα από τα βασικά στοιχεία του IP τηλεφωνικού δικτύου, καθώς είναι υπεύθυνα για την μετάδοση των πληροφοριών στους χρήστες του δικτύου και στους χρήστες του εξωτερικού κόσμου. Είναι συμβατά με διάφορα πρωτόκολλα όπως H.323, SIP, RTP, Q.SIG κτλ, ενώ τα ίδια υποστηρίζουν το Megaco/H.248 πρωτόκολλο και το MGCP (Media Gateway Control Protocol) .

5.1 MGCP (Media Gateway Control Protocol)

Το πρωτόκολλο MGCP χρησιμοποιείται για την επικοινωνία των στοιχείων του voip gateway και αποτελεί ένα συμπληρωματικό πρωτόκολλο των SIP και H.323. Το πρωτόκολλο MGCP προήλθε από την έκδοση 1.1 του πρωτοκόλλου SGCP, το οποίο ήταν ένας συνδυασμός της έκδοσης 1 του SGCP και του IPDC.

5.1.1 Αρχιτεκτονική MGCP

Ο MGC server είναι υπεύθυνος για την διαχείριση των κλήσεων και την ολοκλήρωση των δυνατοτήτων που παρέχονται τους χρήστες. Οι δυνατότητες αυτές διαχέονται στους χρήστες και κατά συνέπεια στο PSTN δίκτυο μέσω των Media Gateways οι οποίοι είναι συνδεδεμένοι με τον MGC.



Σχήμα 21

5.1.2 Εκτιμήσεις Ασφάλειας

Η πραγματικότητα είναι πως δεν έχει σχεδιαστεί κάποιος μηχανισμός ασφάλειας που στο ίδιο το MGCP πρωτόκολλο. Το έγγραφο RFC 2705 αναφέρεται στη χρήση IPsec (είτε AH είτε ESP) για να προστατεύσει τα MGCP μηνύματα. Χωρίς αυτή θα μπορούσανε να πραγματοποιηθούν μη εξουσιοδοτημένες κλήσεις ή να παρεμποδιστούν τρέχουσες εξουσιοδοτημένες κλήσεις. Εκτός από τη χρήση του IPsec, το MGCP επιτρέπει στον call agent να παρέχει gateways με κλειδιά συνόδου (session keys) που να μπορούν να χρησιμοποιηθούν για την κρυπτογράφηση των ακουστικών μηνυμάτων, προκειμένου να προστατευθούν από υποκλοπές. Το κλειδί συνόδου θα χρησιμοποιηθεί αργότερα στην κρυπτογράφηση RTP. Η κρυπτογράφηση RTP, που περιγράφεται στο RFC 1889, μπορεί να εφαρμοστεί. Τα κλειδιά συνόδου

μπορούν να μεταφερθούν μεταξύ του call agent και του gateway με τη χρήση του SDP (RFC 2327).

5.2 Megaco/H.248

Το Megaco/H.248 είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για την επικοινωνία του MGC και του Media Gateway, προκειμένου να επιτευχθεί η μετάδοση της πληροφορίας.

5.2.1 Αρχιτεκτονική Megaco/H.248

Το MEGACO/H.248 έχει βασικά την ίδια αρχιτεκτονική με το MGCP. Οι εντολές του MEGACO/H.248 είναι παρόμοιες με τις εντολές του MGCP. Εντούτοις, τα πρότυπα πρωτοκόλλου είναι αρκετά διαφορετικά. Το MEGACO ερμηνεύει ένα πρότυπο σύνδεσης των gateways που έχει δύο οντότητες: τις λήξεις (πηγή για ένα ή περισσότερα media streams), και το πλαίσιο (ομαδοποίηση των λήξεων που συνδέονται σε μια κλήση). Αντίθετα, το MGCP χρησιμοποιεί τις ακόλουθες δύο οντότητες: τα τερματικά (πηγή των δεδομένων), και την σύνδεση (ένωση μεταξύ δύο τερματικών).

5.2.2 Εκτιμήσεις Ασφάλειας

Το Megaco (RFC 3525) συστήνει μηχανισμούς ασφάλειας που μπορούν να κρυφτούν κάτω από μηχανισμούς μεταφοράς δεδομένων, όπως το IPsec. Το πρωτόκολλο H.248 πηγαίνει ένα βήμα παρακάτω με την απαίτηση ότι οι εφαρμογές του εφαρμόζουν IPsec, εάν το λειτουργικό σύστημα και τα δίκτυα μεταφοράς υποστηρίζουν το IPsec. Το H.248 δηλώνει ότι οι εφαρμογές που χρησιμοποιούν την κεφαλίδα AH θα παρέχουν ένα ελάχιστο σύνολο αλγορίθμων για τον έλεγχο της ακεραιότητας, χρησιμοποιώντας τα χειρωνακτικά κλειδιά (manual keys – RFC 2402).

5.3 Λύσεις σε Θέματα Ασφάλειας στο IP Τηλεφωνικό Δίκτυο

5.3.1 Κρυπτογράφηση στα Ακραία Σημεία

Μια προτεινόμενη λύση για τη συμφόρηση στους δρομολογητές λόγω της κρυπτογράφησης είναι να αντιμετωπιστεί η κρυπτογράφηση / από-κρυπτογράφηση στα ακραία σημεία του δικτύου VOIP. Μια εκτίμηση με αυτήν τη μέθοδο είναι, ότι τα ακραία σημεία πρέπει να είναι υπολογιστικά αρκετά ισχυρά, ώστε να χειριστούν το μηχανισμό κρυπτογράφησης.

Όμως τα κλασικά ακραία σημεία είναι λιγότερο ισχυρά από ότι οι πύλες, οι οποίες μπορούν να επηρεάσουν την επιτάχυνση του υλικού, σε περίπτωση πολλαπλών πελατών. Αν και η ιδανική κρυπτογράφηση θα έπρεπε να διατηρείται σε κάθε άλμα στη διάρκεια ζωής ενός VOIP πακέτου, αυτό μπορεί να μην είναι εφικτό με τα απλά IP τηλέφωνα, τα οποία διαθέτουν περιορισμένες δυνατότητες λογισμικού ή υπολογιστικής δύναμης.

Σε τέτοιες περιπτώσεις, είναι προτιμότερο να κρυπτογραφούνται τα δεδομένα μεταξύ ακραίου σημείου και δρομολογητή (ή αντίστροφα), αλλά η μη κρυπτογραφημένη κυκλοφορία στο LAN είναι ελαφρώς λιγότερο καταστρεπτική, από ότι η μη κρυπτογραφημένη κυκλοφορία σε όλο το Διαδίκτυο. Ευτυχώς, η αυξανόμενη δύναμη επεξεργασίας των νεότερων τηλεφωνικών συσκευών, κάνει την κρυπτογράφηση στα ακραία σημεία λιγότερο προβληματική.

Επιπλέον, το SRTP και το MIKEY είναι τα μελλοντικά πρωτόκολλα για την κρυπτογράφηση των μέσων και τη διαχείριση των κλειδιών, που επιτρέπει την ασφαλή αλληλεπίδραση μεταξύ του H.323 και των βασισμένων στο SIP πελατών.

5.3.2 Secure Real Time Protocol (SRTP)

Το Real-Time Transport Protocol (πρωτόκολλο μεταφοράς πραγματικού χρόνου) ορίζει ένα τυπικό μορφότυπο πακέτου για την παράδοση ήχου και εικόνας με χαρακτηριστικά πραγματικού χρόνου μέσω του διαδικτύου. Δημιουργήθηκε από τον όμιλο Audio Video Transport Working του IETF και δημοσιεύτηκε για πρώτη φορά το 1996 ως RFC 1889. Έπειτα ανανεώθηκε το 2003 και ορίζεται στο RFC 3550.

Το RTP χρησιμοποιείται συνήθως σε:

- Simple multicast Audio Conference: συνδιάσκεψη μόνο φωνής σε
- Audio and Video Conference:Συνδιάσκεψη με ήχο και εικόνα.
- Mixers and Translators: Οι μεταφραστές απλώς μεταφράζουν μια μορφή ωφέλιμου φορτίου σε μια άλλη, ενώ οι μίκτες συνδυάζουν πολλαπλά ρεύματα σε ένα απλό ρεύμα διατηρώντας την αρχική τους μορφή. Μίκτες και μεταφραστές χρησιμοποιούνται συνήθως για την μετάδοση σε δίκτυα χαμηλών και υψηλών ταχυτήτων ταυτόχρονα(low-speed networks and high-speed networks).
- Layered Encodings: Ελέγχει τον ρυθμό μετάδοσης από την πλευρά του δέκτη και απελευθερώνει την πηγή συνδυάζοντας ένα σύστημα layered-encoding και ένα layered-transmission(rate-adaption στον δέκτη).

Το RTP είναι στενά συνδεδεμένο με το RTCP πρωτόκολλο(Real Time Control Protocol). Ενώ το RTP χρησιμοποιείται για την μεταφορά των δεδομένων το RTCP παρέχει πληροφορίες ποιότητας της συνόδου (QoS) καθώς και των μελών της συνόδου. Συνήθως τα RTP- RTCP δεσμεύουν τις θύρες μεταξύ 16384-32767. Το RTP δεσμεύει μια θύρα ζυγού αριθμού ενώ το RTCP την αμέσως επόμενη μονή.

Παρόλο που το κύριο πεδίο εφαρμογής για το οποίο είναι αρχικά σχεδιασμένο το RTP είναι η ικανοποίηση των αναγκών πολυμελούς τηλεδιάσκεψης πολυμέσων, εντούτοις δεν περιορίζεται στη συγκεκριμένη εφαρμογή. Εφαρμογές αποθήκευσης continuous δεδομένων, interactive distributed simulation, active badge, εφαρμογές ελέγχου και μετρήσεων και άλλες εφαρμογές πραγματικού χρόνου μπορούν να χρησιμοποιήσουν το RTP ικανοποιητικά.

Το RTP παρέχει υπηρεσίες μεταφοράς από άκρο σε άκρο, αλλά δεν παρέχει όλη την λειτουργικότητα που παρέχεται από ένα τυπικό πρωτόκολλο μεταφοράς. Για παράδειγμα, το RTP συνήθως λειτουργεί στην κορυφή του UDP για να χρησιμοποιεί τις υπηρεσίες πολύπλεξης και αθροίσματος ελέγχου του πρωτοκόλλου αυτού. Μπορεί όμως να λειτουργεί και πάνω από IPX δίκτυα ή πάνω ATM δίκτυα. Το RTP δεν γνωρίζει την έννοια της σύνδεσης και γι αυτό μπορεί να λειτουργεί είτε πάνω από προσανατολισμένα κατά σύνδεση δίκτυα είτε πάνω από χωρίς σύνδεση πρωτόκολλα χαμηλού επιπέδου.

Το SRTP :

- παρέχει ένα πλαίσιο για την κρυπτογράφηση και την επικύρωση μηνυμάτων των RTP και RTCP ρευμάτων
- μπορεί να επιτύχει υψηλή απόδοση ρυθμού και χαμηλή επέκταση πακέτων
- είναι ανεξάρτητο από μια συγκεκριμένη εφαρμογή RTP σωρών και από συγκεκριμένα πρότυπα κλειδιά διαχείρισης, εν αντιθέσει με το Multimedia Internet Keying (MIKEY) που έχει σχεδιαστεί να λειτουργεί με το SRTP.

Το AES σε counter mode είναι ο προεπιλεγμένος αλγόριθμος, εάν επιδιώκεται κρυπτογράφηση. Το AES-f8 mode είναι μια επιλογή για τις UMTS εφαρμογές. Η προκαθορισμένη μετατροπή επικύρωσης είναι η HMAC-SHA1. Η προεπιλεγμένη σύνοδος επικύρωσης μήκους κλειδιού είναι 160 bits και έτσι η προεπιλεγμένη επικύρωση μήκους ετικέτας θα είναι 80 bits.

Η λειτουργία παραγωγής κλειδιών είναι η AES σε counter mode με ένα κύριο κλειδί διαχείρισης 128 bits. Σε σύγκριση με τις επιλογές ασφαλείας για το RTP, υπάρχουν μερικά πλεονεκτήματα στη χρήση του SRTP. Στη συνέχεια παρουσιάζονται τα πλεονεκτήματα της πρότυπης RTP και H.235 ασφάλειας των media stream δεδομένων.

Το SRTP παρέχει αυξημένη ασφάλεια, η οποία πραγματοποιείται ως εξής:

- Εμπιστευτικότητα για το RTP καθώς επίσης και για το RTCP, κρυπτογραφώντας τα αντίστοιχα ωφέλιμα φορτία
- Ακεραιότητα για ολόκληρα τα RTP και RTCP πακέτα, μαζί με την προστασία επανάληψης
- Η δυνατότητα να αναζωογονούνται περιοδικά τα session keys, τα οποία περιορίζουν την ποσότητα κρυπτογραφημένου κειμένου που παράγεται από ένα σταθερό κλειδί, διαθέσιμο για έναν αντίπαλο στην κρυπτο-αναλυση
- Ένα εκτατό πλαίσιο που επιτρέπει την αναβάθμιση με τους νέους αλγορίθμους κρυπτογράφησης
- Ένα ασφαλές session key με μια ψευδοτυχαία λειτουργία και στα δύο άκρα
- Η χρήση των salting keys που προστατεύουν από τις μη αναμενόμενες επιθέσεις
- Ασφάλεια της μονής και της πολλαπλής εκπομπής των RTP εφαρμογών.

Το SRTP έχει βελτιώσει την απόδοση που επιτυγχάνεται ως εξής:

- Χαμηλό υπολογιστικό κόστος που επιβεβαιώνεται από τους προκαθορισμένους αλγορίθμους
- Χαμηλό κόστος εύρους ζώνης και έναν υψηλό ρυθμό απόδοσης από τον περιορισμό της επέκτασης των πακέτων και από ένα πλαίσιο που συντηρεί την αποδοτικότητα συμπίεσης της RTP κεφαλίδας
- Μικρό ίχνος, που είναι ένας κώδικας μικρού μεγέθους και μία μνήμη δεδομένων, για τη διαμόρφωση των καταλόγων πληροφοριών και επανάληψης.

Τα ακόλουθα χαρακτηριστικά επίσης υποστηρίζουν το SRTP:

- Ορίζεται ως ένα RTP σχεδιάγραμμα, έτσι ώστε να μπορεί να ενσωματωθεί εύκολα στους υπάρχοντες RTP σωρούς. Για παράδειγμα, το SRTP μπορεί να χρησιμοποιήσει το RTP επειδή το κρυπτογραφημένο μέρος είναι το ακριβές μέγεθος του κειμένου για τους προκαθορισμένους αλγορίθμους.

- Παρέχει ανεξαρτησία από τις βαθύτερες αιτίες της μεταφοράς, του δικτύου και των φυσικών στρωμάτων που χρησιμοποιούνται από το RTP. Ειδικότερα την υψηλή ανοχή στην απώλεια και την εκ νέου παραγγελία πακέτων καθώς και την πληθώρα στα λανθασμένα μεταδιδόμενα bit στο κρυπτογραφημένο ωφέλιμο φορτίο.

- Αποφορτίζει τη διαχείριση κλειδιών εξαιτίας του γεγονότος, ότι ένα ενιαίο κύριο κλειδί μπορεί να παρέχει το υλικό διαμόρφωσης για την προστασία της εμπιστευτικότητας και της ακεραιότητας, τόσο για το ρεύμα SRTP όσο και για το αντίστοιχο ρεύμα SRTCP. Για τις ειδικές απαιτήσεις ένα ενιαίο κύριο κλειδί μπορεί να προστατεύσει αρκετά SRTP ρεύματα.

Επειδή το SRTP ορίζεται ως ένα RTP σχεδιάγραμμα, μπορεί να χρησιμοποιηθεί με τα υπάρχοντα πρότυπα πολυμέσων. Η υποστήριξη του H.323 SRTP, καθορίζεται μέσα στο H.235 Annex g, για SIP ή για πιο ακριβείς SDP αυξήσεις που έχουν καθοριστεί, για να μεταφέρουν τα κλειδιά διαχείρισης δεδομένων, που είναι απαραίτητα για το SRTP. Έτσι, ο συνδυασμός του SRTP και του MIKEY μπορεί να χρησιμοποιηθεί για να παρέχει end-to-end κρυπτογράφηση, ακόμη και μεταξύ διαφορετικών προτύπων σηματοδότησης πολυμέσων, όπως το H.323 και το SIP.

5.3.3. Διαχείριση κλειδιών για τα SRTP – MIKEY

Το SRTP χρησιμοποιεί ένα σύνολο ήδη διαπραγματευμένων παραμέτρων από τις οποίες προέρχονται τα session keys για την κρυπτογράφηση, την επικύρωση και την προστασία ακεραιότητας. Το MIKEY περιγράφει ένα σχέδιο διαχείρισης κλειδιών που διευθυνσιοδοτεί τα σενάρια των σε πραγματικό χρόνο πολυμέσων (π.χ. SIP κλήσεις και RTSP σύνοδοι, ροή ρεύματος, μονή εκπομπή, ομάδες, πολλαπλής διανομής) και τα τυποποιεί μέσα στην ομάδα MSEC του IETF.

Το επίκεντρο βρίσκεται στην οργάνωση μιας ένωσης ασφαλείας, για τις ασφαλείς συνόδους πολυμέσων, συμπεριλαμβανομένου της διαχείρισης κλειδιών και αναπροσαρμογής, της ασφαλούς πολιτικής δεδομένων, κ.λπ., έτσι ώστε να

ικανοποιούνται οι απαιτήσεις σε ένα ετερογενές περιβάλλον. Επίσης το MIKEY υποστηρίζει τη διαπραγμάτευση των ενιαίων και πολλαπλών κρυπτο-συνόδων. Αυτό είναι ιδιαίτερα χρήσιμο, για την περίπτωση όπου η διαχείριση κλειδιών εφαρμόζεται σε SRTP, δεδομένου ότι εδώ το RTP και το RTCP μπορούν να εξασφαλιστούν ανεξάρτητα.

Το MIKEY υποστηρίζει τη διαπραγμάτευση των κλειδιών κρυπτογράφησης και των παραμέτρων ασφαλείας για ένα ή περισσότερα πρωτόκολλα ασφαλείας. Αυτό οδηγεί στην ένωση των κρυπτο-δεσμών συνόδου, οι οποίες περιγράφουν μια συλλογή κρυπτο-συνόδων, που μπορεί να έχει ένα κοινό Traffic Encryption Key (TEK) Generation Key (TGK) και παραμέτρους ασφαλείας συνόδου που ανήκουν.

Το MIKEY έχει μερικές σημαντικές ιδιότητες:

- Το MIKEY μπορεί να εφαρμοστεί ως ανεξάρτητη βιβλιοθήκη λογισμικού, που ενσωματώνεται εύκολα σε ένα πρωτόκολλο επικοινωνίας πολυμέσων. Προσφέρει την ανεξαρτησία ενός συγκεκριμένου πρωτοκόλλου επικοινωνίας (SIP, H.323, κ.λπ....)

- Η καθιέρωση του υλικού κλειδιού μέσα σε μια διμερή χειραψία, επομένως το πιο κατάλληλο για τα σε πραγματικό χρόνο σενάρια πολυμέσων
- Υπάρχουν τέσσερις επιλογές για τη διανομή κλειδιών:
    - Το προμοιρασμένο κλειδί
    - Το δημόσιο κλειδί κρυπτογράφησης
    - Η Diffie-Hellman ανταλλαγή κλειδιών που προστατεύεται από την κρυπτογράφηση του δημοσίου κλειδιού
    - Η Diffie-Hellman ανταλλαγή κλειδιών που προστατεύεται με τα προμοιρασμένα κλειδιά και τις λειτουργίες κακών κλειδωμάτων (που χρησιμοποιούν μια επέκταση MIKEY (DHHMAC))

- Υποστήριξη Re-keying
- Multicast Υποστήριξη (ένας αποστολέας)

5.3.4 Καλύτερα σχεδιαστικά διαγράμματα

Η ενσωμάτωση του AES ή κάποιου άλλου ταχύ αλγορίθμου κρυπτογράφησης, θα μπορούσε να βοηθήσει προσωρινά στην αποσυμφόρηση, αλλά αυτό δεν είναι μια εξελικτική λύση, επειδή δεν εξετάζει την βαθιά αιτία της επιβράδυνσης. Χωρίς έναν τρόπο όπου η κρυπτο-μηχανή θα δίνει προτεραιότητα σε πακέτα, η μηχανή αυτή, θα είναι ακόμα ευάλωτη στις επιθέσεις του DoS και στην έλλειψη κυκλοφορίας δεδομένων, εμποδίζοντας τη χρονικά-επείγουσα κυκλοφορία VOIP. Μερικά μεγάλα πακέτα μπορεί να φράξουν τη σειρά αναμονής ,τόσο, ώστε τα πακέτα VOIP να καθυστερούν πάνω από 150 msec καταστρέφοντας ολοκληρωτικά την κλήση.

Η ιδανική κρυπτο-μηχανή θα εφάρμοζε το σχέδιο QoS , ώστε να ευνοηθούν τα πακέτα φωνής, αλλά αυτό δεν είναι ένα ρεαλιστικό σενάριο λόγω των περιορισμών ταχύτητας και πυκνότητας στην κρυπτο -μηχανή. Μια λύση που εφαρμόζεται στους πιο πρόσφατους δρομολογητές, είναι να σχεδιαστούν τα πακέτα με QoS, πριν από τη φάση της κρυπτογράφησης.

Αν και αυτός ο τρόπος λύνει το πρόβλημα για όλη την ισορροπία του πακέτου που εισαγάγει η κρυπτο-μηχανή σε μία δεδομένη στιγμή, δεν εξετάζει το πρόβλημα των πακέτων VOIP φτάνοντας στη σειρά αναμονής μιάς κρυπτο-μηχανής, όπου είναι ήδη φορτωμένη με τα προηγούμενα σχεδιαστικά πακέτα δεδομένων. Επίσης, η προτεραιότητα στο QoS, μπορεί να δοθεί μετά τη διαδικασία κρυπτογράφησης, παρέχοντας τη δυνατότητα στις διαδικασίες κρυπτογράφησής να συντηρούν τα κομμάτια ToS από την αρχική IP κεφαλίδα στη νέα κεφαλίδα IPsec. Αυτή η λειτουργία δεν είναι εγγυημένη και εξαρτάται από το υλικό και το λογισμικό του δικτύου, αλλά εάν εφαρμοστεί, επιτρέπει στο σχεδιασμό του QoS να αντιμετωπίσει τα κρυπτογραφημένα πακέτα, χρησιμοποιώντας τα σε κάθε άλμα.

Υπάρχουν ανησυχίες σχετικά με την ασφάλεια, όποτε δεν είναι σαφείς οι πληροφορίες για το περιεχόμενο ενός πακέτου, συμπεριλαμβανομένου αυτού του σχεδίου ToS. Ακόμα, ούτε τα σχέδια προ-κρυπτογράφησης ή μετα-κρυπτογράφησης δεν εφαρμόζουν πραγματικά το QoS ή οποιοδήποτε άλλο σχέδιο που δίνει προτεραιότητα στο να ενισχυθεί ο χρονοπρογραμματιστής FIFO της κρυπτο-μηχανής.

Οι περιορισμοί ταχύτητας και πυκνότητας σε αυτήν την συσκευή, μπορεί να μην επιτρέψουν σε τέτοιους αλγορίθμους να εφαρμοστούν για κάποιο χρονικό διάστημα.

5.3.5 Συμπίεση του Μεγέθους των Πακέτων

Προτείνεται μια νέα προσέγγιση στα ζητήματα QoS που συνδέονται με το VOIPsec. Η λύση αυτή στοχεύει στην αύξηση του μεγέθους των πακέτων που προέρχονται από τη χρήση του IPsec. Εφαρμόστηκε το cIPsec: μια έκδοση του IPsec που συμπιέζει την εσωτερική κεφαλίδα ενός πακέτου περιορίζοντάς την σε περίπου τέσσερα bits. Αυτό είναι δυνατόν, επειδή ένα μεγάλο μέρος των δεδομένων στις εσωτερικές κεφαλίδες ενός πακέτου, παρέμεινε σταθερό ή αναπαρήχθη στην εξωτερική κεφαλίδα.

Τα αρχικά αποτελέσματα της δοκιμής δείχνουν ότι η συμπίεση των κεφαλίδων IPsec, οδηγεί στο ότι η χρήση εύρους ζώνης είναι συγκρίσιμη με αυτήν της IP. Αυτό στη συνέχεια οδηγεί σε μικρότερο jitter, λανθάνουσα κατάσταση και καλύτερη απόδοση των κρυπτο-μηχανών.

Επίσης η απόδοση των κρυπτο -μηχανών βελτιώνεται. Βέβαια υπάρχει κάποιο τίμημα για αυτές τις επιταχύνσεις. Το σχέδιο συμπίεσης εστιάζει περισσότερο στις ικανότητες της CPU και της μνήμης αυτών των τερματικών, προκειμένου να επιτευχθεί η συμπίεση. Φυσικά και οι δύο άκρες μιας σύνδεσης πρέπει να χρησιμοποιήσουν τον ίδιο αλγόριθμο συμπίεσης. Παρόλα αυτά, διαπιστώθηκε ότι ο χρόνος που χάθηκε στη συμπίεση, ανακτήθηκε στη φάση της κρυπτογράφησης, δεδομένου ότι η κρυπτο-μηχανή είναι αποδοτικότερη με συμπιεσμένα πακέτα.

Ένα πράγμα που δεν εξετάστηκε είναι η τεράστια προσοχή που δίνεται στο ακραίο σημείο της CPU ,σε αντιδιαστολή με την κρυπτο-μηχανή. Το ακραίο σημείο της CPU μπορεί να είναι υπολογιστικά αργό (στην περίπτωση μία απλής τηλεφωνικής συσκευής VOIP) ή μπορεί να εκτελεί πολύ περισσότερες διαδικασίες, αντί μόνο VOIP (στην περίπτωση ενός τηλεφώνου βασισμένο σε PC). Σε κάθε περίπτωση, ο πραγματικός χρόνος που απαιτείται για να εκτελέσει τη συμπίεση μπορεί να υπερβεί το χρόνο που κερδίζεται στην κρυπτο-μηχανή.

Αξίζει να σημειωθεί ότι το σχέδιο συμπίεσης που χρησιμοποιείται σε cIPsec, συμπιέζει μόνο τις πληροφορίες κεφαλίδας των πακέτων. Τα ζητήματα συμπίεσης QoS που συνδέονται με τους ακουστικούς κωδικοποιητές/αποκωδικοποιητές, δεν ισχύουν σε αυτό το σενάριο, επειδή κανένα πραγματικό μέσο δεν συμπυκνώνεται, παρά μόνο οι IP κεφαλίδες. Εντούτοις, η απώλεια πακέτων έχει μια επιδεινωμένη επίδραση στα πακέτα που συμπιέζονται με βάση το σχέδιο cIPsec. Το σχέδιο, πρέπει να διατηρήσει τις πληροφορίες στα ακραία σημεία του συστήματος, σχετικά με την τρέχουσα σύνοδο. Όταν τα πακέτα χάνονται, δεν μπορούν να σταλούν ξανά και τα ακραία σημεία χρειάζονται επανασυγχρονισμό. Βέβαια, ο χρόνος που κερδίζεται στην κρυπτο-μηχανή και η ασφάλεια που παρέχεται, μπορεί να αξίζουν το τίμημα αυτής της προσέγγισης.

5.3.6 Επίλυση του NAT/IPsec Ασυμβίβαστου

Το RSIP σχεδιάζεται ως αντικατάσταση του NAT και παρέχει ένα σαφές tunnel μεταξύ των υπολογιστών υπηρεσίας και του RSIP Gateway. Το RSIP υποστηρίζει και το AH και το ESP, αλλά η εφαρμογή RSIP θα απαιτούσε μια σημαντική εξέταση της τρέχουσας LAN αρχιτεκτονικής. Έτσι, ενώ είναι μια αρκετά κομψή λύση, αυτήν την περίοδο είναι μη πραγματοποιήσιμη. Ίσως το RSIP, δεν χρησιμοποιείται ευρέως ως αποτέλεσμα αυτών των προβλημάτων. Η μέθοδος του IPv6 της tunnel μεσολάβησης, χρησιμοποιεί ένα tunnel IPv6 ως ένα tunnel Ipsec και ενθυλακώνει ένα IPv6πακέτο, σε ένα πακέτο IPv4. Όμως και αυτή η λύση απαιτεί βελτιώσεις στο LAN και δεν λειτουργεί σε καταστάσεις όπου χρησιμοποιούνται πολλά NATs.

Το IPNL εισάγει ένα νέο επίπεδο στα πρωτόκολλα δικτύων μεταξύ του IP και του TCP/UDP,για να λύσει το πρόβλημα, αλλά το IPNL είναι ανταγωνιστικό με το IPv6, όμως το IPv6 είναι ένα πρότυπο που χρησιμοποιείται πιο πολύ. Η πιο διαδεδομένη λύση στο πρόβλημα της μετάβασης στο NAT, είναι η ενθυλάκωση UDP του IPsec. Αυτή η εφαρμογή υποστηρίζεται από το IETF και επιτρέπει αποτελεσματικά σε όλη την ESP κυκλοφορία, να διαπεράσει το NAT. Στο tunnel mode, αυτό το πρότυπο περιλαμβάνει το κρυπτογραφημένο Ipsec πακέτο, σε ένα UDP πακέτο με μια νέα IP

κεφαλίδα και μια νέα UDP κεφαλίδα, χρησιμοποιώντας συνήθως τη θύρα 500. Το πεδίο SPI μέσα στο ενθυλακωμένο UDP πακέτο είναι όλο μηδενικά, για να το διαφοροποιήσει από μια πραγματική επικοινωνία IKE.

Αυτή η λύση, επιτρέπει στα IPsec πακέτα να διαπεράσουν τα πρότυπα NATs και από τις δύο κατευθύνσεις. Η υιοθέτηση αυτής της πρότυπης τυποποιημένης μεθόδου, πρέπει να επιτρέψει στην VOIPsec κυκλοφορία να διαπεράσει τα NATs, αν και προστίθενται κάποια επιπλέον overhead στη διαδικασία ενθυλάκωσης / αποθυλάκωσης. Η διαπραγμάτευση IKE θα απαιτηθεί επίσης, για να επιτραπεί η διαμεσολάβηση του NAT. Το πρόβλημα που παραμένει είναι, ότι η βασισμένη σε IP επικύρωση πακέτων δεν μπορεί να βεβαιωθεί μέσω του NAT, (αν και θα μπορούσαν να χρησιμοποιηθούν πλήρως κατάλληλα ονόματα περιοχών domain names) όμως η χρήση ενός κοινού μυστικού (συμμετρικό κλειδί) που συζητήθηκε μέσω του IKE, θα μπορούσε να παρέχει την επικύρωση. Είναι σημαντικό να σημειωθεί ότι η βασισμένη σε IP επικύρωση είναι αδύνατη έναντι των μεθόδων που χρησιμοποιούν τα πρωτόκολλα κρυπτογράφησης.

Κεφάλαιο 6ο

Συμπεράσματα

Όταν στο δίκτυο της επιχείρησης ενσωματώνεται ο εξοπλισμός της IP Τηλεφωνίας , υπάρχουν ορισμένες πρακτικές και μέθοδοι που πρέπει να εφαρμοστούν ώστε να εξασφαλιστεί η προστασία του εξοπλισμού και ολόκληρου του δικτύου από ανεπιθύμητες επιθέσεις.

- ✓ Η παροχή ασφάλειας στην IP τηλεφωνία εξαρτάται κυρίως από την δομή και ανάπτυξη του δικτύου, την χρήση των κατάλληλων Πρωτοκόλλων Ασφαλείας, των δυναμικών και ισχυρών Μηχανισμών Ασφαλείας, την χρήση Firewalls, Session Borders Controllers και των Intrusion Detection συστημάτων ασφαλείας . Με αυτές τις μεθόδους ίσως καταφέρουμε να λέμε

ότι η ασφάλεια στην IP τηλεφωνία μπορεί να φτάσει τα επίπεδα ασφάλειας της ψηφιακής τηλεφωνίας.

- ✓ Σε αντίθεση με κάποιο συνηθισμένο PC , ο server που υποστηρίζει τον εξοπλισμό της IP τηλεφωνίας θα πρέπει να εγκαθίσταται σε ένα απομονωμένο περιβάλλον ώστε να έχουν πρόσβαση σε αυτό όσο τον δυνατόν λιγότεροι χρήστες . Με αυτό τον τρόπο μειώνονται οι ευκαιρίες πρόσβασης σε ανεπιθύμητους επισκέπτες , αυξάνοντας έτσι το ποσοστό ασφαλείας του server καθώς αι την ομαλή παροχή υπηρεσιών του.

- ✓ Για την ομαλότερη και ασφαλέστερη λειτουργία του εξοπλισμού, είναι απαραίτητη η δημιουργία Vlans . Με αυτό τον τρόπο θα διαχωρίζεται η μετάδοση της φωνής από την μεταφορά των data δημιουργώντας ένα επιπλέον πέπλο προστασίας.

- ✓ Η χρήση των Firewalls, routers και switches αυξάνει το επίπεδο ασφαλείας στην IP τηλεφωνία. Αυτό συμβαίνει καθώς μειώνεται ο αριθμός των μη εξουσιοδοτημένων για πρόσβαση στον εξοπλισμό της IP Τηλεφωνίας, με αποτέλεσμα να υπάρχουν λιγότερες ανεπιθύμητες προσβάσεις στα πρωτόκολλα και στις υπηρεσίες που υποστηρίζει και παρέχει η IP τηλεφωνία.

- ✓ Ο server που υποστηρίζει τον εξοπλισμό της IP τηλεφωνίας παρέχει συγκεκριμένες υπηρεσίες στους χρήστες του τηλεπικοινωνιακού εξοπλισμού. Η καλύτερη πολιτική ασφαλείας είναι η μη εγκατάσταση επιπλέον software για την παροχή μεγαλύτερης ασφάλειας στο δίκτυο στον συγκεκριμένο server, καθώς θα επηρεάσει την ομαλή λειτουργία του.

- ✓ Η διαχείριση και υποστήριξη του τηλεπικοινωνιακού εξοπλισμού πρέπει να γίνεται από εξουσιοδοτημένα άτομα με συγκεκριμένους κωδικούς. Η οποιαδήποτε ενέργεια κατά της διάρκεια της υποστήριξης και επιλύσεων βλαβών πρέπει να καταγράφεται σε ένα συγκεκριμένο αρχείο. Επιπλέον οι κωδικοί που χρησιμοποιούν οι εξουσιοδοτημένοι χρήστες θα πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα.

Η υιοθέτηση και η εφαρμογή των παραπάνω συστάσεων αποτελεί μια καλή πρακτική για την παροχή καλύτερης ασφάλειας στην IP τηλεφωνία. Παρόλα αυτά, δεν είναι οι μοναδικές πρακτικές που πρέπει να εφαρμοστούν καθώς κάθε εταιρεία παραπέμπει σε διαφορετικές προκλήσεις και απαιτήσεις για το δίκτυό της. Η συνεχής ενημέρωση με τις τρέχουσες πρακτικές για παροχή ασφαλείας στην βιομηχανία της τηλεφωνίας και της Τεχνολογίας γενικότερα, αποτελεί μια πολύ καλή ενέργεια για την διατήρηση ή και την βελτίωση της ασφάλειας.

ΠΑΡΑΡΤΗΜΑ

A

ACK
Acknowledgement

AH
Authentication Header

ARP
Address Resolution Protocol

D

DHCP
Dynamic Host Configuration Protocol

DoS
Denial of Service

DNS
Domain Name System

H

HMAC
Hash Message Authentication Code

HMAC MD5
Hash Message Authentication Code - Message-Digest Algorithm 5

HMAC SHA
Hash Message Authentication Code - Secure Hash Algorithm

I

IKE
Internet Key Exchange

ISP
Internet Service Provider

L

LAN
Local Area Network

M

MGCP
Media Gateway Control Protocol

MIKEY
Multimedia Internet KEYing

MIME
Multipurpose Internet Mail Extensions

P

PCM
Pulse-code Modulation

PSTN
Public Switched Telephone Network

Q

QoS
Quality of Service

R

RAS
Registration Admission Status

RTP
Real-time Transport Protocol

S

SGSP
Simple Gateway Control Protocol

SIP
Session Internet Protocol

SMTP
Simple Mail Transfer Protocol

SSH
Secure Shell

T

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

U

UDP
User Datagram Protocol

URI

Uniform Resource Identifier

V

VAD
Voice Activity Detection

VLAN
Virtual LAN

VoIP
Voice over Internet Protocol

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Security Handbook, 2002

[2] The State of IP Telephony, 2002

[3] IP Telephony Security, 2003

[4] IP Telephony Security in Depth, 2003

[5] Security in Telecommunications and Information Technology, 2003

[6] Securing Your Network for IP Telephony , 2004

[7] Cisco IP Communications Security, 2004

[8] Security of Cisco CallManagerbased IP Telephony against malicious hacker attacks, 2004

[9] Breaking throughVoIP security, 2004

[10] Security Considerations for Voice Over IP Systems, 2005

[11] Voice Security Primer: Protecting the Voice Infrastructure, Call-Management System, Applications, and Endpoints, 2005

[12] Moving from concepts to real solutions: Vulnerability Analysis and Best Practices For Adopting IP Communications, 2006

[13] Voice Security, 2007

[14] Securing the Unified Communications–Enabled Enterprise, 2007

[15] RFC 3261 - SIP: Session Initiation Protocol
http://www.faqs.org/rfcs/rfc3261.html

[16] SIP: Papers
http://www.cs.columbia.edu/sip/papers.html

[17] Purpose of SIP | iptel.org-Internet Telephony
http://www.iptel.org/sip/intro/purpose

[18] Portal for contributing to the promotion and knowledge of SIP and associated technologies, by posting and maintaining white papers
http://www.tech-invite.com/

[19] Session Initiation Protocol - Wikipedia, the free encyclopedia- http://en.wikipedia.org/wiki/Session_Initiation_Protocol

[20] SIP, Session Initiation Protocol http://www.networksorcery.com/enp/protocol/sip.htm

[21] http://www.answeringphoneservices.com

[22] www.avaya.com