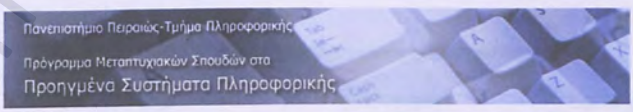
Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ασφάλεια σε VoIP συστήματα**
Ονοματεπώνυμο Φοιτητή	**Καμπύλη Ελευθερία του Ιωάννου**
Αριθμός Μητρώου	**ΠΣΠ 060-65**
Κατεύθυνση	**Δικτυοκεντρικά Πληροφοριακά Συστήματα**
Επιβλέπων	**Φούντας Ευάγγελος, Καθηγητής**



Ημερομηνία Παράδοσης **Ιούνιος 2010**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Φούντας Ευάγγελος Καθηγητής	Τσικούρας Παναγιώτη-Γεώργιος Αναπληρωτής Καθηγητής	Αποστόλου Δημήτριος Λέκτορας

ΠΕΡΙΛΗΨΗ

Αυτή η πτυχιακή εργασία παρουσιάζει και μελετά τα συστήματα VoIP και τη σχέση τους με την ασφάλεια. Πιο συγκεκριμένα, στα δύο πρώτα κεφάλαια παρουσιάζονται γενικότερα τα VoIP συστήματα, οι εφαρμογές που έχουν καθώς επίσης και οι αρχιτεκτονικές στις οποίες στηρίζονται. Στα επόμενα κεφάλαια αναλύονται τα κυριότερα πρωτόκολλα που χρησιμοποιούντα σ΄ αυτά τα συστήματα, οι κυριότερες επιθέσεις που μπορούν να δεχτούν και οι μηχανισμοί ασφαλείας που διαθέτουν. Γίνεται επίσης εκτενέστερη αναφορά στην ασφάλεια που προσφέρει το SIP πρωτόκολλο, καθώς είναι το κυριότερο που χρησιμοποιείται στα VoIP συστήματα.

Τέλος, αναλύονται τα προβλήματα που παρουσιάζονται στις VoIP τεχνολογίες και προτείνεται ένας μηχανισμός ασφάλειας και η αρχιτεκτονική του λύση.

In this thesis, VoIP systems are presented and their relation to security is examined. More specifically, in the first chapters of the thesis we analyze VoIP technologies more generally, the way they are applied in systems and furthermore, the architectures that they depend on. In the next chapters, protocols that apply on VoIP systems are analyzed in detail. Moreover, the most dangerous VoIP attacks and the security mechanisms are presented. Because of the importance of SIP protocol in VoIP systems, the security that offers is described in a more extended way.

Finally, in the last chapter of the thesis, problems that rise in VoIP systems are analyzed and a secure solution is suggested along with the solution's architecture.

ΕΙΣΑΓΩΓΗ

Με την πάροδο των χρόνων τα δίκτυα τηλεφωνίας έχουν εισάγει πολλές καινούριες υπηρεσίες που όχι μόνο μεταφέρουν το ακουστικό σήμα αλλά είναι πλέον κατάλληλα για την ανταλλαγή πληροφοριών, τη διακίνηση δεδομένων και εικόνων. Σ' αυτό έχουν βοηθήσει πολύ οι αλλαγές της δομής των δικτύων τηλεπικοινωνίας καθώς επίσης και οι εξελίξεις που διαδραματίζονται στο χώρο του internet, βασισμένες στο Internet Protocol (IP), και τέλος η ελάττωση του κόστους επικοινωνίας.

Τα παραπάνω επιτεύχθηκαν με την ολοκλήρωση των υπηρεσιών δεδομένων και φωνής, βάση της ανάγκης για χαμηλότερο κόστος των δικτύων πακέτων μεταγωγής καθώς και για βελτίωση ποιότητας και αξιοπιστίας της φωνής. Ένα από τα βασικά κίνητρα χρήσης της τηλεφωνίας μέσω Internet (Internet Telephony) είναι το πολύ χαμηλό κόστος που συνεπάγεται.

Στις μέρες μας, η τεχνολογία του VoIP (Voice over Internet Protocol) παρουσιάζει ταχύτατη ανάπτυξη και αρχίζει να χρησιμοποιείται ολοένα και περισσότερο, τόσο από μεγάλες επιχειρήσεις, όσο και από το ευρύ κοινό. Η τεχνολογία αυτή προσφέρει εξαιρετικά φθηνές τηλεφωνικές υπηρεσίες, με ποιότητα που βελτιώνεται μέρα με τη μέρα, και έτσι τείνει να αντικαταστήσει την παραδοσιακή τηλεφωνία που όλοι γνωρίζουμε.

Στο σημείο αυτό, θα ήθελα να δώσω ιδιαίτερες ευχαριστίες στον κ. Κωνσταντίνο Πατσάκη για την υποστήριξη και τη συνεργασία για τη συμβολή του στην ολοκλήρωση αυτής της διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ στη VoIP τεχνολογία

1.1 Voice Over IP (VoIP)

Το VoIP ουσιαστικά μεταδίδει τη φωνή σε μορφή πακέτου πάνω από το IP δίκτυο, με τη βοήθεια του Internet Protocol (IP). Αυτό το κάνει ευέλικτο και έχει εφαρμογή σε οποιοδήποτε δίκτυο δεδομένων που χρησιμοποιεί IP (όπως για παράδειγμα τα τοπικά δίκτυα LAN, τα Intranets και φυσικά το Internet).

Ο τρόπος που λειτουργεί το VoIP είναι αρχικά η ψηφιοποίηση του σήματος της φωνής, η συμπίεση και η μετατροπή του σε IP πακέτα και τέλος η διαβίβαση του μέσω του IP δικτύου. Σημαντικό ρόλο παίζουν επίσης τα πρωτόκολλα σηματοδοσίας έτσι ώστε να να ξεκινήσουν ή να τελειώσουν κλήσεις, να μεταφέρουν πληροφορίες, να διαχειριστούν τα χαρακτηριστικά μιας κλήσεις ή και να εντοπίσουν τους χρήστες.

Υπάρχουν τέσσερις τρόποι για να πραγματοποιηθεί μία κλήση μέσω VoIP: από **PC σε PC**, από **τηλέφωνο σε τηλέφωνο**, από **PC σε τηλέφωνο** και από **τηλέφωνο σε PC**. Στη δεύτερη περίπτωση, είτε το τηλέφωνο μπορεί να είναι κανονικά συνδεδεμένο στο τηλεφωνικό δίκτυο, είτε μπορεί να είναι IP-τηλέφωνο συνδεδεμένο πάνω σε δίκτυο δεδομένων.

Σε όλες τις παραπάνω περιπτώσεις χρησιμοποιείται το Internet Protocol με αποτέλεσμα να επιτυγχάνεται η καλύτερη δυνατή ποιότητα υπηρεσίας. Οι δύο βασικές εφαρμογές του VoIP είναι σε δίκτυα ιδιωτικών εταιρειών και σε δημόσια δίκτυα.

Οι ιδιωτικές εταιρείες με απομακρυσμένα γραφεία που συνδέονται μεταξύ τους μέσω intranet, για τις υπηρεσίες δεδομένων, μπορούν να εκμεταλλευθούν το τοπικό αυτό δίκτυο με την προσθήκη υπηρεσιών φωνής και fax χρησιμοποιώντας τις τεχνολογίες VoIP. Η χρησιμοποίηση ενός μόνο δικτύου και για φωνή και για δεδομένα έχουν σαν αποτέλεσμα τη μείωση του κόστους και την αποφυγή των δαπανών πρόσβασης στο τηλεφωνικό δίκτυο που είναι ιδιαίτερα ακριβή για τις πολυεθνικές εταιρίες. Παράλληλα επιτυγχάνεται και η ποιότητα εξυπηρέτησης (Quality of service, QoS) χρησιμοποιώντας η κάθε εταιρεία το ιδιωτικό της intranet, και η ποιότητα φωνής παραμένει σε υψηλά επίπεδα.

Όσον αφορά την εφαρμογή του VoIP σε δημόσια δίκτυα, τα πράγματα είναι λίγο πιο πολύπλοκα γιατί είναι απαραίτητη η χρήση των gateways, ώστε να μεταφέρουν τη φωνή στους παροχείς υπηρεσιών (Internet Providers ή Internet Telephony Service Providers) οι οποίοι αναπτύσσουν ειδικά δίκτυα για να μεταφέρουν τη ροή πολυμέσων όπως είναι το VoIP. Οι Internet Providers με σκοπό να αυξήσουν τα έσοδα τους και να αποφύγουν τη μηνιαία αμοιβή που καταβάλουν σε επίκαιρους παρόχους, ενδιαφέρονται για το VoIP, που μοιάζει σαν ένας νέος τρόπος ώστε να προσφέρουν καινούριες υπηρεσίες με μεγαλύτερη αξία και να βελτιώσουν το ίδιο το δίκτυό τους. Μακροπρόθεσμα δε, η χρήση των IP δικτύων θα οδηγήσει σε νέες εφαρμογές, κυρίως σε εφαρμογές πολυμέσων που απαιτούν τη σύγκλιση φωνής, βίντεο, δεδομένων και fax και επιπλέον θα κάνει τους παρόχους (carriers) ιδιαίτερα ανταγωνιστικούς στην αγορά.

Όλα τα παραπάνω όμως έχουν αρκετά πλεονεκτήματα αλλά και μειονεκτήματα τα οποία θα αναφερθούν στη συνέχεια.

1.1.1 Πλεονεκτήματα και μειονεκτήματα

Θέλοντας να συνοψίσουμε τα βασικά πλεονεκτήματα της τεχνολογίας VoIP, έχουμε τα ακόλουθα:

- **Χαμηλότερες δαπάνες μεταφοράς** :

Οι εταιρίες μπορούν σημαντικά να ελαττώσουν τους μηνιαίους λογαριασμούς τηλεφώνου, κατευθύνοντας τις κλήσεις φωνής πάνω από τα εταιρικά δίκτυα δεδομένων, πάρα από έναν μεταφορέα. Η εξοικονόμηση αυτή εξαρτάται από πολλούς παράγοντες. Δύο από αυτούς είναι ο όγκος των κλήσεων εντός της εταιρίας και η μεγάλη γεωγραφική έκταση όπου είναι διασπαρμένες οι πληροφορίες προς επεξεργασία. Οι εταιρίες με γραφεία σε εκτεταμένες περιοχές, μπορούν να έχουν το μεγαλύτερο κέρδος καθώς μπορούν να ελαττώσουν κατά πολύ τις διεθνείς δαπάνες κλήσεως σε μεγάλες αποστάσεις. Οι δαπάνες αυτές είναι

συνήθως ιδιαίτερα υψηλές όταν η κλήση δημιουργείται σε μια ξένη χώρα στην οποία υπάρχει ακόμα μονοπώλιο στην αγορά τηλεπικοινωνιών. Σε μερικές περιπτώσεις το κέρδος αυτό μπορεί να επεκταθεί στις κλήσεις εκτός της εταιρίας με τη χρήση PSTN πυλών.

- **Οικονομικοί παράγοντες** :

Το οικονομικό όφελος της μετάδοσης κλήσεων φωνής πάνω από δίκτυα δεδομένων οφείλεται σε δύο τεχνικούς παράγοντες. Πρώτον, τα δίκτυα δεδομένων έχουν σχεδόν πάντα διαθέσιμη χωρητικότητα. Οι διαχειριστές δικτύων παρέχουν μεγάλες χωρητικότητες για να αποφύγουν τη συμφόρηση κατά τις ώρες αιχμής. Ταυτόχρονα, οι κλήσεις φωνής χρησιμοποιούν σχετικά λίγο εύρος ζώνης. Τα χαρακτηριστικά της ανθρώπινης φωνής, ιδιαίτερα τα μεγάλα διαστήματα παύσης που δημιουργούνται κατά τη διάρκεια της συνομιλίας, επιτρέπουν μεγάλη συμπίεση στην ψηφιακή μεταφορά της κλήσης. Με αυτόν τον τρόπο είναι δυνατόν να προστεθούν στο τέλος κάθε πακέτου επιπλέον πληροφορίες στις υπάρχουσες συνδέσεις δικτύων δεδομένων χωρίς να απαιτείται επιπλέον χωρητικότητα σε αυτές τις συνδέσεις. Ακόμα και όταν τέτοιες αυξήσεις πρέπει να γίνουν στο υπάρχον δίκτυο λόγω του μεγάλου όγκου κλήσεων το κόστος παραμένει χαμηλό συγκρινόμενο με αυτό των μεταφορέων για τη μεταφορά του ίδιου αριθμού κλήσεων.

- **Μειωμένο μακροπρόθεσμο κόστος κατοχής δικτύου** :

Εκτός από τη μείωση των μηνιαίων λογαριασμών τηλεφώνου μιας εταιρίας, η συγκλίνουσα αρχιτεκτονική δικτύων επίσης, μειώνει το τρέχον κόστος αναγνώρισης δύο ξεχωριστών δικτύων, ένα για τη φωνή και ένα για τα δεδομένα. Το κόστος αυτό περιλαμβάνει : την ανάγκη αγοράς δύο ξεχωριστών συνόλων εξοπλισμού, το χρόνο που απαιτείται από το προσωπικό σε αυτή την εργασία και στη συντήρηση του εξοπλισμού, τη χορήγηση αδειών οποιουδήποτε λογισμικού σχετικά με τη διαχείριση του εξοπλισμού, και τον έλεγχο κίνησης στα δύο δίκτυα. Με την επανάσταση του Internet, η ζήτηση για ειδικευμένους, έμπειρους τεχνικούς είναι πολύ μεγάλη. Αυτό έχει σαν αποτέλεσμα οι μισθοί των εργαζομένων στα δίκτυα φωνής και δεδομένων να είναι υψηλοί. Οι εταιρίες είναι σε θέση να ελαττώσουν τις ανάγκες τους σε τεχνικό προσωπικό οργανώνοντας πιο αποδοτικά τις εργασίες δικτύου. Με αυτό τον τρόπο μειώνουν κατά πολύ το ανθρώπινο δυναμικό.

- **Προηγμένες εφαρμογές** :

Το μεγαλύτερο κέρδος από τη συγκλινόμενη δικτύωση φωνής/ δεδομένων μπορεί να είναι η καινούρια γενιά εφαρμογών της. Για παράδειγμα τα πραγματικού χρόνου πολυμέσα βίντεο/ ήχο, συνδιάσκεψη, εκπαίδευση εξ αποστάσεως, και την ενσωμάτωση συνδέσεων φωνής (links) σε ηλεκτρονικά έγγραφα. Πριν από λίγα χρόνια, το Internet δεν ήταν έτοιμο να παίξει πρωταγωνιστικό ρόλο. Τώρα όμως είναι. Το VoIP είναι μια πολύτιμη υπηρεσία. Χρειάζεται λοιπόν, να ενσωματωθούν οι ISPs με την IP τηλεφωνία. Ο μεγάλος ανταγωνισμός στις τηλεπικοινωνίες περιόρισε τα έσοδα στις βασικές υπηρεσίες φωνής και δεδομένων. Για να παραμείνουν επωφελημένοι οι προμηθευτές υπηρεσιών πρέπει να παρέχουν νέες υπηρεσίες ώστε να κρατήσουν τους πελάτες τους και ταυτόχρονα να περιορίσουν τα έξοδά τους. Μόνο μέσω της ενσωμάτωσης των δικτύων κυκλωμάτων και πακέτων μπορούν οι προμηθευτές υπηρεσιών να επωφεληθούν από την παγκοσμιοποίηση του τηλεφωνικού δικτύου μεταγωγής κυκλώματος (σημερινό PSTN), από τη δύναμη της εσωτερικής ευελιξίας στο βασικό λογισμικό και την ανοικτή αρχιτεκτονική των δικτύων πακέτων. Ο εξοπλισμός των δικτύων βασισμένα σε πακέτα (packet-based) είναι ευκολότερο να αναβαθμιστεί και να διαμορφωθεί, δίνοντας τη δυνατότητα γρήγορης εξέλιξης στην αγορά. Η βασισμένη στο λογισμικό αρχιτεκτονική των μηχανημάτων μπορεί να συμβάλλει στη γρήγορη ανάπτυξη των νέων υπηρεσιών.

Στον αντίποδα, τα μειονεκτήματα της τεχνολογίας VoIP συνοψίζονται στα ακόλουθα:

- **Απώλεια ποιότητας φωνής :**

Οι τεχνικοί γνωρίζουν πως τα δίκτυα δεδομένων είναι πολύ διαφορετικά από τα δίκτυα φωνής. Στα δίκτυα δεδομένων, κυρίως Ethernet που κυριαρχούν στα εταιρικά υπολογιστικά περιβάλλοντα, πακέτα αναπηδούν αόριστα, ακαθόριστα. Μπορεί να συγκρουσθούν και να καταστραφούν ακόμα και να χαθούν. Τόσο οι μηχανισμοί διόρθωσης σφάλματος σε Ethernet εξοπλισμό όσο και το ίδιο το IP πρωτόκολλο μπορούν εύκολα να αντισταθμίσουν την απώλεια των δεδομένων. Όμως η απώλεια πακέτων μπορεί να έχει σημαντικές επιπτώσεις στις κλήσεις φωνής, που απαιτούν μια καλή ποιότητα, πραγματικού χρόνου ροή πακέτων

από τη μία άκρη του δικτύου στην άλλη. Και ενώ ο ανθρώπινος νους μπορεί να κατανοήσει την ανθρώπινη ομιλία ακόμα και όταν υπάρχει μεγάλη παραμόρφωση, οι χρήστες έχουν εξοικειωθεί σε ένα συγκεκριμένο επίπεδο ποιότητας κλήσεως.

- **Απώλεια αξιοπιστίας :**

Τα δίκτυα δεδομένων δεν είναι ακόμα τόσο αξιόπιστα όσο τα δίκτυα φωνής. Όλοι έχουμε ακούσει τις φράσεις : «πάγωσε ο υπολογιστής ή το δίκτυο είναι κάτω». Αυτό όμως σπάνια συμβαίνει με τα τηλέφωνα ή με τους τηλεφωνικούς μεταφορείς . Η άμεση και συνεχής πρόσβαση στους άλλους χρήστες με τη χρήση τηλεφώνου είναι ο βασικότερος λόγος που λίγοι θέλουν να αντικαταστήσουν το τηλέφωνο με τη φωνητική επικοινωνία παρά τα μεγάλα οικονομικά οφέλη που παρέχει.

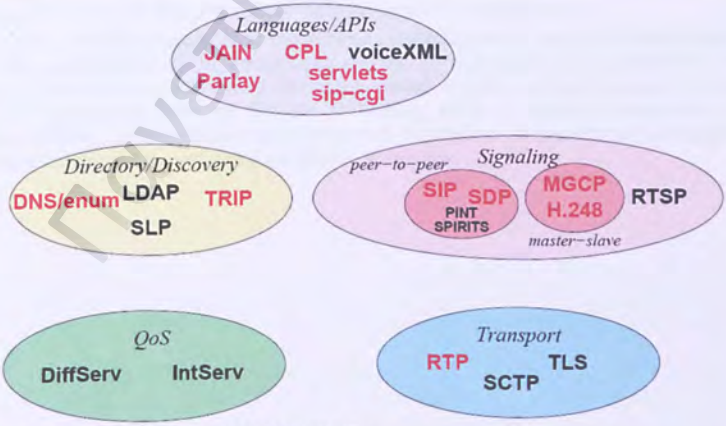
- **Ταχεία εξέλιξη της τεχνολογίας :**

Ο αλματώδης ρυθμός ανάπτυξης στην τεχνολογία των υπολογιστών, και των επικοινωνιών γενικότερα, κάνει σήμερα τους επιχειρηματίες να είναι διστακτικοί όσον αφορά την οποιαδήποτε αγορά νέου εξοπλισμού. Δύο είναι οι κύριοι λόγοι που συμβάλλουν στην αναποφασιστικότητα των επιχειρηματιών για την επένδυση σε μια νέα υπηρεσία. Ένας, είναι η μεγάλη πιθανότητα ότι μια άλλη καλύτερη λύση για το VoIP θα έρθει σύντομα μετά από τη δέσμευση ενός προϊόντος σε έναν προμηθευτή. Εάν η επένδυση σε αυτό το προϊόν είναι σημαντική, είναι σχεδόν άσκοπο να το αχρηστεύσουν και να διαλέξουν την καινούρια καλύτερη λύση. Μια άλλη σημαντικότερη ανησυχία για τους υπεύθυνους, αποτελεί το γεγονός ότι η επιλογή ενός προϊόντος που οδηγεί στη σύγκλιση φωνής- δεδομένων μπορεί να οδηγήσει σε μια συμφωνία πέρα από την ίδια τη VoIP λύση, που αναγκάζει μια μακροπρόθεσμη υπόσχεση για τη δικτύωση της εταιρίας με αυτή την αρχιτεκτονική. Αυτή η ανησυχία επιδεινώνεται από την έλλειψη καθαρών προτύπων στην αγορά του VoIP. Στην απουσία τέτοιων προτύπων οι αρμόδιοι για τον εξοπλισμό της εταιρίας με τη σύγχρονη τεχνολογία στηρίζουν την ανησυχία τους που αφορά τη δέσμευση των εταιριών σε οποιαδήποτε ιδιόκτητη αρχιτεκτονική δομή.

- **Έλλειψη εμπειρίας και πείρας :**

Η VoIP τεχνολογία είναι καινούρια. Κάθε νέα υπηρεσία πρέπει να ελέγχεται και έπειτα να κυριαρχεί στην αγορά. Αυτό όμως παίρνει χρόνο. Χωρίς την κατάλληλη πείρα και το προσεκτικό σχεδιασμό η τεχνολογία μπορεί να είναι ενάντια στην εξέλιξη.

VoIP protocol architecture



Εικόνα 1: Αρχιτεκτονική του πρωτοκόλλου VoIP

1.2 ΕΦΑΡΜΟΓΕΣ

Σχεδόν όλες οι απαιτήσεις της φωνητικής επικοινωνίας, που μπορεί να εκτείνονται από ένα απλό σύστημα εσωτερικής ενδοεπικοινωνίας μέχρι ένα σύνθετο πολλαπλών σημείων (multi-point) σύστημα τηλεσυνεδριάσεων, μπορούν να εκπληρωθούν από συστήματα VoIP. Με τη χρήση τους πραγματοποιούνται τηλεφωνικές κλήσεις και στέλνονται μηνύματα τηλεομοιοτυπίας (facsimiles) μέσω δικτύων δεδομένων που βασίζονται στο IP, με την κατάλληλη ποιότητα φωνής και ταυτόχρονα με το μεγαλύτερο δυνατό όφελος. Για παράδειγμα, ανάλογα με την ποιότητα που θέλουμε να πετύχουμε (πχ. μπορεί ο χρήστης να θέλει υψηλότερη ποιότητα στις εξωτερικές κλήσεις απ'ότι στις εσωτερικές εταιρικές κλήσεις), ο VoIP εξοπλισμός μπορεί να προσαρμοστεί και να διαμορφώσει διαφορετικά περιβάλλοντα, ακόμα και να συνδυαστεί με την παραδοσιακή τηλεφωνία.

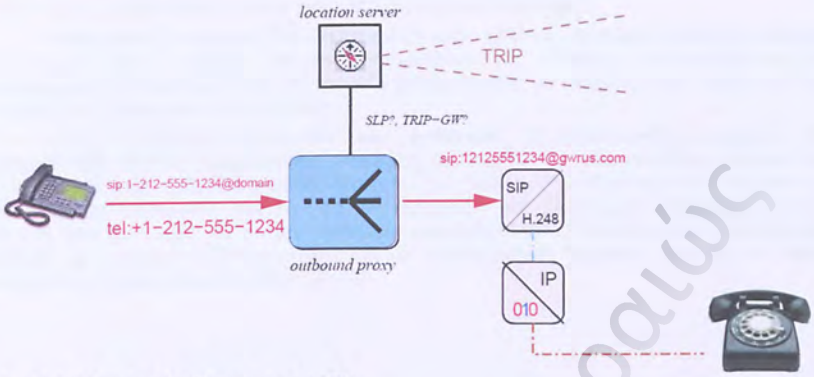
Για τους παραπάνω λόγους τα συστήματα αυτά έχουν πολλές εφαρμογές στην καθημερινή ζωή. Για παράδειγμα, τα συνηθισμένα τηλέφωνα μπορούν να εξοπλιστούν κατάλληλα ώστε να λειτουργούν σαν μια Internet συσκευή πρόσβασης και ταυτόχρονα να παρέχουν τις υπηρεσίες ενός κανονικού τηλεφώνου (internet –aware telephones). Η σύνδεση ανάμεσα στην εταιρεία και στο κύριο PBX μπορεί να αντικατασταθεί με δικτυακή σύνδεση και να παρέχει μεγαλύτερη οικονομία και δυνατότητες στο σύστημα (Εσωτερική ζεύξη πάνω από εταιρικά δίκτυα). Επιπλέον, κάποιο περιφερειακό γραφείο μπορεί να αποκτήσει πρόσβαση σε εταιρικό δίκτυο και κατ' επέκταση σε φωνή, δεδομένα και άλλες υπηρεσίες (πχ. τηλεφωνικό κέντρο).

Η τελευταία εφαρμογή θα μπορούσε να επεκταθεί ώστε οι κλήσεις σε κάποιο γραφείο να γίνονται μέσω ενός κεντρικού υπολογιστή που συνδέεται στο internet ή και ακόμα και η κύρια πρόσβαση στο internet δίνει τη δυνατότητα σε έναν πελάτη να έχει πρόσβαση στις υπηρεσίες πελατών online πέραν από τα ζητήματα που αφορούν την απλή πλοήγηση. Έτσι οι εφαρμογές του ηλεκτρονικού εμπορίου αναπτύσσονται και ανοίγονται καινούριες προοπτικές στους χρήστες. Για παράδειγμα, χρησιμοποιώντας το VoIP, οι επισκέπτες μιας ιστοσελίδας θα μπορούσαν πατώντας ένα κουμπί να ανοίξουν μια φωνητική συνομιλία με ένα κέντρο που μπορεί να απαντηθεί οποιαδήποτε ερώτησή τους ή να εξεταστεί κάποιο πρόβλημα που έχουν. Με τον τρόπο αυτό αυτόματα οι επισκέπτες των αντίστοιχων ιστοσελίδων μετατρέπονται σε αγοραστές και η επικοινωνία παύει να είναι τόσο προβληματική όσο παλιότερα.

Ακόμα μια από τις εφαρμογές για την IP τηλεφωνία είναι η πραγματικού χρόνου μετάδοση μηνυμάτων fax, που ονομάζεται επίσης Fax over IP (FoIP). Για να λειτουργήσει μια τέτοια διάταξη πρέπει τα δεδομένα να μετατραπούν σε μορφή πακέτου, να χειριστεί η μετατροπή από αναλογικό σε ψηφιακό, να ελεγχθούν πρωτόκολλα και να επιβεβαιωθεί η ολοκληρωμένη διανομή των ανιχνευτών δεδομένων με τη σωστή σειρά.

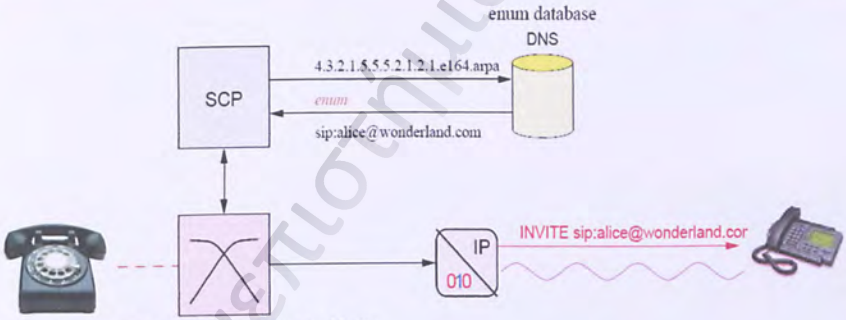
Εκτός από τις εταιρείες που σχετίζονται εξολοκλήρου με internet, πολλές είναι αυτές που επίσης χρησιμοποιούν τις εφαρμογές και την IP τεχνολογία της τηλεφωνίας. Τέτοιες εταιρείες, εκτός απ΄αυτές που έχουν ιδιωτικά ή τοπικά δίκτυα, είναι και οι εταιρείες παροχής internet ή τηλεφωνίας (Internet Service Providers, ISPs ή Internet Telephony Service Providers, ITSPs), οι μεταφορείς συναλλαγών ή οι μεγάλων αποστάσεων μεταφορείς, τα τηλεφωνικά κέντρα και οι ευρύτερες υπηρεσίες γραφείων.

VoIP to PSTN



Εικόνα 2: Κλήση από VoIP δίκτυο σε PSTN

PSTN to VoIP



Εικόνα 3: Κλήση από PSTN δίκτυο σε VoIP

Προς το παρόν, η επικοινωνία μέσω VoIP γίνεται ανάμεσα σε προσωπικούς υπολογιστές και τηλεφώνων. Στην περίπτωση των υπολογιστών γίνεται μετατροπή του αναλογικού σήματος φωνής σε IP. Στην περίπτωση των τηλεφώνων, ένα τηλέφωνο του δικτύου PSTN χρησιμοποιεί μια πύλη VoIP για να κάνει τη μετατροπή. Στο μέλλον, η επικοινωνία από τηλέφωνο σε τηλέφωνο με χρήση πυλών VoIP πιθανολογείται να αποτελέσει τον κυρίαρχο μέσο επικοινωνίας. Παρόλα αυτά το σύνολο των εφαρμογών VoIP δεν περιορίζεται στις απλές τηλεφωνικές συσκευές. Οι μελλοντικές συνδέσεις αναμένεται να περιλαμβάνουν:

Κινητά τηλέφωνα: δε θα δρομολογούν απλώς τηλεφωνικές κλήσεις πάνω στο Internet, αλλά επίσης θα μετατρέπονται σε επικοινωνίες "click to talk" για άμεση επικοινωνία.

PDA και τηλέφωνα Wi-Fi: όταν θα αποτελούν τμήμα ενός δικτύου Wi-Fi, θα χρησιμεύουν στη δημιουργία ενός προσωπικού, ιδιωτικού τηλεφωνικού συστήματος εντός ενός σπιτιού.

Cable και DSL modems: με τη βοήθεια ενός laptop, ενός headset, καθώς και με την προσθήκη του κατάλληλου software, θα μπορούν να πραγματοποιηθούν κλήσεις μέσω της οθόνης. Με την προσθήκη κάποιων φθηνών εφαρμογών ή υλικού, χαρακτηριστικά όπως η αναμονή και η αναγνώριση κλήσης φαίνονται πραγματοποιήσιμες.

PBXs: ένα IP-enabled PBX θα επιτρέπει τους χρήστες να πραγματοποιούν κλήσεις με τηλέφωνα IP ή laptops και να χρησιμοποιούν το Internet. Σε ανεπιθύμητες ή προβληματικές καταστάσεις, ένα off-site IP PBX θα μπορεί να συμβάλει στη διατήρηση της συνέχειας της λειτουργικής διαδικασίας.

Άλλες συσκευές hardware και software: Οι τηλεφωνικές εταιρείες θα χρησιμοποιούν έξυπνη δρομολόγηση (intelligent routing), IP Centrex και άλλες τεχνολογίες για τη δημιουργία software-defined δικτύων. Τα δίκτυα IP καθιστούν την παραπάνω ποικιλομορφία συσκευών δυνατή. Το IP συνδυάζει τις λειτουργικές διαφοροποιήσεις ανάμεσα στις συσκευές: τα κινητά τηλέφωνα μετατρέπονται σε προσωπικούς ψηφιακούς βοηθούς, τα τηλέφωνα SIP μετατρέπονται σε υπολογιστικές μηχανές Java και τα Wi-Fi handsets σε τερματικά σημεία κλήσεων SIP.

ΚΕΦΑΛΑΙΟ 2

ΤΜΗΜΑΤΑ ΕΝΟΣ VoIP ΔΙΚΤΥΟΥ

Στο προηγούμενο κεφάλαιο αναφέρθηκαν οι τέσσερις βασικές λειτουργίες που μπορούν να υλοποιηθούν με τη βοήθεια των δικτύων VoIP. Παρόλο που προσεγγίζουν διαφορετικά τις παραπάνω υλοποιήσεις απ' ότι το δημόσιο τηλεφωνικό δίκτυο (PSTN), φαίνεται ότι τα σημαντικότερα τμήματα που απαρτίζουν ένα VoIP σύστημα μοιάζουν σε λειτουργία με τα τμήματα ενός PSTN συστήματος.

Από τα παραπάνω προκύπτει ότι οι στοιχειώδεις λειτουργίες του PSTN δε χάνονται, αλλά μπορούν να εκτελεστούν και από τα VoIP δίκτυα. Τα πέντε τμήματα από τα οποία αποτελείται ένα VoIP δίκτυο είναι οι **συσκευές** (VoIP τηλέφωνα, κονσόλες κλπ), τα **PBX** (Call Processing Servers), τα **gateways**, το **IP δίκτυο**, και τα **SBC** (Session Border Controllers).

2.1 Συσκευές

Για την πραγματοποίηση εισερχόμενων και εξερχόμενων VoIP κλήσεων οι τελικοί χρήστες χρησιμοποιούν VoIP τηλέφωνα, κονσόλες και άλλες συσκευές.

Τα VoIP τηλέφωνα είναι δύο ειδών. Είτε μπορεί να μοιάζουν με τα γνωστά παραδοσιακά τηλέφωνα και να βασίζονται σε υλικό, είτε μπορεί να βασίζονται σε λογισμικό, οπότε στην περίπτωση αυτή ονομάζονται softphones. Τα softphones έχουν τις ίδιες λειτουργίες με τα IP τηλέφωνα και προσφέρουν τις ίδιες δυνατότητες, αλλά η διαφορά τους είναι κυρίως στο ότι απευθύνονται πρωτίστως σε κινητούς χρήστες που χρησιμοποιούν φορητούς υπολογιστές.

Οι VoIP κονσόλες έχουν επίσης εγκατεστημένο λογισμικό για softphones και έχουν τη δυνατότητα να συνδεθούν και να αλληλεπιδράσουν με IP τηλεφωνικές συσκευές. Οι κονσόλες αυτές είναι ουσιαστικά εφαρμογές οι οποίες προσφέρουν κάποια χαρακτηριστικά ελέγχου και έχουν δώσει τη δυνατότητα να αναπτυχθεί ένας νέος τύπος VoIP συσκευής που με τη βοήθεια ενός καλωδίου δικτύου τύπου Ethernet και μιας απλής αναλογικής συσκευής, πραγματοποιείται η σύνδεση με το IP δίκτυο. Όλα τα απαραίτητα VoIP πρωτόκολλα μπορούν να εκτελεστούν με την παραπάνω συσκευή αν χρησιμοποιηθούν οι κατάλληλοι επεξεργαστές και υλικό.

2.2 PBX

Τα PBX είναι κεντρικοί servers οι οποίοι διαχειρίζονται και ελέγχουν τις εισερχόμενες και εξερχόμενες VoIP συνδιαλέξεις. Κατά τη διάρκεια μιας τέτοιας κλήσης τα δεδομένα που ανταλλάσσονται είναι δεδομένα φωνής (payload) και δεδομένα σηματοδοσίας (signaling) ώστε να ξεκινήσει ή να τελειώσει μια συνδιάλεξη.

Τα PBX συνήθως διαχειρίζονται τα δεδομένα σηματοδοσίας που ανταλλάσσονται μεταξύ χρηστών για τον έλεγχο, την αρχικοποίηση και τον τερματισμό μιας VoIP κλήσης(πχ. SIP μηνύματα). Τα μηνύματα για τη μεταφορά των δεδομένων φωνής συνήθως δε γίνονται απ' τα PBXs.

2.3 GATEWAYS

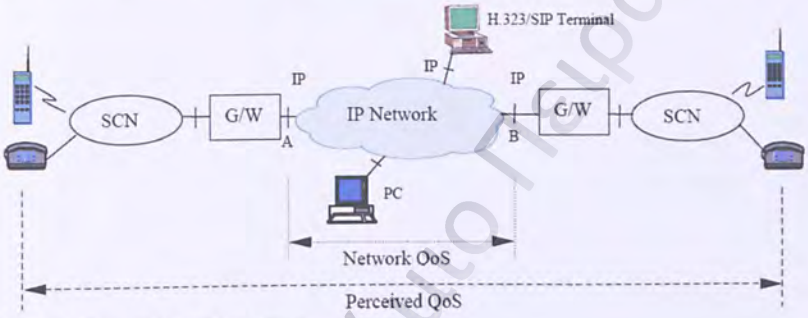
Τα gateways (πύλες) παίζουν πρωταρχικό ρόλο στην επικοινωνία ενός VoIP δικτύου με τον «έξω» κόσμο. Με τη χρήση ενός PSTN-to-VoIP Gateway επιτυγχάνεται η σύνδεση των χρηστών που βρίσκονται σε δύο διαφορετικά επικοινωνιακά δίκτυα, όπως για παράδειγμα το δημόσιο PSTN τηλεφωνικό δίκτυο και ένα VoIP δίκτυο ιδιωτικού παρόχου.

Για τη μετατροπή του σήματος φωνής από αναλογικό σε ψηφιακό και τη δημιουργία των πακέτων φωνής IP, το σύστημα VoIP χρησιμοποιεί media gateways. Έτσι δημιουργείται το απαραίτητο interface για να εκτελεστούν η λειτουργίες φωνής (λειτουργίες CODEC), προσαρμόζοντάς τες σε μια ακολουθία πακέτων UDP (RTP μεταφορά) μέσω του IP δικτύου.

Ένα χαρακτηριστικό γνώρισμα αυτών των media gateways είναι ότι αποτελούν πύλες ζεύξεων με σκοπό να συνδέσουν το δίκτυο PSTN με δίκτυα VoIP. Παρέχουν

υπηρεσίες έτσι ώστε να υπάρχει το κατάλληλο interface μεταξύ του παραδοσιακού αναλογικού τηλεπικοινωνιακού δικτύου και των IP-based δικτύων. Εναλλακτικά, είναι πιθανό να συναντήσουμε αντί για τον όρο 'media gateway', τον όρο 'gatekeeper'. Αυτό υποδεικνύει την ανάπτυξη της τεχνολογίας στο χώρο αυτό καθώς το δεύτερο όνομα δείχνει την πρόοδο που έχει γίνει ώστε η ίδια συσκευή να εκτελεί λειτουργίες gatekeeping, όπως Call Admission Control (CAC) και διαχείριση εύρους ζώνης, καθώς επίσης και την μετατροπή του σήματος φωνής από αναλογικό σε ψηφιακό σήμα, καθώς και άλλες στοιχειώδεις εργασίες επεξεργασίας φωνής που παραδοσιακά εκτελούνται από media gateways. Σε περίπτωση που έχουμε IP τηλέφωνο, όλα τα παραπάνω εκτελούνται απ' την ίδια τη συσκευή του τηλεφώνου.

Εκτός από τις παραπάνω λειτουργίες, τα media gateways παρέχουν επίσης και κάποιες προαιρετικές λειτουργίες. Πέρα απ'την αναλογική και ψηφιακή συμπίεση που αναφέρθηκε, η συλλογή στατιστικών (statistics gathering), η καταστολή σιωπής (silence suppression) και η ακύρωση ηχούς (echo cancellation) είναι κάποιες απ' αυτές. Η μορφή με την οποία μπορούν να εμφανιστούν τα διάφορα gateways είναι είτε σαν PC γενικού σκοπού που εκτελούν VoIP λογισμικό, είτε σαν dedicated πλαίσια τηλεπικοινωνιακού εξοπλισμού.



Εικόνα 4: διαδικτυακή σύνδεση VoIP

2.4 IP δίκτυο

Το IP δίκτυο είναι απαραίτητο για τη μεταφορά της audio πληροφορίας, προσφέροντας άκρως ικανοποιητική ποιότητα. Πολλές είναι υπηρεσίες μεταφοράς δεδομένων οι οποίες έχουν χρησιμοποιήσει δίκτυα IP, προτιμώντας τα ανάμεσα από άλλα δίκτυα επικοινωνιών.

Σε περίπτωση που το IP δίκτυο χρησιμοποιείται εκτός από τη μεταφορά φωνής και για τη μεταφορά και άλλου είδους δεδομένων, τότε θα πρέπει να μπορεί να διακρίνει τη διαφορά μεταξύ των τύπων αυτών και να δώσει την κατάλληλη προτεραιότητα. Προφανώς, σε περίπτωση που τα δεδομένα είναι μια ακολουθία φωνής, θα πρέπει να δοθεί προτεραιότητα, γιατί απαιτείται μεταφορά σε πραγματικό χρόνο και μια τέτοια πληροφορία είναι εξαιρετικά ευαίσθητη στην καθυστέρηση, στην απώλεια πακέτων και στο φαινόμενο jitter.

Απαιτείται λοιπόν ισορροπία για την επίτευξη των παραπάνω και αυτή επέρχεται με τη χρήση της τάξης της υπηρεσίας (CoS – Class of Service). Με το CoS εξασφαλίζεται η προτεραιότητα στα πακέτα μιας συγκεκριμένης εφαρμογής. Στις real-time VoIP εφαρμογές, οι υπηρεσίες φωνής έχουν τη δυνατότητα να μην επηρεάζονται από άλλες κυκλοφοριακές ροές και έτσι αποφεύγονται οι γνωστές ανεπάρκειες των dedicated κυκλωμάτων του παλιότερου δικτύου PSTN.

2.5 SBC (Session Border Controllers)

Τα SBCs λειτουργούν σε πραγματικό χρόνο με σκοπό, κατά τη διάρκεια ανταλλαγής των μηνυμάτων σηματοδοσίας, να ελέγχουν τη συμφόρηση και την κυκλοφορία του δικτύου. Κατά την εξέλιξη μιας VoIP κλήσης, το SBC έχει τη δυνατότητα να ελέγξει το περιεχόμενο της

πληροφορίας, οπότε ταυτόχρονα ο έλεγχος του εύρους ζώνης είναι εφικτός καθώς επίσης και η απομόνωση των προβλημάτων που δημιουργούνται μέσα στο δίκτυο. Ακόμα, επειδή το SBC μπορεί να ελέγξει και να συσχετίσει τα δεδομένα με τη σηματοδότηση, το καθιστά υπεύθυνο για την ασφάλεια και την ποιότητα των υπηρεσιών (QoS – Quality of Service).

Τα VoIP πρωτόκολλα σηματοδοσίας που υποστηρίζονται από τα SBCs είναι τα SIP, H.323, H.248, GCP, RTP (Real-Time Transport Protocol) και RTCP (Real-Time Transport Control Protocol) για τα οποία θα μιλήσουμε στα παρακάτω κεφάλαια. Όλα τα παραπάνω πρωτόκολλα συνδέονται με τη μεταφορά φωνής, βίντεο και άλλων πολυμεσικών δεδομένων.

ΚΕΦΑΛΑΙΟ 3

Το πρωτόκολλο H.323

Το πρωτόκολλο H.323 είναι ένα πρότυπο επικοινωνιών της σειράς H.32x . Με τη βοήθεια αυτού του πρωτοκόλλου έχουμε τη δυνατότητα επικοινωνίας με χρήση πολυμέσων πάνω από διάφορα είδη δικτύων όπως ISDN, PSTN και άλλα τοπικά δίκτυα, διασφαλίζοντας παράλληλα και την ποιότητα εξυπηρέτησης (Quality of Service). Το πρότυπο αυτό της ITU είναι βασικό στοιχείο έτσι ώστε να επιτρέπεται η μεταφορά video, φωνής και δεδομένων πάνω από IP δίκτυο.

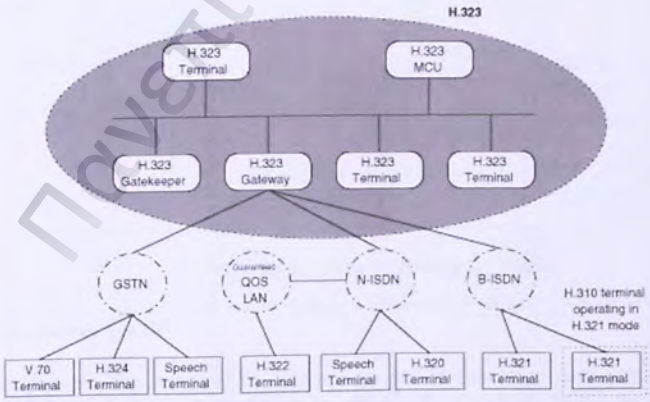
Το H.323 ενσωματώνει πολλά πρωτόκολλα όπως:

- Το πρότυπο **H.225.0**: μορφή και ροή μηνυμάτων σηματοδοσίας.
- Το πρότυπο **H.245**: έλεγχος κλήσεων και αποκατάσταση κλήσεων πολυμέσων.
- Το πρωτόκολλο **RAS**: καθορισμός μηνυμάτων (registration, access, status messages) και ανταλλαγή πληροφοριών μεταξύ τερματικών σημείων και των gateways.
- Τύπος συμπίεσης **G.711**: συμπίεση ήχου.
- Τύπος συμπίεσης **H.261**: συμπίεση εικόνας.

3.1 ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Βασικά χαρακτηριστικά του πρωτοκόλλου αυτού ότι αν ένας πελάτης H.323 υποστηρίζει μόνο επικοινωνία με ήχο, αυτό δεν τον κάνει ασύμβατο με κάποιον που μπορεί να υποστηρίζει επιπλέον επικοινωνία με δεδομένα και video. Κατά τη διάρκεια της σύνδεσης των δύο πελατών ανταλλάσσονται δεδομένα ανάμεσα στα τερματικά και ο ένας καταλαβαίνει τι μπορεί να υποστηρίξει ο άλλος και η επικοινωνία γίνεται με βάση τις ελάχιστες κοινές υπηρεσίες. Για να λειτουργήσουν όλα τα παραπάνω σωστά, κωδικοποιητές για video και ήχο είναι απαραίτητοι. Τα δύο τερματικά κατά τη διάρκεια του 'call set up' θα συμφωνήσουν για τη χρήση ενός κοινού CODEC για να συνδεθούν και να υπάρχει payload.

Ένα ακόμα χαρακτηριστικό του H.323 είναι ότι μπορούμε να έχουμε περιορισμό στο bandwidth (εύρος ζώνης) ή ακόμα και χρονικούς περιορισμούς στις κλήσεις. Παράλληλα υποστηρίζονται υπηρεσίες χρέωσης, υπηρεσίες εμπιστευτικότητας αλλά και έγκρισης – πιστοποίησης ταυτότητας καθώς επίσης και βοηθητικές υπηρεσίες όπως η προώθηση κλήσης.



Εικόνα 5: H.323 χαρακτηριστικά

Επιπλέον, το H.323 μπορεί να υποστηρίξει και σύνδεση μεταξύ τριών και πλέον τερματικών, στηριζόμενο σε μια πλατφόρμα πιο ευέλικτη και με περισσότερες υπηρεσίες. Είναι ανεξάρτητο από λειτουργικά αλλά και μηχανικά συστήματα και όχι μόνο μπορεί να χρησιμοποιηθεί σε PCs αλλά και σε IP τηλέφωνα, καλωδιακή τηλεόραση κ.ά. Στις επικοινωνίες πολλών τερματικών (πάνω από 2 τερματικών) υποστηρίζεται και η multicast μετάδοση, δηλαδή η αποστολή μετάδοσης σε πολλούς αποδέκτες. Το παραπάνω σημαίνει ότι αν έχουμε πολλούς προορισμούς, τότε το πακέτο στέλνεται μια φορά. Στην αντίθετη περίπτωση που έχουμε μόνο έναν αποδέκτη (unicast) δημιουργούνται πολλές point-to-point αποστολές και κατά την εκπομπή στέλνεται πακέτο παντού ανεξάρτητα από το αν έχει ζητηθεί ή όχι. Αυτό σημαίνει ότι οι πόροι του δικτύου δεν χρησιμοποιούνται τόσο αποτελεσματικά όσο θα έπρεπε.

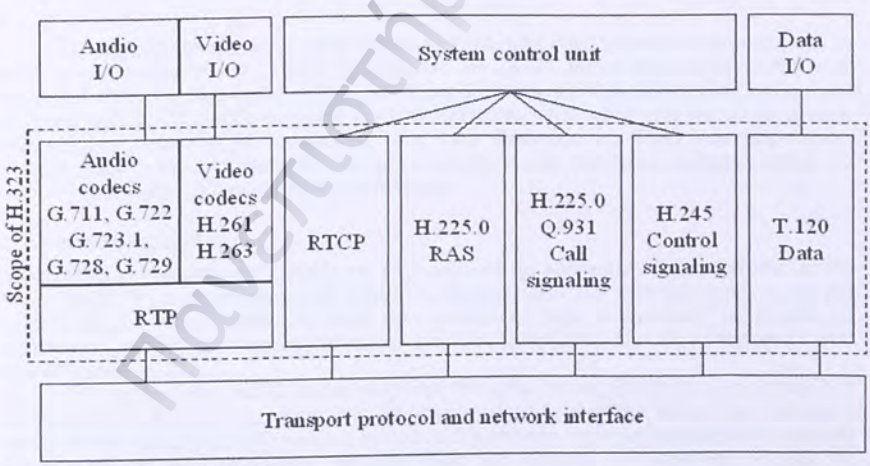
3.2 H.323 ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Το πρωτόκολλο H.323 είναι ικανό να εγκαταστήσει συνδέσεις πολυμέσων από σημείο σε σημείο (point-to-point) και από σημείο σε πολλαπλά σημεία (point-to-multipoint). Αυτό πετυχαίνεται συνδέοντας μεταξύ τους τερματικά (**terminals**), πύλες (**gateways**), ελεγκτές πύλης (**gatekeepers**) και ελεγκτές πολλαπλών σημείων (multipoint control units, **MCU**).

3.2.1 Τερματικά

Το ρόλο ενός τερματικού μπορεί να παίξει είτε ένα PC, είτε άλλες συσκευές multimedia που υποστηρίζουν το πρωτόκολλο H.323, έτσι ώστε να εδραιώσει την επικοινωνία διπλής κατεύθυνσης πραγματικού χρόνου. Όπως αναφέρθηκε και πιο πάνω το τερματικό θα πρέπει να υποστηρίζει αρχικά audio επικοινωνία και δευτερευόντως video και data.

Πιο συγκεκριμένα, τα τερματικά του H.323 υποστηρίζουν τα πρωτόκολλα H.245 για τη δημιουργία καναλιών, H.255 για τη σηματοδοσία και την προετοιμασία μιας κλήσης, το RTP/RTCP για την εξυπηρέτηση πακέτων video και audio, RAS για την καταχώρηση και την άδεια πρόσβασης στους ελεγκτές πύλης (gatekeepers), G.711 audio CODEC και video CODECs και T-120 πρωτόκολλα τηλεδιάσκεψης.



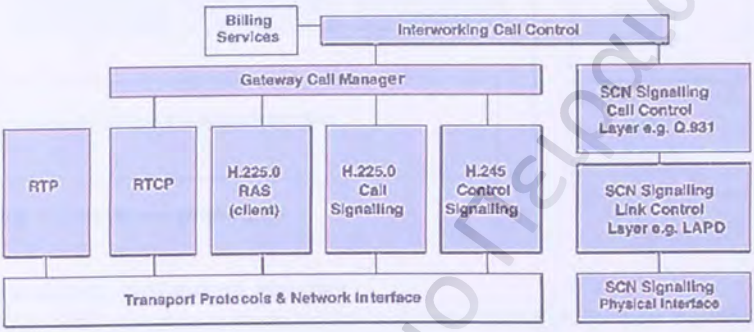
Εικόνα 6: Αρχιτεκτονική H.323

Τα τερματικά του H.323 είναι συμβατά με H.324 τερματικά σε ασύρματο δίκτυο, τερματικά H.310 σε B-ISDN, τερματικά H.320 σε ISDN, τερματικά H.321 σε B-ISDN και τερματικά H.322 σε LAN με εγγυημένο QoS.

3.2.2 Πύλες

Ένα gateway έχει τη δυνατότητα να συνδέει δίκτυα που δεν υποστηρίζουν το ίδιο πρωτόκολλο. Για παράδειγμα, μια κοινή περίπτωση στην τηλεφωνία είναι η σύνδεση IP δικτύου με κάποιο δίκτυο μεταγωγής κυκλώματος, μέσω της πύλης H.323. Η πύλη αυτή από τη μια "μιλάει" με το H.323 και τρέχει πρωτόκολλα για τον έλεγχο της σηματοδότησης, για την έναρξη και τη διακοπή της κλήσης και για τη λειτουργία του gatekeeper, και απ΄ την άλλη "μιλάει" με το δίκτυο μεταγωγής κυκλώματος και χρησιμοποιεί πρωτόκολλα ειδικά για switched circuit networks (SCN), π.χ. ISDN και SS7.

Ένα άλλο χαρακτηριστικό των gateways είναι ότι στην περίπτωση που τα τερματικά δε μπορούν να καταλήξουν σε έναν κοινό τρόπο επικοινωνίας, τότε αυτά έχουν τη δυνατότητα να μεταφράσουν τις πληροφορίες video και audio που ανταλλάσσονται.



Εικόνα 7: Λειτουργία των gateways

Το γεγονός ότι μια πύλη μπορεί να συμπεριφέρεται σαν ένα H.323 τερματικό, απ΄ τη μεριά που επικοινωνεί με H.323, δε σημαίνει ότι το IP δίκτυο την αντιμετωπίζει σαν τερματικό. Το δίκτυο έχει τη δυνατότητα να ξεχωρίζει πύλες και τερματικά με τη βοήθεια των ελεγκτών πύλης. Έτσι κάθε συσκευή κατά το registration που κάνει στο δίκτυο δηλώνει τι είναι και έτσι ο τρόπος αντιμετώπισης τους είναι διαφορετικός. Λόγω των παραπάνω, υπάρχει περίπτωση ένα gateway να μη συναντάται σαν αυτόνομη συσκευή, αλλά να βρίσκεται υλοποιημένη σαν μέρος του gatekeeper.

3.2.3 Ελεγκτές πύλης

Οι gatekeepers ελέγχουν τις κλήσεις και διαχειρίζονται το bandwidth, όπως ορίζεται απ΄ το RAS. Επειδή δεν είναι υποχρεωτικό τμήμα του δικτύου, δεν είναι πάντοτε παρόντες σε μια συνδεσμολογία. Στην περίπτωση όμως που υπάρχουν, όλα τα τερματικά θα πρέπει να λαμβάνουν υπόψη την παρουσία τους και να χρησιμοποιούν τις υπηρεσίες που προσφέρουν.

Το πρωτόκολλο H.323 ορίζει πως ένας ελεγκτής πύλης θα πρέπει να μεταφράζει διευθύνσεις, να ελέγχει τις εισόδους στο τερματικό, να ορίζει το εύρος ζώνης των κλήσεων, καθώς επίσης σε κάποιες περιπτώσεις να έχει τη δυνατότητα να σηματοδοτεί τον έλεγχο των κλήσεων και να είναι υπεύθυνος για την άδεια της κλήσης, τη διαχείρισή της και τη δρομολόγησή της.

Υπάρχει περίπτωση, όπως και πριν, ένας gatekeeper να μη συναντάται σαν αυτόνομη συσκευή, αλλά να βρίσκεται υλοποιημένη σαν μέρος του gateway.

3.3.1 ΔΙΑΣΚΕΨΗ ΠΟΛΥΜΕΣΩΝ

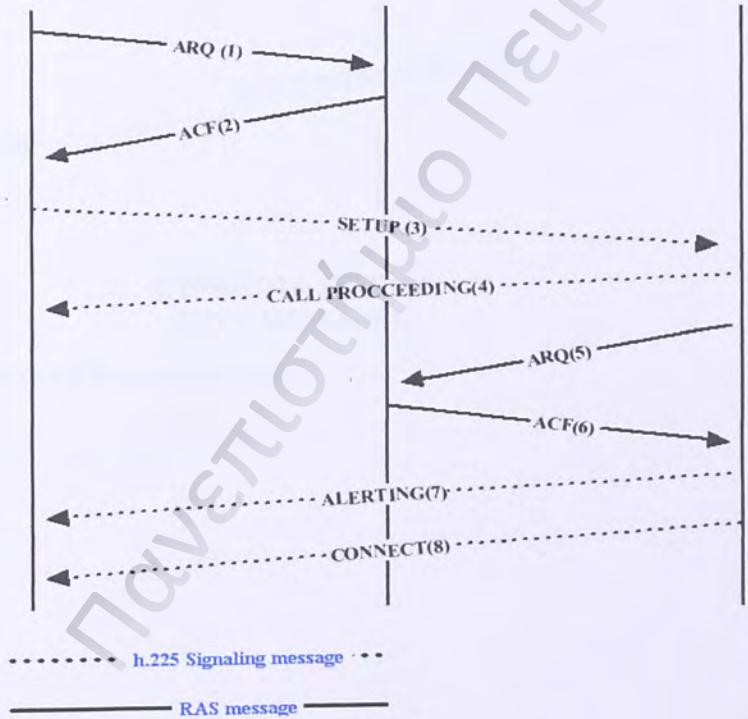
Το multimedia conferencing είναι μια δυνατότητα που παρέχεται μέσω του H.323 και είναι απαραίτητο για μεταφορά αρχείων, αποστολή fax και instant messaging. Το πρωτόκολλο T.120 δίνει αυτή τη δυνατότητα στο H.323 και είναι ειδικά σχεδιασμένο για τις ανάγκες διάσκεψης σε πραγματικό χρόνο μεταξύ πολλών τερματικών σε διαφορετικά δίκτυα.

Τα πλεονεκτήματα της μεθόδου αυτής σε σχέση με τη συνηθισμένη ανταλλαγή δεδομένων είναι ότι επιτρέπεται η διακίνηση και διανομή δεδομένων σε πολλαπλά σημεία ταυτόχρονα, οπότε μια ομάδα μπορεί να ασχοληθεί με το ίδιο αντικείμενο. Ακόμα το γεγονός ότι το T.120 λειτουργεί πάνω απ΄ το επίπεδο μεταφοράς, καθιστά το πρωτόκολλο ανεξάρτητο από τον τύπο του δικτύου και το λογισμικό που το στηρίζει. Τέλος, εκτός απ΄ τον έλεγχο που παρέχεται απ΄ το δίκτυο, υποστηρίζεται και επιπλέον έλεγχος λαθών, διασφαλίζοντας έτσι μια πιο αξιόπιστη παράδοση.

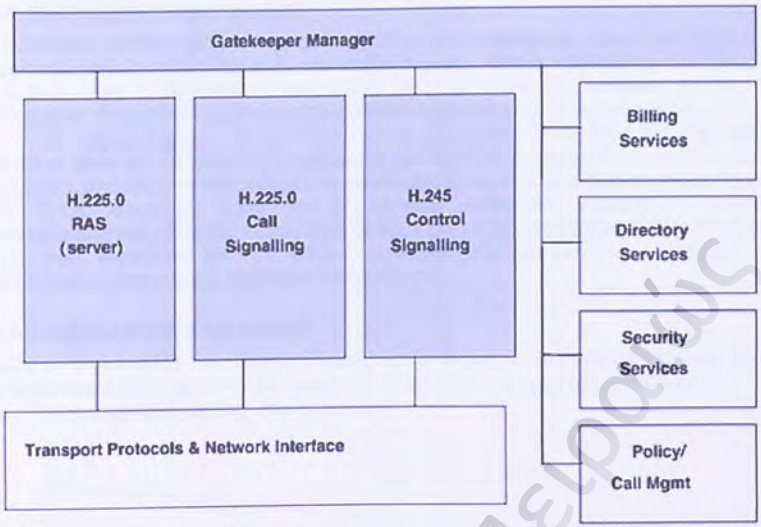
3.3.2 ΔΙΑΔΙΚΑΣΙΕΣ ΣΥΝΔΕΣΗΣ

Παρακάτω παρουσιάζονται κάποια παραδείγματα κλήσεων που αποκαθίστανται μέσω του πρωτοκόλλου H.323, έχοντας δύο τερματικά που συνδέονται με έναν gatekeeper:

- Αποκατάσταση κλήσης στο H.323



Εικόνα 9: Ροή μηνυμάτων H.323 σε μια βασική κλήση



Εικόνα 8: Λειτουργία των gatekeepers

3.2.4 Ελεγκτές πολλαπλών σημείων

Τα MCUs είναι προαιρετικές συσκευές που καθιστούν δυνατή τη σύνδεση περισσότερων των τριών τερματικών και τη μεταξύ τους συνδιάσκεψη.

3.3 ΣΗΜΑΤΟΔΟΣΙΑ ΚΛΗΣΕΩΝ ΚΑΙ ΕΛΕΓΧΟΥ

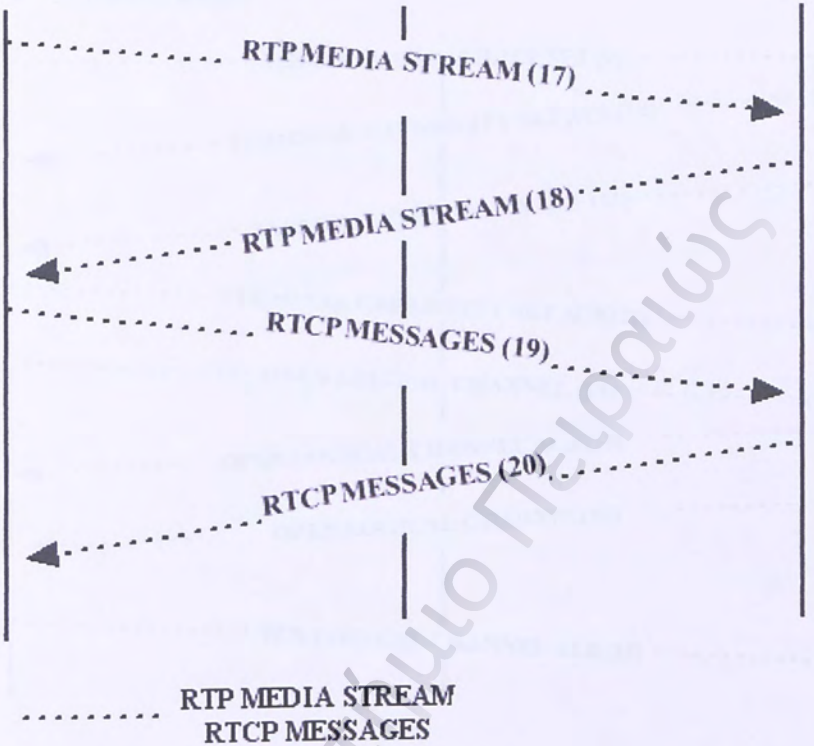
Το πρωτόκολλο H.323 επιτρέπει τη χρήση πολλών ρυθμίσεων από τα τερματικά. Αυτό επιτυγχάνεται με τη βοήθεια του πρωτοκόλλου H.245, του οποίου η ύπαρξη είναι υποχρεωτική σε όλα τα τερματικά σημεία. Έτσι προσδίδεται ευελιξία στο δίκτυο, αλλά είναι απαραίτητη η προ-συνεννόηση των τερματικών σε κοινές ρυθμίσεις πριν από την εκκίνηση της συνομιλίας.

Για να επιτευχθεί η παραπάνω συνεννόηση, τα δύο τερματικά ανταλλάσσουν όλες τους τις ικανότητες (όπως CODECs, bit rates, media types κ.α.) . Αφού τελειώσει η ανταλλαγή δυνατοτήτων, στέλνονται επιπλέον μηνύματα ελέγχου ροής, που παρέχουν ενημέρωση στα τερματικά σημεία για τα προβλήματα επικοινωνίας που παρουσιάζονται, όπως επίσης και μηνύματα για την ενημέρωση των τερματικών σημείων ή για αλλαγή κωδικοποιητή-αποκωδικοποιητή (codec).

Μια ακόμα λειτουργία του H.323 είναι το άνοιγμα και το κλείσιμο των λογικών καναλιών. Λογικά κανάλια είναι ουσιαστικά οι συνδέσεις μιας κατευθύνσεις από άκρο σε άκρο (unidirectional end-to-end links). Διαφορετικά κανάλια χρησιμοποιούνται για video, διαφορετικά για ήχο και διαφορετικά για δεδομένα. Η δημιουργία και το κλείσιμο αυτών των καναλιών γίνεται με τη βοήθεια του πρωτοκόλλου H.245, με μηνύματα που στέλνονται μέσω του καναλιού 0 που είναι πάντα ενεργό.

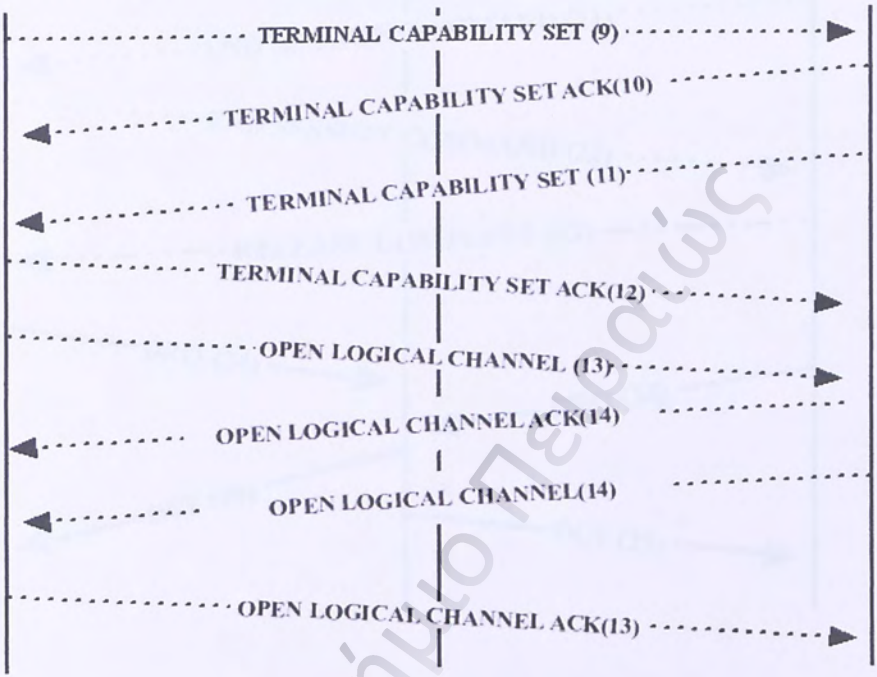
Όσον αφορά τη σηματοδοσία των κλήσεων, το H.323 χρησιμοποιείται για την ολοκλήρωση της σύνδεσης των τερματικών και για τη μεταφορά δεδομένων για εφαρμογές πραγματικού χρόνου. Η μεταφορά αυτή μπορεί να γίνει είτε μέσω κάποιου gatekeeper, είτε απ΄ ευθείας (direct call signaling). Τον τρόπο τελικά που θα γίνει η μεταφορά τον αποφασίζει ο ελεγκτής πύλης κατά τη διάρκεια της ανταλλαγής μηνυμάτων του RAS για τον έλεγχο πρόσβασης.

- Ροή πληροφορίας



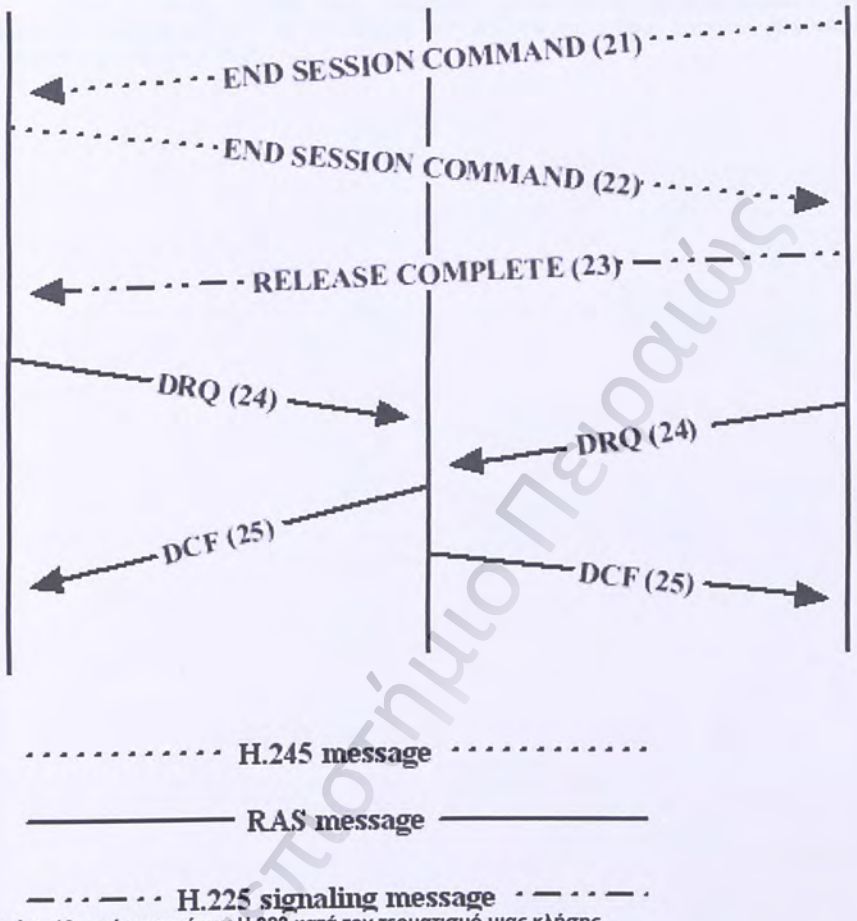
Εικόνα 10: Ροή RTP μηνυμάτων H.323

- Σηματοδοσία ελέγχου



Εικόνα 11: Σηματοδοσία ελέγχου H.323

- Τέλος κλήσης



Εικόνα 12: ροή μηνυμάτων H.323 κατά τον τερματισμό μιας κλήσης

3.4 ΑΣΦΑΛΕΙΑ

Το H.235 ασχολείται με τέσσερα θέματα που έχουν σχέση με την ασφάλεια:

- πιστοποίηση (authentication),
- ακεραιότητα (integrity),
- μυστικότητα (privacy),
- μη-αποκήρυξη (non-repudiation).

Η πιστοποίηση είναι ένας μηχανισμός που διασφαλίζει ότι οι χρήστες των τερματικών σημείων που παίρνουν μέρος σε μια συνομιλία είναι αυτοί που λένε ότι είναι. Παρέχεται μέσω του έλεγχου πρόσβασης των τερματικών σημείων. Υπεύθυνος για τον έλεγχο είναι ο ελεγκτής πύλης που ελέγχει τη ζώνη. Η ακεραιότητα παρέχει τα μέσα που επιβεβαιώνουν ότι τα δεδομένα σε κάθε πακέτο δεν έχουν αλλοιωθεί. Η μυστικότητα και η εμπιστευτικότητα παρέχονται μέσω κωδικοποίησης που κρύβει τα δεδομένα έτσι ώστε αν κάποιο πακέτο γίνει αντιληπτό να μην είναι δυνατή η ανάγνωσή του. Η μη-αποκήρυξη είναι

ένας τρόπος προστασίας έναντι κάποιου που θα ισχυριστεί ότι δεν πήρε μέρος σε μια συνομιλία ενώ ξέρουμε ότι ήταν εκεί.

Στην υλοποίηση αυτών των υπηρεσιών μπορούν να χρησιμοποιηθούν και υπάρχοντα πρότυπα όπως το IP security (IPsec) και το φυσικό επίπεδο ασφάλειας (transport layer security, TLS).

ΚΕΦΑΛΑΙΟ 4

ΧΡΗΣΙΜΑ ΠΡΩΤΟΚΟΛΛΑ

4.1 MGCP (media gateway control protocol)

Ο ρόλος του MGCP πρωτοκόλλου είναι να στέλνει εντολές από τους call agents στα gateways και αυτοί να τις εφαρμόζουν. Έτσι ορίζουν την ομαλή επικοινωνία τους. Το πρωτόκολλο αυτό προέκυψε από τη συγχώνευση δύο άλλων πρωτοκόλλων, του SGCP και του IPDC, και επιτρέπει σε έναν κεντρικό συντονιστή να ελέγχει τη δραστηριότητα στα IP τηλέφωνα και στα gateways και να τους δίνει οδηγίες για την αποστολή δεδομένων σε συγκεκριμένες διευθύνσεις. Τους ελεγκτές κλήσης (call agents) μπορούμε αν τους συναντήσουμε και ως media gateway controllers (πύλες ελέγχου φορέων επικοινωνίας).

Οι καινούριες έννοιες που ισχύουν με το MGCP πρωτόκολλο είναι η σύνδεση (**connection**), τα τερματικά σημεία (**endpoints**), τα γεγονότα (**events**) και τα σήματα (**signals**). Οι συνδέσεις και τα τερματικά σημεία χρησιμοποιούνται ώστε να δημιουργηθεί ένας διάδρομος μεταξύ των συνομιλούντων και τα γεγονότα και τα σήματα για την έναρξη και τον τερματισμό μιας κλήσης.

Τα endpoints ουσιαστικά αποτελούν τους πομπούς και τους δέκτες των δεδομένων. Οι συνδέσεις μεταξύ τους μπορούν να γίνουν πάνω από TCP, ATM και άλλα δίκτυα και να είναι είτε συνδέσεις point to point, είτε multipoint συνδέσεις.

Όσον αφορά τα γεγονότα και τα σήματα, ο call agent έχει τη δυνατότητα να ενημερωθεί για τα παραπάνω. Για παράδειγμα αν ξεκινήσει μια κλήση ή σηκώσει το ακουστικό κάποιο τερματικό σημείο, ο call agent θα λάβει το αντίστοιχο σήμα. Ανάλογα με τον τύπο της τερματικής συσκευής και με τις υπηρεσίες που υποστηρίζει, μπορεί να καταλάβει και να ανταποκριθεί στα γεγονότα και στα σήματα που θα δεχθεί.

Όπως φανερώνεται απ΄ τα παραπάνω, οι προγραμματιστικές δυσκολίες συγκεντρώνονται στους ελεγκτές κλήσης, έτσι ώστε οι παροχείς τέτοιων υπηρεσιών να παρέχουν εύκολη και φτηνή πρόσβαση στο δίκτυο.

4.1.1 Κυριότερες εντολές πρωτοκόλλου

Οι κυριότερες εντολές που χρησιμοποιούνται στο πρωτόκολλο MGCP είναι οι παρακάτω:

CreateConnection: δημιουργία σύνδεσης ανάμεσα σε μια θύρα (IP διεύθυνση) και σε ένα τερματικό σημείο. Η σύνδεση αυτή προσδιορίζεται μοναδικά από μια ταυτότητα (ConnectionId)

ModifyConnection: αλλαγή παραμέτρων μιας υπάρχουσας σύνδεσης.

DeleteConnection: διαγραφή υπάρχουσας σύνδεσης. Η διαγραφή αυτή γίνεται είτε από την πύλη, είτε από τον ελεγκτή κλήσης.

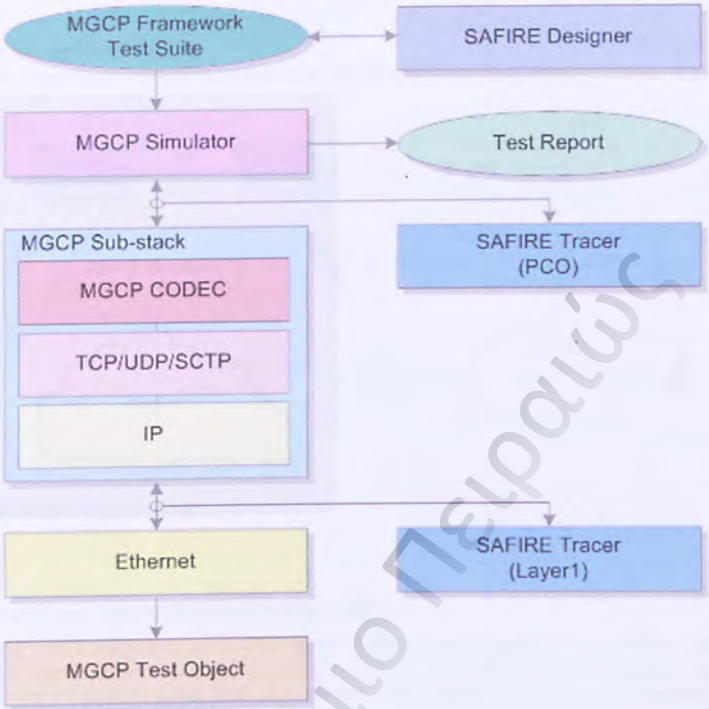
NotificationRequest: σήμα για ενημέρωση ότι κάποιο γεγονός έλαβε χώρα στο τερματικό σημείο.

Notify: η απάντηση στην εντολή NotificationRequest που στέλνεται από την πύλη.

AuditEndpoint: εντολή που στέλνει ο call agent, όταν θέλει να ρωτήσει για την κατάσταση στην οποία βρίσκεται κάποιο τερματικό.

AuditConnection: εντολή που στέλνει ο call agent, όταν θέλει να ρωτήσει πληροφορίες για μια συγκεκριμένη σύνδεση, ρωτώντας ακριβώς για κάποιο συγκεκριμένο ConnectionId.

RestartInProgress: εντολή που στέλνει το gateway όταν θέλει να δηλώσει ότι ένα τερματικό είναι εκτός λειτουργίας.



Εικόνα 13: MGCP αρχιτεκτονική

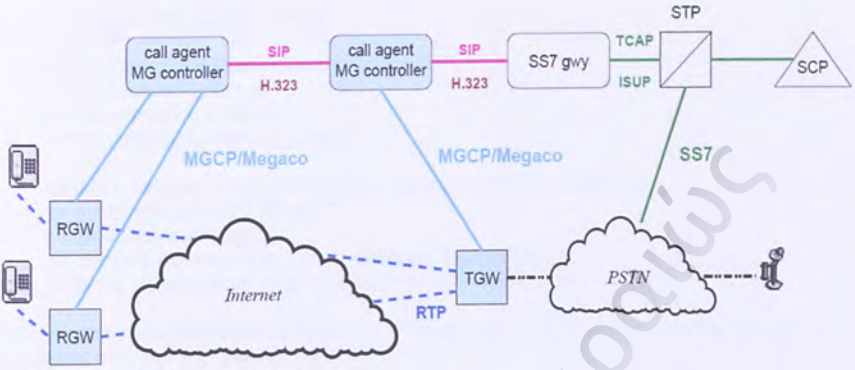
4.1.2 Δημιουργία Σύνδεσης

Η σύνδεση δύο τερματικών που βρίσκονται σε gateways, τα οποία ελέγχονται απ' τον ίδιο call agent γίνεται ως εξής:

Ο call agent ζητάει απ΄ την πύλη να φτιάξει μια σύνδεση με το τερματικό. Τότε η πύλη στέλνει πίσω μια απάντηση με τα χαρακτηριστικά της συνόδου. Οι πληροφορίες που περιέχονται στην απάντηση είναι απαραίτητες ώστε κάποιος να μπορέσει να συνομιλήσει με το συγκεκριμένο χρήστη. Στο σημείο αυτό ο call agent στέλνει την περιγραφή αυτή στο δεύτερο gateway, ώστε να μπορέσει να δημιουργήσει τη σύνδεση με το δεύτερο τερματικό σημείο και το δεύτερο gateway απαντά στέλνοντας τη δική της περιγραφή για τα χαρακτηριστικά της συνόδου της. Όταν ο call agent λάβει και τη δεύτερη απάντηση την προωθεί στο πρώτο τερματικό σημείο. Με τον τρόπο αυτό τα δύο τερματικά σημεία έχουν ανταλλάξει με επιτυχία τα χαρακτηριστικά και τις δυνατότητές τους και είναι σε θέση να επικοινωνήσουν.

Σε περίπτωση που τα δύο gateways έχουν διαφορετικούς call agents, η παραπάνω διαδικασία διαφέρει λίγο. Αυτό που γίνεται ουσιαστικά στην περίπτωση αυτή είναι ότι η ανταλλαγή των περιγραφών των συνόδων γίνεται πρώτα μεταξύ των δυο ελεγκτών, βασισμένη σε ειδικό πρωτόκολλο σηματοδοσίας.

MGCP/SIP architecture



Εικόνα 14: MGCP/SIP αρχιτεκτονική

4.2 SDP (Session Description Protocol)

Οι πληροφορίες που παρέχονται με το SDP είναι το όνομα και ο σκοπός της συνόδου, που αναφέρθηκε σε προηγούμενο κεφάλαιο, καθώς επίσης τα media, τα πρωτόκολλα, τους κωδικοποιητές και τις πληροφορίες που είναι απαραίτητες για το χρονισμό και όλα αυτά σε μια μορφή μικρού κειμένου. Το SDP είναι σε θέση να συνεργάζεται με πρωτόκολλα όπως τα SIP, HTTP κ.α. Επιπλέον επειδή μια σύνδεση μεταξύ δύο τερματικών έχει συγκεκριμένη διάρκεια και η σύνοδος θα παραμένει ενεργή μόνο για το συγκεκριμένο χρονικό διάστημα. Για το λόγο αυτό τα SDP μαζί με τις υπόλοιπες πληροφορίες μεταφέρουν και την ώρα έναρξης και λήξης μιας συνόδου.

4.2.1 Σύνταξη μηνύματος SDP

Ένα μήνυμα SDP αποτελείται από γραμμές της μορφής: *<τύπος>=<τιμή>*

Τύπος: ένας case significant χαρακτήρας.
Τιμή: κείμενο με μορφή που εξαρτάται από την τιμή του πεδίου <τύπος>.

Το μήνυμα αυτό έχει την παρακάτω μορφή:

```
v=0
o=mhandley 2890844526 2890842807 IN IP4 126.16.64.4
s=SDP Seminar
i=A Seminar on the session description protocol
u=http://www.cs.ucl.ac.uk/staff/M.Handley/sdp.03.ps
e=mjh@isi.edu (Mark Handley)
c=IN IP4 224.2.17.12/127
t=2873397496 2873404696
a=recvonly
m=audio 49170 RTP/AVP 0
m=video 51372 RTP/AVP 31
m=application 32416 udp wb
a=orient:portrait
```

4.2.2 Περιγραφή των πεδίων του μηνύματος

v= έκδοση πρωτοκόλλου
o= δημιουργός της συνόδου
s= το όνομα της συνόδου
i= πληροφορίες για τη σύνοδο *
u= URI *
e= διεύθυνση ηλεκτρονικού ταχυδρομείου *
p= τηλεφωνικό νούμερο *
c= πληροφορίες σύνδεσης *
b= πληροφορίες εύρους ζώνης

Μηδέν ή περισσότερες ενότητες με πληροφορίες συγχρονισμού
z= ρυθμίσεις χρονικής ζώνης *
k= κλειδί κωδικοποίησης *
a= μηδέν ή περισσότερα χαρακτηριστικά της συνόδου *
Μηδέν ή περισσότερες περιγραφές μέσων (media)

Κάθε περιγραφή συγχρονισμού αποτελείται από ένα πεδίο 't=' που προαιρετικά μπορεί να ακολουθείται από ένα ή περισσότερα πεδία 'r=' :
t= χρόνος κατά τον οποίο η σύνοδος είναι ενεργή
r= μηδέν ή περισσότερες επαναλήψεις *

Κάθε περιγραφή μέσου ξεκινάει όπως είπαμε με 'm=' και ακολουθούν τα παρακάτω προαιρετικά πεδία :
m= όνομα μέσου (media) και διεύθυνση μεταφοράς
i= τίτλος μέσου *
c= πληροφορίες σύνδεσης *
b= πληροφορίες εύρους ζώνης *
k= κλειδί κωδικοποίησης *
a= μηδέν ή περισσότερα χαρακτηριστικά media

Οι πληροφορίες της σύνδεσης (c=) και τα χαρακτηριστικά μέσα (media) (a=) στο επίπεδο συνόδου απευθύνονται σε όλα τα μέσα (media) της συνόδου εκτός και αν αναιρούνται από κάποιο πεδίο 'c=' ή 'a=' με το ίδιο όνομα μέσου (media).

ΚΕΦΑΛΑΙΟ 5

Το πρωτόκολλο SIP

Το SIP, όπως και το HTTP, είναι ένα client-server πρωτόκολλο (πελάτη - διακομιστή). Προτείνεται για τη δημιουργία VoIP συνδέσεων και είναι γνωστό και ως πρωτόκολλο εκκίνησης συνόδου, αφού το όνομα του προέρχεται από το αγγλικό Session Initiation Protocol. Είναι ένα πρωτόκολλο που ΄τρέχει΄ στο επίπεδο εφαρμογής (application-layer control protocol) και χρησιμοποιείται για την έναρξη, την τροποποίηση και τον τερματισμό τηλεφωνικών κλήσεων μέσω internet ή για τη διανομή πολυμέσων ή δημιουργία τηλεδιασκέψεων κ.α. Η κάθε τηλεφωνική κλήση (σύνοδος - session) μπορεί να αποτελείται από έναν ή περισσότερους συμμετέχοντες.

5.1 SIP ΑΡΧΙΤΕΚΤΟΝΙΚΗ

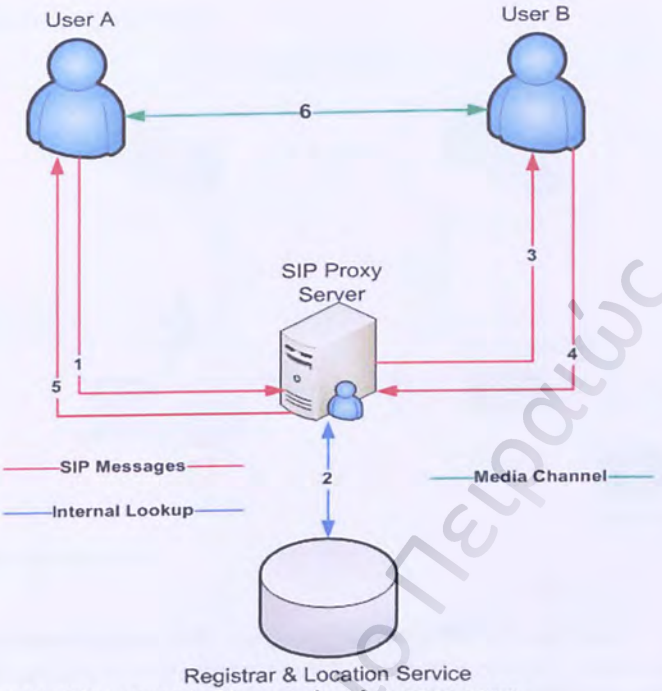
Στο SIP, που όπως αναφέρθηκε είναι ένα client-server πρωτόκολλο, ο πελάτης στέλνει requests και ο διακομιστής αφού τα επεξεργαστεί στέλνει την κατάλληλη απάντηση. Τα αιτήματα αυτά και οι απαντήσεις (requests - replies) αποτελούν μια συναλλαγή (transaction). Όσον αφορά τις κωδικοποιήσεις και αποκωδικοποιήσεις που χρειάζονται να γίνουν στα codecs, το SIP συνεργάζεται με το SDP (Session Description Protocol), που είναι πρωτόκολλο περιγραφής συνόδων και θα το περιγράψουμε αναλυτικότερα σε επόμενο κεφάλαιο. Οι πληροφορίες που περιέχονται μέσα στα SDP, ανταλλάσσονται μεταξύ των συμμετεχόντων της συνόδου και τους επιτρέπουν να συμφωνήσουν σε ένα σύνολο συμβατών μέσων.

Τα χαρακτηριστικά που διέπουν το πρωτόκολλο αυτό είναι ο προσδιορισμός της τοποθεσίας του χρήστη (user location) και του συστήματος που χρησιμοποιείται για επικοινωνία, καθώς επίσης και αν ο συγκεκριμένος χρήστης που θα λάβει μέρος στο transaction είναι διαθέσιμος (user availability). Το SIP είναι ακόμα ικανό να αποκαταστήσει μια κλήση και να ανταλλάξει τις παραμέτρους που είναι απαραίτητες σε όλες τις πλευρές που λαμβάνουν μέρος στο τηλεφώνημα (call setup). Οι πληροφορίες που αντιστοιχούν στον κάθε χρήστη είναι οι ικανότητες που έχει (user capabilities) και θα μεταφερθούν στους υπόλοιπους χρήστες. Όλοι οι χειρισμοί μιας κλήσης μπορούν να υποστηριχθούν απ το SIP πρωτόκολλο (call handling) όπως πχ. μια μεταφορά (call transfer) ή μια προώθηση(call forward) καθώς επίσης και ο τερματισμός της.

Κάποια απαραίτητα στοιχεία που απαρτίζουν το SIP και μας βοηθούν να το κατανοήσουμε καλύτερα είναι τα παρακάτω:

Ο πελάτης (client) είναι αυτός που στέλνει τα requests ο διακομιστής (server) είναι αυτός που τα λαμβάνει, στέλνει τα απαραίτητα replies και εξυπηρετεί τους πελάτες.

Η κλήση SIP αναγνωρίζεται από ένα μοναδικό call-id και αποτελείται από χρήστες που έχουν κληθεί απ την ίδια πηγή. Κάθε τέτοια πρόσκληση έχει ξεχωριστό call-id. Η επικεφαλίδα ενός SIP μηνύματος περιέχει τα πεδία To και From. Τα πεδία αυτά καθορίζουν τα σκέλη της κλήσης. Για το ίδιο call-id, τα μηνύματα από τον A στον B ανήκουν στο ίδιο σκέλος όπως και τα μηνύματα με την αντίθετη φορά.

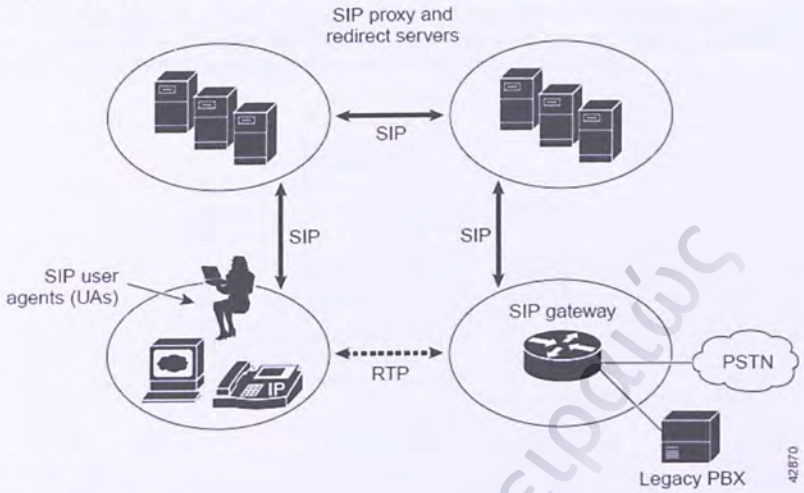


Εικόνα 15: SIP επικοινωνία δύο χρηστών, μέσω proxy server

Μια SIP συναλλαγή καθορίζεται από ένα μοναδικό αριθμό ακολουθίας που ονομάζεται CSeq και περιλαμβάνει όλα τα μηνύματα, από το πρώτο αίτημα που στέλνει ο πελάτης ως την απόκριση του διακομιστή. Εκτός απ΄ τον κύριο διακομιστή, στο πρωτόκολλο αυτό συναντάμε τις έννοιες του ενδιάμεσου διακομιστή (Proxy server), το διακομιστή επανακατεύθυνσης (Redirect server), το διακομιστή θέσης (Location server) και τον outbound proxy. Ο Proxy server μπορεί να λειτουργήσει και σα διακομιστής και σαν πελάτης και κυρίως προωθεί μηνύματα άλλων πελατών. Ο Redirect server, αντίθετα με τον proxy, δεν προωθεί τα μηνύματα που δέχεται αλλά στέλνει πίσω στον αποστολέα τους τη νέα διεύθυνση που πρέπει να ξαναστείλει το μήνυμα. Ο Location server βοηθά τους άλλους δύο διακομιστές να πάρουν πληροφορίες για τη θέση του παραλήπτη ενός μηνύματος. Τέλος, ο outbound proxy είναι ένας proxy που δέχεται όλη την κίνηση που δημιουργείται, ακόμα και αυτή που προορίζεται για κάποιο άλλο τερματικό-πομπό και βρίσκεται κοντά στον πελάτη που δημιουργεί τα μηνύματα.

Επιπλέον, υπάρχει και ένας διακομιστής - εγγραφέας (registrar) που δέχεται τα μηνύματα REGISTER και ένας user agent, ο οποίος είναι μια εφαρμογή που περιλαμβάνει τόσο τον user agent client όσο και τον user agent server. Ο user agent client είναι το τμήμα που στέλνει μηνύματα ενώ ο user agent server τα δέχεται.

Figure 1-1 SIP Architecture



Εικόνα 16: SIP αρχιτεκτονική

5.2 Διευθυνσιοδότηση SIP - εύρεση server - SIP συναλλαγή

Οι διευθύνσεις που χρησιμοποιεί το SIP μοιάζουν σε μορφή μ΄ αυτές ενός e-mail. Μπορούμε να συναντήσουμε διευθύνσεις της μορφής user@domain, user@host, user@ip_address, phonenumber@gateway μέσω των οποίων βρίσκεται ο διακομιστής στον οποίο «ανήκει» ο χρήστης που έχει καλεστεί.

Το πλεονέκτημα της μορφής αυτής είναι ότι η διεύθυνση αυτή μπορεί να μετατραπεί σε URI και να ενσωματωθεί σε μια ιστοσελίδα έτσι ώστε ενεργοποιώντας μια σύνδεση (link) ξεκινάει η κλήση όπως γίνεται στο mailto:URL.

Η εύρεση του διακομιστή είναι η διαδικασία δρομολόγησης του επόμενου βήματος, γνωστή και σα next-hop routing. Σε περίπτωση που ο διακομιστής βρει πολλούς διακομιστές στην ίδια απόσταση, τότε το SIP, με τη βοήθεια του proxy server, μπορεί να στείλει παράλληλα το ίδιο εισερχόμενο request σε πολλούς διακομιστές.

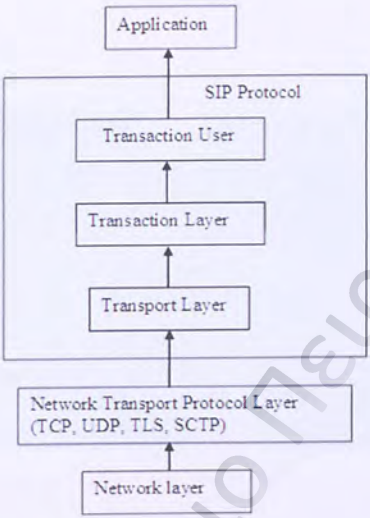
Αφού βρεθεί ο κατάλληλος server για να δρομολογηθεί η κλήση, τότε στέλνονται όλα τα αιτήματα που προορίζονται γι αυτόν. Για την αποστολή των requests χρησιμοποιούνται δυο πρωτόκολλα, το UDP και το TCP. Το TCP είναι πιο αξιόπιστο και τα μηνύματα της ίδιας συναλλαγής μεταφέρονται μέσω της ίδιας σύνδεσης. Αν χρησιμοποιηθεί UDP, τότε το reply στέλνεται με βάση τις πληροφορίες που περιέχει το πεδίο Via στην επικεφαλίδα του αιτήματος. Η αξιοπιστία του πρωτοκόλλου UDP εξασφαλίζεται με την επαναποστολή.

Σε περίπτωση που η τοποθεσία του χρήστη αλλάξει, η πληροφορία αυτή θα γραφτεί δυναμικά σε ένα SIP server. Το τμήμα του server που εκτελεί αυτή τη λειτουργία ονομάζεται location manager (διαχειριστής θέσης) και όταν ερωτηθεί για κάποιο συγκεκριμένο χρήστη, τότε ο location manager επιστρέφει μια λίστα με όλες τις πιθανές τοποθεσίες.

Αν αλλάξουν άλλες παράμετροι της συνόδου, τότε στέλνεται ένα νέο μήνυμα **INVITE** με το ίδιο call-id και με περιεχόμενο τις νέες παραμέτρους, αλλά με διαφορετικό CSeq. Το CSeq πρέπει να είναι μεγαλύτερο από κάθε προηγούμενο request του πελάτη στο server.

5.3 ΙΔΙΟΤΗΤΕΣ SIP

Επειδή το SIP βασίζεται σε κείμενο, με τη βοήθεια του ISO 10646 σε κωδικοποίηση UTF-8, είναι πολύ εύκολο να υλοποιηθεί σε γλώσσες όπως java, tcl και perl και να ερευνηθούν τυχόν λάθη. Οι δυνατότητες αυτές το κάνουν πολύ αξιόπιστο και ευέλικτο.



Εικόνα 17: SIP layers

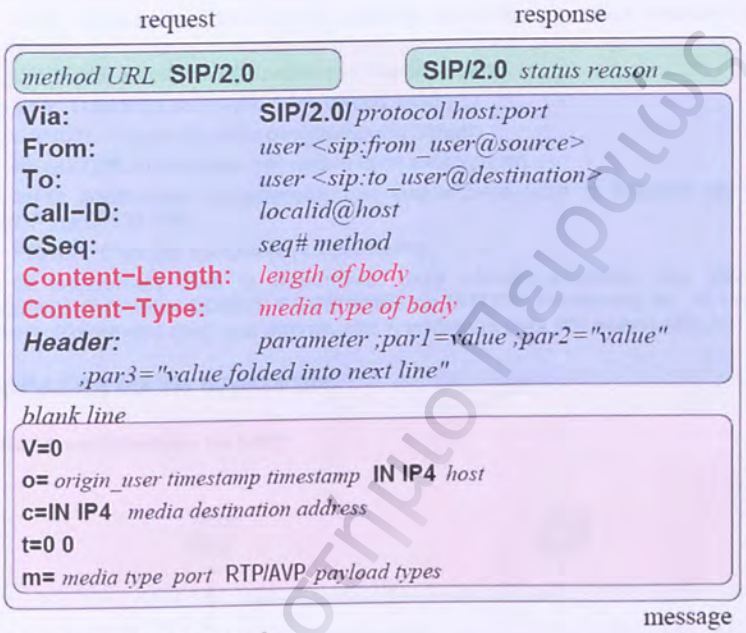
Μια SIP κλήση μπορεί να αποτελείται από περισσότερες από μία συναλλαγές (transactions), εκ των οποίων κάθε μια μπορεί να ακολουθεί διαφορετική διαδρομή. Το INVITE μήνυμα μπορεί να περάσει από πολλούς servers στην περίπτωση αυτή. Όταν μια συναλλαγή τελειώσει, τότε τα δεδομένα της κλήσης δεν αποθηκεύονται και ο server δε θυμάται τους συμμετέχοντες στην κλήση. Αυτό έχει σαν αποτέλεσμα να μην επηρεάζονται οι κλήσεις σε περίπτωση crash & recover του server, να μην δεσμεύονται για μεγάλο χρονικό διάστημα οι πόροι του συστήματος και να ελευθερώνονται κατά το πέρας της κλήσης, πράγμα που κάνει το σύστημα πολύ αξιόπιστο.

Αν ρίξουμε μια πιο λεπτομερή ματιά στον τρόπο που λειτουργούν οι συγκεκριμένοι διακομιστές θα διαπιστώσουμε ότι η συμπεριφορά τους ταιριάζει με την τεχνική αποστολής αυτοτελών πακέτων (datagram), αρχιτεκτονική του internet που τα πακέτα περιέχουν αρκετές πληροφορίες για να δρομολογούνται ανεξάρτητα. Έτσι οι διακομιστές λαμβάνουν ένα μήνυμα, το απαντούν ή το προωθούν και ύστερα ξεχνούν τα πάντα.

5.4 ΜΗΝΥΜΑΤΑ SIP

Τα κυριότερα μηνύματα είναι το αίτημα που δημιουργείται από έναν πελάτη ή απόκριση που δημιουργείται από ένα διακομιστή. Μια πετυχημένη πρόσκληση ενός πελάτη αποτελείται από δύο requests: το INVITE ακολουθούμενο από ένα ACK. Το INVITE χρησιμοποιείται για να καλέσει κάποιον ο πελάτης σε μια συνομιλία ή σε μια διάσκεψη και όταν λάβει την απάντηση, τότε με το ACK επιβεβαιώνει ότι έλαβε το reply. Συνήθως το INVITE περιέχει μέσα SDP έτσι ώστε να δώσει τις απαραίτητες πληροφορίες στο χρήστη που βρίσκεται στην άλλη πλευρά της σύνδεσης. Αντίστοιχα, ο καλούμενος χρήστης, όταν θα δεχθεί να λάβει μέρος στην κλήση αυτή, θα στείλει κι αυτός τα δικά του χαρακτηριστικά με ένα παρόμοιο μήνυμα.

Όσον αφορά τη σύνταξη των SIP μηνυμάτων, ακολουθούν τις προδιαγραφές του HTTP/1.1, είτε είναι μηνύματα αιτήματος (request), είτε μηνύματα απόκρισης (response). Και οι δυο τύποι μηνυμάτων έχουν παρόμοια μορφή. Αποτελούνται από μια αρχική γραμμή κατάστασης (έκδοση του SIP και status-code), ένα ή περισσότερα πεδία επικεφαλίδας , μια γραμμή που περιέχει μόνο ένα χαρακτήρα ώστε να δείξει το τέλος της επικεφαλίδας και προαιρετικά το σώμα του μηνύματος. Η μορφή ενός τέτοιου μηνύματος φαίνεται στο επόμενο σχέδιο:



Εικόνα 18: SIP request and response

Το status-code είναι ο κώδικας κατάστασης και αποτελείται από έναν τριψήφιο αριθμό. Οι τύποι αυτού του πεδίου περιγράφονται παρακάτω:

1xx: Το αίτημα ελήφθη και προωθείται για επεξεργασία (180 RINGING)

2xx: Πετυχημένη παραλαβή (200 OK)

3xx: Επιπλέον ενέργειες πρέπει να γίνουν για να ολοκληρωθεί το αίτημα (302 MOVED TEMPORARILY)

4xx: Το αίτημα έχει λάθος σύνταξη ή δεν μπορεί να εκπληρωθεί από αυτόν το διακομιστή (404 NOT FOUND)

5xx: Το αίτημα δεν έχει λάθη αλλά ο διακομιστής δεν μπορεί να το εκπληρώσει (501 NOT IMPLEMENTED)

6xx: Το αίτημα δεν μπορεί να εκπληρωθεί από κανένα διακομιστή (600 BUSY EVERYWHERE)

Μια SIP εφαρμογή δεν είναι απαραίτητο να μπορεί να ερμηνεύσει όλα τα πεδία της επικεφαλίδας, αν και θα ήταν επιθυμητό. Οπότε αν δεν καταλάβει κάποιο απ΄ αυτά τότε το

αγνοεί. Τα είδη των πεδίων της επικεφαλίδας ξεχωρίζουν σε πεδία που χρησιμοποιούνται και στους δυο τύπους μηνύματος, σε πεδία που ορίζουν το περιεχόμενο του μηνύματος, σε πεδία που μεταφέρουν επιπλέον πληροφορίες για το αίτημα και τον αποστολέα του και σε πεδία που δίνουν πληροφορίες στον πελάτη για το διακομιστή και για την παραπέρα πρόσβαση στον πόρο που περιγράφεται στο request-uri.

Το SIP χρησιμοποιεί κάποιες μεθόδους, των οποίων τα ονόματα είναι case sensitive:

INVITE: Προσκαλεί ένα χρήστη ή μια υπηρεσία σε μια σύνοδο. Το σώμα του μηνύματος περιέχει την περιγραφή της συνόδου.

ACK: Επιβεβαιώνει ότι ο καλών χρήστης έχει λάβει την τελική απόκριση σε ένα αίτημα INVITE.

OPTIONS: Χειρίζεται τις δυνατότητες του διακομιστή.

BYE: Τερματίζει μια κλήση ή ένα αίτημα κλήσης.

CANCEL: Τερματίζει κάθε ανολοκλήρωτο αίτημα.

REGISTER: Καταγράφει την τωρινή θέση ενός χρηστή.

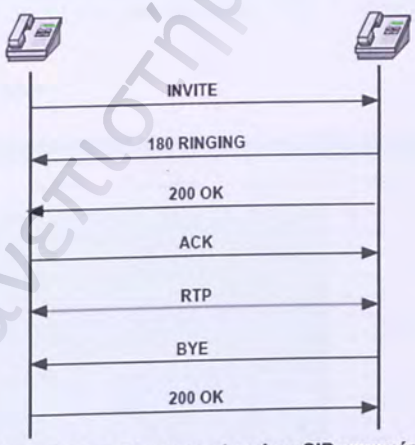
INFO: Αναπαριστά πληροφορίες που εμφανίζονται κατά τη διάρκεια της κλήσης όπως ISUP και DTFM τόνοι.

PRACK: Είναι μια προσωρινή επιβεβαίωση.

Οι βασικότερες είναι οι παραπάνω, αλλά κάποιες επιπλέον που μπορεί να συναντήσουμε είναι και οι **COMET**, **SUBSCRIBE** και **NOTIFY**. Αν κάποιες απ΄ τις μεθόδους δεν υποστηρίζονται από τους user agents, τότε η απάντηση είναι **501 server failure**.

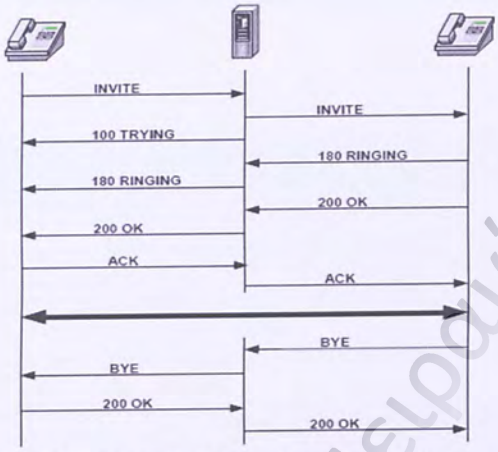
5.5 ΠΑΡΑΔΕΙΓΜΑΤΑ ΚΛΗΣΕΩΝ

5.5.1 Απλό παράδειγμα κλήσης



Εικόνα 18: Απευθείας σύνδεση δύο χρηστών μέσω SIP μηνυμάτων

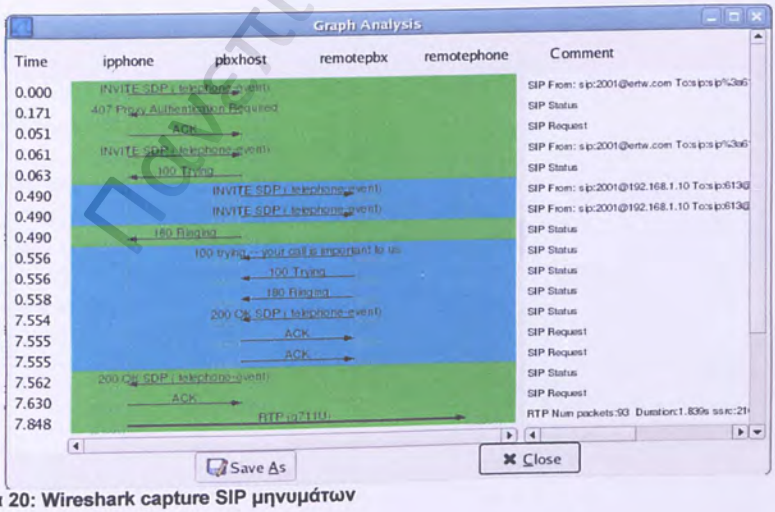
5.5.2 Παράδειγμα κλήσης με proxy server



Εικόνα 19: Σύνδεση δύο χρηστών με SIP μηνύματα, μέσω gateway

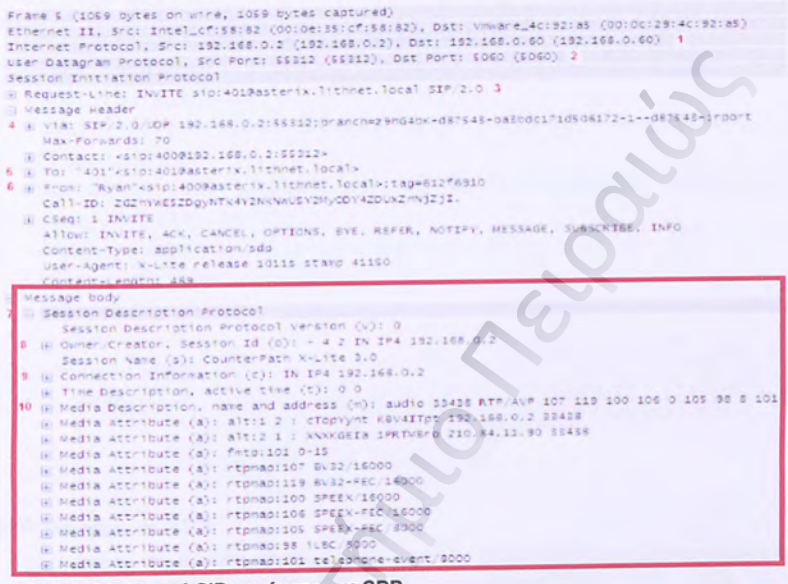
Τα παραδείγματα δείχνουν τη χρήση των αποκρίσεων που μεταφέρουν πληροφορίες για την κατάσταση της κλήσης. Εδώ η υποδοχή της κλήσης γίνεται αμέσως (100 Trying), το τηλέφωνο χτυπάει (180 Ringing), μπαίνει στην ουρά και περιοδικά ενημερώνει για την κατάσταση της κλήσης. Επειδή τα δυο τερματικά έχουν συμφωνήσει στα μέσα επικοινωνίας, επιβεβαιώνεται η κλήση χωρίς να συμπεριληφθεί ξανά η περιγραφή της συνόδου (ACK). Ο τερματισμός της κλήσης γίνεται όταν ο σταλθεί το μήνυμα BYE και επιβεβαιωθεί με το 200 OK.

5.5.3 Παράδειγμα με SDP



Εικόνα 20: Wireshark capture SIP μηνυμάτων

Στο παράδειγμα αυτό βλέπουμε ότι το INVITE, καθώς και το 200 OK που παίρνουμε σα response, περιέχουν SDP. Έτσι φαίνεται ο τρόπος ανταλλαγής των ικανοτήτων του κάθε μέλους της συνόδου. Τα SDP περιέχονται στο κύριο σώμα το μηνύματος και έχουν την παρακάτω μορφή:



Εικόνα 21: Μορφή SIP μηνύματος με SDP

5.5.4 Παράδειγμα SIP SUBSCRIBE

```
SUBSCRIBE sip:bob@macrosoft.com SIP/2.0
Event: presence
To: sip:bob@macrosoft.com
From: sip:user@example.com
Contact: sip:user@userpc.example.com
Call-ID: knsd08alas9dy@3.4.5.6
CSeq: 1 SUBSCRIBE
Expires: 3600
Content-Length: 0
```

5.5.5 Παράδειγμα SIP NOTIFY

```
NOTIFY sip:user@userpc.example.com
To: sip:user@example.com
From: sip:alice@wonderland.com
Call-ID: knsd08alas9dy@3.4.5.6
CSeq: 1 NOTIFY
Content-Type: application/xpidf+xml
<?xml version="1.0"?>
<!DOCTYPE presence
PUBLIC "-//IETF//DTD RFCxxxx XPIDF 1.0//EN" "xpidf.dtd">
<presence>
<presentity uri="sip:alice@wonderland.com;method="SUBSCRIBE">
<atom id="779js0a98">
<address uri="sip:alice@wonderland.com;method=INVITE">
<status status="closed"/>
</address>
</atom>
</presentity>
</presence>
```

5.6 SIP versus H.323

Ένα από τα πιο δυνατά σημεία του SIP είναι η δυνατότητά του να ενσωματώνει άλλα πρωτοκολλά. Πιο συγκεκριμένα το SIP μπορεί να συνεργάζεται πολύ καλά με δυο εφαρμογές που κυριαρχούν στο internet , το web και το mail. Η συνεργασία του SIP με το Web είναι σε πολλά επίπεδα. Και τα δύο μεταφέρουν περιεχόμενο MIME και αυτό επιτρέπει στο SIP να επιστρέφει το αποτέλεσμα ενός μηνύματος σε μια ιστοσελίδα.

Οι χρήστες αναγνωρίζονται με τη χρήση ενός URL που μπορεί να μπει σε κάθε εφαρμογή που χρησιμοποιεί URLs , όπως το mail και το web. Έτσι μπορεί να εκκινήσει κανείς μια κλήση κάνοντας απλά ένα click όπως ακριβώς για να πάει σε μια άλλη ιστοσελίδα. Με τη χρήση προς τα πίσω συμβατότητας το SIP μπορεί να έχει πρόσβαση σε εργαλεία όπως το CGI (common gateway interface). Μέσω προγραμματισμού μπορούν να υλοποιηθούν υπηρεσίες, όπως η προώθηση κλήσης και εικονικά ιδιωτικά δίκτυα (virtual private networks).

Μια διεύθυνση SIP είναι ίδια με μια διεύθυνση email. Έτσι ένα μήνυμα **INVITE** μπορεί να σταλεί και μέσω mail αν όλοι οι άλλοι τρόποι αποτύχουν. Επίσης η μορφή των μηνυμάτων SIP και SMTP είναι παρόμοια και ένας διακομιστής μπορεί εύκολα να μετατρέψει ένα μήνυμα SIP σε mail και να το προωθήσει στον παραλήπτη στην περίπτωση που είναι offline.

Εκτός από το SIP, υπάρχουν κι άλλα πρωτόκολλα που διευκολύνουν τη μετάδοση φωνής πάνω από IP δίκτυα. Ένα τέτοιο πρωτόκολλο είναι και το H.323. Το H.323 δημιουργήθηκε σύμφωνα με τα διεθνή πρότυπα τηλεπικοινωνιών (ITU) και χρησιμοποιείται και για τα πακέτα τηλεφωνίας και για την τηλεοπτική ροή (video streaming). Το πρότυποο H.323 ενσωματώνει πολλά πρωτόκολλα, συμπεριλαμβανομένου του Q.931 για τη σηματοδότηση, του H.245 για τη διαπραγμάτευση, και το RAS για τον έλεγχο συνόδου. Το H.323 ήταν από τα πρώτα πρότυπα για τον έλεγχο κλήσης για VoIP.

Το SIP και το H.323 σχεδιάστηκαν για να εξετάσουν τον έλεγχο των συνόδων και τις λειτουργίες σηματοδότησης σε μια κλήση. Αν και το SIP και το H.323 μπορούν να χρησιμοποιηθούν για να επικοινωνούν με endpoints περιορισμένης νοημοσύνης, είναι το ίδιο κατάλληλα για να υποστηρίξουν συνδέσεις μεταξύ περισσότερο ευφυών χρηστών.

Αν και τα μηνύματα SIP δεν είναι άμεσα συμβατά με το H.323, και τα δύο πρωτόκολλα μπορούν να συνυπάρξουν στο ίδιο δίκτυο τηλεφωνίας, εάν διαθέτουμε μια συσκευή που υποστηρίζει τη διαλειτουργικότητα. Παραδείγματος χάριν, ένας call agent θα μπορούσε να χρησιμοποιήσει H.323 για να επικοινωνήσει με τα gateways και SIP για τη σηματοδοσία της εσωτερικής κλήσης. Κατόπιν, αφού πραγματοποιηθεί η σύνδεση, η ροή πληροφοριών μεταφέρεται μεταξύ των δύο πυλών ως RTP stream.

Ο παρακάτω πίνακας περιέχει μια μικρή σύγκριση των δύο πρωτοκόλλων:

Aspect	SIP	H.323
Clients	Intelligent	Intelligent
Network intelligence and services	Provided by servers(Proxy, Redirect, Registrar)	Provided by gatekeepers
Model used	Internet/WWW	Telephony/Q.SIG
Signaling protocol	UDP or TCP	TCP (UDP is optional in version 3)
Media protocol	RTP	RTP
Code basis	ASCII	Binary (ASN.1 encoding)
Other protocols used	IETF/IP protocols, such as SDP, HTTP/1.1, IPmc and MIME	ITU/ISDN protocols, such as H.225, H.245 and H.450
Vendor interoperability	Widespread	Widespread

Εικόνα 22: SIP vs H.323

5.7 SIP-based υπηρεσίες

Άλλες υπηρεσίες που υποστηρίζονται από το SIP πρωτόκολλο είναι η προώθηση κλήσεων, η μεταφορά τους, η αναμονή κλήσεων, η μεταφορά των DTMF ψηφίων σαν ροή RTP καθώς και η υπηρεσία του τηλεφωνητή (voicemail).

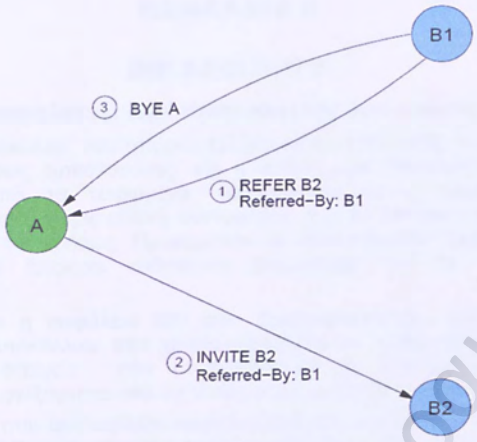
Η προώθηση κλήσεων (Call forwarding): γίνεται με τη βοήθεια της βασικής συμπεριφοράς του INVITE μηνύματος που προωθείται από έναν proxy.

Η μεταφορά των κλήσεων (Call transfer): γίνεται με την ανταλλαγή REFER μηνυμάτων, όπως φαίνεται και στο πιο κάτω σχήμα.

Η αναμονή (Call hold): πετυχαίνεται βάζοντας ξεχωριστά για κάθε μέσο την τιμή της διεύθυνσής του ίση με 0.0.0.0.

Η μεταφορά των DTMF ψηφίων (DTMF carriage): γίνεται μέσω του RTP stream.

Η υπηρεσία του τηλεφωνητή (Voice mail): επιτυγχάνεται με τη χρήση ειδικών URL(s) και πιθανότατα τη χρήση RTSP.



Εικόνα 23: SIP flow για την υπηρεσία Call Transfer

ΚΕΦΑΛΑΙΟ 6

SIP SECURITY

6.1 Εκτιμήσεις ασφάλειας: Πρότυπο απειλής και χρήση ασφάλειας

Το SIP δεν είναι πρωτόκολλο που μπορείς εύκολα να το ασφαλίσεις. Η χρήση μεσαζόντων, οι πολύπλευρες σχέσεις εμπιστοσύνης, και η user-to-user λειτουργία του φέρνουν την ασφάλεια μακριά από τα τετριμμένα. Απαιτούνται λύσεις ασφάλειας, που είναι αναπτυσσόμενες σήμερα, χωρίς εκτενή συντονισμό, που να μπορούν να εφαρμοστούν σε πολλά περιβάλλοντα και χρήσεις. Προκειμένου να ικανοποιηθούν αυτές οι διαφορετικές ανάγκες, απαιτούνται διάφοροι ευδιάκριτοι μηχανισμοί που θα εφαρμοστούν στο πρωτόκολλο SIP.

Σημειώστε ότι η ασφάλεια SIP που επισημαίνεται δεν έχει καμία σχέση με τηνασφάλεια των πρωτοκόλλων που χρησιμοποιούνται σε συνεργασία μ αυτό, όπως το RTP. Οποιαδήποτε στοιχεία που συνδέονται με μια σύνοδο μπορούν να είναι κρυπτογραφημένα και ανεξάρτητα από οποιαδήποτε σχετική SIP σηματοδοσία.

Οι εκτιμήσεις που ακολουθούν αρχικά εξετάζουν ένα σύνολο κλασικών μοντέλων απειλής που προσδιορίζουν ευρέως τις ανάγκες ασφάλειας SIP. Έπειτα απαριθμούνται οι απαιτήσεις για τις εφαρμογές του SIP, μαζί με τις επεκτάσεις στις οποίες αυτοί οι μηχανισμοί ασφάλειας θα μπορούσαν να χρησιμοποιηθούν για να βελτιώσουν το SIP.

6.2 Επιθέσεις και πρότυπα απειλής

Αυτό το τμήμα απαριθμεί μερικές απειλές που πρέπει να είναι κοινές για τις περισσότερες επεκτάσεις του SIP. Τα ακόλουθα παραδείγματα παρέχουν έναν πλήρη κατάλογο των απειλών ενάντια στο SIP.

Αυτές οι επιθέσεις υποθέτουν ένα περιβάλλον στο οποίο οι επιτιθέμενοι μπορούν ενδεχομένως να διαβάσουν οποιοδήποτε πακέτο στο δίκτυο και αναμένεται ότι το SIP θα χρησιμοποιείται συχνά στο δημόσιο internet. Οι επιτιθέμενοι στο δίκτυο μπορεί να είναι σε θέση να τροποποιούν τα πακέτα, να κλέβουν υπηρεσίες, να κρυφακούν τις συνδιαλέξεις ή να διακόπτουν τις συνόδους.

6.2.1 Υποκλοπή εγγραφής

Ο μηχανισμός εγγραφής SIP επιτρέπει σε έναν user agent για να αυτοπροσδιοριστεί σε έναν registrar, σα μια συσκευή στην οποία βρίσκεται ένας χρήστης. Ο registrar αξιολογεί την ταυτότητα που βρίσκεται μέσα στην κεφαλίδα From ενός REGISTER μηνύματος και καθορίζει εάν αυτό

Το αίτημα μπορεί να τροποποιήσει τις διευθύνσεις των επαφών που συνδέονται με την κεφαλίδα To. Ενώ αυτοί οι δύο τομείς είναι συχνά ίδιοι, υπάρχουν πολλές έγκυρες περιπτώσεις στις οποίες κάποιος τρίτος μπορεί να καταχωρήσει τις επαφές εκ μέρους ενός χρήστη.

Η κεφαλίδα From από ένα SIP request μήνυμα, μπορεί να τροποποιηθεί αυθαίρετα από τον ιδιοκτήτη του UA, και αυτό ανοίγει την πόρτα σε κακόβουλες εγγραφές. Ένας επιτιθέμενος που υποκαθιστά επιτυχώς ένα συμβαλλόμενο μέρος (κανονικό χρήστη) μπορεί για παράδειγμα να μπει στο σύστημα και να διαγράψει όλες τις υπάρχουσες επαφές για ένα URI και στη συνέχεια να καταχωρήσει δικές του συσκευές σαν συμβαλλόμενα μέλη. Έτσι θα μπορεί να κατευθύνει όλα τα request μηνύματα που προορίζονται για το χρήστη, στη συσκευή του επιτιθέμενου.

Αυτή η απειλή ανήκει σε μια οικογένεια απειλών που στηρίζονται στην απουσία κρυπτογράφησης του δημιουργού ενός request. Οποιαδήποτε SIP UAS που αντιπροσωπεύουν μια υπηρεσία μπορεί να θέλουν να αποκτήσουν πρόσβαση ελέγχου στους πόρους του συστήματος με τη βοήθεια των requests αυθεντικοποίησης που λαμβάνουν. Ακόμη, για παράδειγμα και τα SIP τηλέφωνα ενδιαφέρονται για την ταυτότητα των δημιουργών των requests.

Αυτή η απειλή καταδεικνύει την ανάγκη για τις υπηρεσίες ασφάλειας που επιτρέπουν στις SIP οντότητες να επικυρώσει τους δημιουργούς των requests.

6.2.2 Προσωποποιώντας έναν server

Η περιοχή στην οποία ένα αίτημα κατευθύνεται διευκρινίζεται μέσα από το πεδίο Request-URI. Οι UAs συνήθως έρχονται σε επαφή με έναν server στο domain αυτό προκειμένου να πάρουν το request. Εντούτοις, υπάρχει πάντα η πιθανότητα ο επιτιθέμενος να υποκαταστήσει το server και τελικά το request του χρήστη να υποκλαπεί από κάποιο άλλο συμβαλλόμενο μέρος.

Αυτό το είδος των απειλών έχει τις παραπάνω ιδιότητα, πολλές από τις οποίες είναι κρίσιμες. Για το λόγο αυτό η πρόληψη αυτής της απειλής απαιτεί μέσα με τα οποία ένας user agent (UA) μπορεί να επικυρώσει τους κεντρικούς υπολογιστές στους οποίους στέλνουν τα requests.

6.2.3 Αλλαγή των 'κύριων σωμάτων' των μηνυμάτων

Όσον αφορά τα requests των SIP UAs, αυτά δρομολογούνται μέσω proxy servers. Ανεξάρτητα από το πώς καθιερώνεται η εμπιστοσύνη ανάμεσα στους UAs και στους servers, θα πρέπει να υπάρχει για να κατευθύνει το μήνυμα, αλλά αυτό δε σημαίνει ότι πρέπει να υπάρχει και για να ελέγχει τυχόν αλλαγές και τροποποιήσεις στο σώμα των μηνυμάτων.

Ας εξετάσουμε έναν UA που χρησιμοποιεί τα σώματα των SIP μηνυμάτων για να επικοινωνήσει με τη σύνοδο και να ανταλλάξει κλειδιά κρυπτογράφησης για μια συνομιλία. Αν και εμπιστεύεται τον server που έρχεται σε επαφή για να παραδώσει το σήμα, μπορεί να μη θέλει ο administrator του domain να μπορεί να αποκρυπτογραφήσει οποιαδήποτε στοιχείο της συνόδου. Ακόμα χειρότερα, θα μπορούσε ο server να ήταν ήδη κακόβουλος και να τροποποιούσε το κλειδί της συνόδου. Είτε θα μπορούσε να εμφανίζεται σαν κάποιος ενδιάμεσος της συνομιλίας, είτε ακόμα και να αλλάξει τα χαρακτηριστικά ασφαλείας που έχουν ζητηθεί απ τον UA.

Αυτή η οικογένεια των απειλών ισχύει όχι μόνο για τα κλειδιά συνόδου, αλλά για τις μορφές του περιεχομένου του SIP μηνύματος. Αυτό μπορεί να περιλαμβάνει τα σώματα MIME που πρέπει να δοθούν στο χρήστη, τα SDP ή σήματα τηλεφωνίας που περιλαμβάνονται στο αίτημα. Οι εισβολείς μπορεί για παράδειγμα να αλλάξουν το σώμα των SDP, έτσι ώστε να οδηγήσουν το RTP stream σε μια συσκευή υποκλοπής τηλεφωνικών συνδιαλέξεων προκειμένου να κρυφακούσουν τη συνομιλία.

Επίσης πρέπει να σημειώσουμε ότι μερικοί τομείς των SIP μηνυμάτων είναι πολύ σημαντικοί, όπως για παράδειγμα το Subject. Εντούτοις, δεδομένου ότι πολλά τμήματα των μηνυμάτων επιθεωρούνται ή αλλάζουν από τους servers κατά τη διάρκεια της δρομολόγησης του request, υπάρχουν κομμάτια που δε γίνεται να είναι ασφαλή σε όλη τη διαδρομή του request. Για το λόγο αυτό ο user agent θέλει να τα σώματα των μηνυμάτων καθώς και κάποιες κεφαλίδες να είναι ασφαλείς σε όλη τη διαδρομή του αιτήματος. Οι μηχανισμοί ασφαλείας που απαιτούνται για τα σώματα των μηνυμάτων περιλαμβάνουν εμπιστευτικότητα, ακεραιότητα, και επικύρωση. Αυτές οι υπηρεσίες πρέπει να είναι ανεξάρτητες από τα μέσα που χρησιμοποιούνται για να εξασφαλίσουν τις αλληλεπιδράσεις με τους μεσάζοντες όπως είναι οι proxy servers.

6.2.4 Καταστρέφοντας τις συνδιαλέξεις

Μόλις ολοκληρωθεί μια σύνδεση μετά την ανταλλαγή των αρχικών μηνυμάτων, στη συνέχεια μπορεί να σταλούν κι άλλα αιτήματα που τροποποιούν την κατάσταση του διαλόγου ή/και της συνόδου. Είναι πολύ σημαντικό να εξασφαλίσουμε ότι τέτοια μηνύματα δε θα αλλοιωθούν απ τους εισβολείς.

Ας εξετάσουμε μια περίπτωση στην οποία ένας επιτιθέμενος συλλαμβάνει κάποια αρχικά μηνύματα σε έναν διάλογο δύο συμβαλλόμενων μερών, έτσι ώστε να μάθει διάφορες παραμέτρους της συνόδου όπως τα To tag, From tag κ.α. και στη συνέχεια να στείλει ένα μήνυμα BYE στη σύνοδο. Ο επιτιθέμενος θα μπορούσε να κάνει αυτό το μήνυμα να φαίνεται

σα να έχει σταλεί από κάποιον απ τα δύο συμβαλλόμενα μέλη. Έτσι με το που λάβει ο ένας απ τους δύο συμμετέχοντες το BYE, η σύνοδος θα τερματιστεί πρόωρα.

Παρόμοιες απειλές περιλαμβάνουν και τη μετάδοση re-INVITEs που αλλάζουν τη σύνοδο και μειώνουν την ασφάλεια της ή κατευθύνουν το RTP stream σε συσκευές υποκλοπής. Η αποτελεσματικότερη ενέργεια ενάντια σε αυτήν την απειλή είναι η επικύρωση του αποστολέα του BYE. Σε αυτήν την περίπτωση, μόνο μπορούμε να ξέρουμε ότι το BYE προήλθε από το ίδιο συμβαλλόμενο μέρος με το οποίο είχε ολοκληρωθεί νωρίτερα η σύνδεση.

Επίσης, εάν ο επιτιθέμενος δεν έχει τη δυνατότητα να μάθει τα στοιχεία της συνόδου, λόγω εμπιστευτικότητας, τότε δε μπορεί να στείλει κάποιο BYE. Εντούτοις, κάποιοι μεσάζοντες όπως οι proxy servers θα πρέπει να έχουν τη δυνατότητα να επιθεωρούν τις παραμέτρους αυτές, αφού ολοκληρωθεί η πρώτη σύνδεση της συνόδου.

6.2.5 Denial of Service (DoS) και Ενίσχυση

Οι DoS επιθέσεις επικεντρώνονται στο να κάνουν ένα δίκτυο μη διαθέσιμο, συνήθως αυξάνοντας υπερβολικά την κυκλοφορία του δικτύων και των διεπαφών του. Μια διανεμημένη DoS επίθεση επιτρέπει σε έναν χρήστη δικτύων να προκαλέσει συνωστισμό στον κύριο host του δικτύου, με μια υπερβολική αύξηση της κυκλοφορίας.

Οι επιτιθέμενοι μπορούν να δημιουργήσουν ψευδή αιτήματα που περιέχουν ψεύτικη Διεύθυνση IP και κεφαλίδα Via, έτσι ώστε και να στείλουν αυτά τα requests σε ένα μεγάλο αριθμό παραληπτών. Ομοίως, οι επιτιθέμενοι μπορεί να χρησιμοποιούν τα ψεύτικα πεδία των μηνυμάτων σε ένα request που αναγνωρίζει τον κύριο host και μετά θα στείλουν τέτοια μηνύματα σε όλους τους proxy servers.

Η χρήση πολλαπλής διανομής για τη μετάδοση των SIP αιτημάτων μπορεί να αυξήσει τη δυνατότητα για DoS επιθέσεις. Αυτά τα προβλήματα καταδεικνύουν μια γενική ανάγκη να καθοριστούν οι αρχιτεκτονικές που θα ελαχιστοποιούν τους κινδύνους DoS.

6.3 ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ

Από τις απειλές που είδαμε παραπάνω, καταλαβαίνουμε ότι οι θεμελιώδεις υπηρεσίες ασφάλειας που απαιτούνται για το SIP πρωτόκολλο είναι: η συντήρηση της εμπιστευτικότητας και ακεραιότητας του μηνύματος, που αποτρέπουν τις επιθέσεις επανάληψης των μηνυμάτων και την παρεμπόδιση των DoS επιθέσεων. Τα σώματα των SIP μηνυμάτων απαιτούν χωριστά την ασφάλεια των υπηρεσιών εμπιστευτικότητας, ακεραιότητας και επικύρωσης.

Η πλήρης κρυπτογράφηση των μηνυμάτων παρέχει τα καλύτερα μέσα για να συντηρηθεί η ασφάλεια, ωστόσο αυτό δεν είναι δυνατό. Για παράδειγμα, υπάρχουν πεδία μέσα στα μηνύματα όπως τα Request-URI, Route και Via, τα οποία πρέπει να είναι ορατά στους proxies στις περισσότερες αρχιτεκτονικές δικτύων, έτσι ώστε να δρομολογούνται σωστά τα SIP requests. Θα πρέπει ακόμα να σημειώσουμε ότι οι servers πρέπει να τροποποιούν μερικά χαρακτηριστικά γνωρίσματα των μηνυμάτων ώστε να λειτουργήσει σωστά το SIP.

Για το σκοπό αυτό προτείνονται μηχανισμοί ασφάλειας χαμηλού επιπέδου (low-layer security)για το SIP, οι οποίοι επιτρέπουν την κρυπτογράφηση ολόκληρων των SIP requests ή των SIP responses και ακόμη αφήνουν τα endpoints να επιβεβαιώσουν την ταυτότητα των servers, στους οποίους στέλνουν τα requests.

Ένας ανεξάρτητος μηχανισμός ασφάλειας για τα σώματα των SIP μηνυμάτων παρέχει αμοιβαία επικύρωση (authentication), καθώς επίσης και ένα όριο στο βαθμό στον οποίο οι user agents θα πρέπει να εμπιστεύονται τους μεσάζοντες.

6.3.1 HTTP Authentication

Το SIP παρέχει μια ικανότητα, βασισμένη στο HTTP, η οποία στηρίζεται στους 401 και 407 κώδικες απάντησης (401 και 407 response) καθώς επίσης και στα πεδία κεφαλίδας που περιέχουν πιστοποιητικά μεταφοράς. Χωρίς σημαντικές τροποποιήσεις, η επαναχρησιμοποίηση του προτύπου HTTP Digest authentication μέσα στο SIP επιτρέπει την

προστασία επανάληψης (πχ reINVITEs)και τη μονόδρομη επικύρωση (one-way authentication).

6.3.2 Μεταφορά και ασφάλεια δικτύων

Η μεταφορά και ασφάλεια των δικτύων κρυπτογραφεί την κίνηση της σηματοδοσίας και εγγυάται την εμπιστευτικότητα και την ακεραιότητα των μηνυμάτων. Δύο δημοφιλείς εναλλακτικές λύσεις για την παροχή της ασφάλειας στη μεταφορά των πακέτων στο δίκτυο είναι αντίστοιχα το **TLS** και το **IPSec**.

Το **IPSec** είναι ένα πρωτόκολλο που αποτελείται από ένα σύνολο εργαλείων και μπορεί να χρησιμοποιηθεί ως αντικαταστάτης του παραδοσιακού IP πρωτοκόλλου. Το IPSec συνηθέστερα χρησιμοποιείται σε αρχιτεκτονικές όπου οι hosts και τα administrative domains έχουν μια υπάρχουσα σχέση εμπιστοσύνης το ένα με το άλλο. Το πρωτόκολλο αυτό εφαρμόζεται συνήθως σε επίπεδο λειτουργικών συστημάτων ή σε ένα gateway ασφάλειας. Μπορεί επίσης να χρησιμοποιηθεί σε μια hop-by-hop βάση.

Σε πολλές αρχιτεκτονικές δεν απαιτείται η αφομοίωση του IPSec με SIP εφαρμογές. Το IPSec είναι ίσως καταλληλότερο στις επεκτάσεις στις οποίες η προσθήκη της ασφάλειας στους SIP hosts θα ήταν δύσκολη. Επίσης οι user agents που έχουν ήδη μια σχέση με τον proxy server τους είναι καλοί υποψήφιοι για να χρησιμοποιήσουν IPSec.

Το TLS παρέχει ασφάλεια ανεξάρτητα των πρωτοκόλλων σύνδεσης που χρησιμοποιούνται. Μπορεί να διευκρινιστεί ως το πλέον επιθυμητό πρωτόκολλο μεταφορών μέσα στις κεφαλίδες Via και SIP-URI. Το TLS ταιριάζει περισσότερο σε αρχιτεκτονικές στις οποίες οι hosts δεν έχουν προηγούμενη σχέση εμπιστοσύνης.

6.3.3 S/MIME

Όπως αναφέρθηκε και παραπάνω, η κρυπτογράφηση ολόκληρων μηνυμάτων θα ήταν πολύ καλό βήμα για την ασφάλεια των VoIP συστημάτων, αλλά αυτό δεν είναι εφικτό λόγω των proxy servers, οι οποίοι θα πρέπει να βλέπουν και κάποιες φορές να επεξεργάζονται τμήματα των μηνυμάτων έτσι ώστε να τα δρομολογήσουν σωστά. Σε περίπτωση που οι ενδιάμεσοι (proxy servers) δεν υποστηρίζουν ασφάλεια, τότε το SIP μήνυμα θα θεωρείται μη-δρομολογήσιμο.

Εντούτοις, το S/MIME επιτρέπει στους user agents του SIP να κρυπτογραφήσουν τα σώματα των MIME, εξασφαλίζοντας ασφάλεια χωρίς να επηρεάζονται οι κεφαλίδες του μηνύματος. Είναι επίσης πιθανό να χρησιμοποιηθεί το S/MIME για να παρέχει μια μορφή ακεραιότητας και εμπιστευτικότητα για τις κεφαλίδες του μηνύματος SIP μέσω του message tunneling.

6.3.4 SIPS URI Scheme

Το SIPS URI μπορεί να χρησιμοποιηθεί ως διεύθυνση για έναν συγκεκριμένο χρήστη - το URI από το οποίο ο χρήστης έχει γίνει κανονικά γνωστός. Όταν χρησιμοποιείται ως Request-URI του μηνύματος, το πρότυπο SIP δηλώνει ότι κάθε βήμα πάνω από τον οποίο διαβιβάζεται το αίτημα, μέχρι να φθάσει το αίτημα στην αρμόδια SIP οντότητα, πρέπει να είναι εξασφαλισμένο με TLS. Όταν χρησιμοποιείται από το δημιουργό ενός αιτήματος, το SIPS υπαγορεύει ότι ολόκληρη η πορεία του αιτήματος εξασφαλίζεται από άποψη ασφάλειας.

Εδώ θα πρέπει να σημειώσουμε ότι στο SIPS URI scheme, η μεταφορά είναι ανεξάρτητη από TLS, και γι αυτό τα "sips:alice@atlanta.com;transport=tcp" και "sips:alice@atlanta.com;transport=sctp" είναι εξίσου έγκυρα. (το UDP δεν είναι έγκυρη μεταφορά για το SIPS). Η χρήση "transport=tls" έχει εξαληφθεί εν μέρει επειδή είναι συγκεκριμένο για ένα μόνο βήμα του αιτήματος.

6.4 Λύσεις ασφάλειας

Οι λειτουργίες αυτών των μηχανισμών ασφάλειας μπορούν να ακολουθήσουν τα υπάρχοντα μοντέλα ασφάλειας που ισχύουν στο internet και στο email μέχρι κάποιο βαθμό.

Σε ένα υψηλό επίπεδο, οι UAs επικυρώνουν τους εαυτούς τους στους servers με ένα όνομα χρήστη και έναν κωδικό πρόσβασης. οι servers επικυρώνονται στους UAs που βρίσκονται ένα βήμα μακριά ή σε άλλους servers, με τη βοήθεια ενός πιστοποιητικού που παραδίδεται από το TLS.

Σε ένα peer-to-peer επίπεδο, οι UAs εμπιστεύονται το δίκτυο για να επικυρώσουν ο ένας τον άλλο, όμως το S/MIME μπορεί επίσης να χρησιμοποιηθεί για να δώσει άμεση επικύρωση όταν το δίκτυο δε δίνει, ή εάν το δίκτυο δεν υποστηρίζει ασφάλεια.

6.5 Ιδιωτικότητα

Τα μηνύματα SIP περιέχουν συχνά τις ευαίσθητες πληροφορίες για τους αποστολείς τους – και όχι μόνο το τι έχουν να πουν, αλλά και με το ποιους επικοινωνούν, όταν επικοινωνούν και για ποιο χρονικό διάστημα, και που βρίσκονται όταν συμμετέχουν στις συνόδους.

Πολλές εφαρμογές, καθώς και οι χρήστες τους, απαιτούν ότι αυτό το είδος των ιδιωτικών πληροφοριών θα πρέπει να αποκρύπτεται από κάθε συμβαλλόμενο μέλος που δε χρειάζεται να ξέρει.

Υπάρχουν επίσης λιγότερο άμεσοι τρόποι με τους οποίους μπορούν να αποκαλυφθούν οι ιδιωτικές πληροφορίες. Εάν ένας χρήστης ή μια υπηρεσία επιλέξει να μπορούν να τη βρουν σε μια διεύθυνση που από το όνομα της εικάζεται ότι μπορεί να ανήκει σ΄ αυτόν , τότε συμβιβάζεται η παραδοσιακή μέθοδος μυστικότητας που εξασφαλίζει την ασφάλεια, έχοντας έναν μη καταχωρημένο "τηλεφωνικός αριθμό". Μια εφαρμογή θα πρέπει να είναι σε θέση να περιορίσει, σε μια per-user βάση, τι είδους θέση και τι είδους πληροφορίες διαθεσιμότητας δίνονται στις διάφορες κατηγορίες χρηστών που επικοινωνεί.

Σε μερικές περιπτώσεις, οι χρήστες μπορεί να θελήσουν να κρύψουν τις προσωπικές τους πληροφορίες που περιέχονται στις κεφαλίδες των μηνυμάτων και μεταβιβάζουν την ταυτότητά τους. Αυτό μπορεί να ισχύσει όχι μόνο για την κεφαλίδα From, που αντιπροσωπεύει το δημιουργό του αιτήματος, αλλά και για την To. Μπορεί να μην είναι σωστό να μεταβιβαστεί στον τελικό προορισμό πχ. ένα όνομα ταχείας κλήσης ή ένα προσδιοριστικό για μια ομάδα στόχων, καθένα απ΄ τα οποία θα αφαιρούνταν από το Request-URI κατά τη διάρκεια της δρομολόγησης του αιτήματος, αλλά δε θα άλλαζε στην κεφαλίδα To αν αυτά τα δύο ήταν αρχικά τα ίδια. Κατά συνέπεια μπορεί για λόγους μυστικότητας να είναι επιθυμητή η δημιουργία μιας κεφαλίδας To που να διαφέρει από το πεδίο Request-URI.

ΚΕΦΑΛΑΙΟ 7

ΑΣΦΑΛΕΙΑ VOIP

Η ασφάλεια των υποδομών VoIP αποτελεί μια από τις σημαντικότερες προκλήσεις και για τις λειτουργικές και για τις ερευνητικές κοινότητες, επειδή η ασφάλεια δεν ήταν βασικό συστατικό στις αρχικές φάσεις έρευνας και ανάπτυξης του πρωτοκόλλου VoIP. Η αγορά απαιτεί αυτήν την περίοδο λύσεις ασφάλειας για αμιγώς VoIP συστήματα ενώ η έρευνα και η προτυποποίηση προσπαθούν ακόμα σκληρά να αντιμετωπίσουν τα ζητήματα αυτά.

Τα τελευταία χρόνια, προέκυψαν διάφορες προσεγγίσεις, αλλά οι περισσότερες από αυτές εξετάζουν μόνο την υπεράσπιση του συστήματος ενάντια σε ένα υποσύνολο των πιθανών παραγόντων επίθεσης και όχι σε όλο το σύνολό τους.

Η προσέγγιση που θα δώσουμε είναι βασισμένη σε ένα συνδυασμό μιας αμιγώς VoIP παγίδας και σε ένα σχέδιο ελέγχου εφαρμογών, βασισμένο στο SIP. Μια τέτοια προσέγγιση είναι ικανή εντοπίζει τους διάφορους τύπους επιθέσεων:

Η VoIPspecific παγίδα είναι καταλληλότερη για την παρεμπόδιση των κοινωνικών επιθέσεων όπως Spam πάνω από την τηλεφωνία μέσω internet (SPIT) και των VoIP Phishing, καθώς επίσης και άλλων ενεργειών αναγνώρισης. Ενώ η SIP προσέγγιση προσαρμόζεται για να ανιχνεύσει ψευδή χρήση και Denial of Service.

7.1 VOIP ΑΠΕΙΛΕΣ ΚΑΙ ΠΡΟΒΛΗΜΑΤΑ

Οι απειλές της VoIP ασφάλειας είναι παρόμοιες μ αυτές που αντιμετωπίζουν τα δίκτυα δεδομένων. Η κύρια πηγή απειλών έρχεται από το γεγονός ότι και η σηματοδότηση και ο έλεγχος του VoIP μεταφέρεται πάνω απ το δίκτυο IP. Επομένως, η υποδομή VoIP έχει τις ίδιες ευαισθησίες με τα δίκτυα δεδομένων. Ανάμεσα στις πιο επικίνδυνες VoIPspecific επιθέσεις έχουν μπει η κλοπή ταυτότητας, η παράνομη χρήση και οι κοινωνικές επιθέσεις.

Οι επιθέσεις DoS μπορούν να στραφούν ενάντια στην υποδομή VoIP (servers, proxies, agents) και να οδηγήσουν στον ακρωτηριασμό και στο συνολικό κλείσιμο μιας υποδομής VoIP. Ioi, worms και backdoors μπορούν να επιτρέψουν τον έλεγχο των τηλεφώνων IP και των VoIP proxies έχοντας κάτι παραπάνω από έναν απλό κακόβουλο σκοπό.

Επιπλέον, με τη VoIP τεχνολογία που αναπτύσσεται πολύ γρήγορα, οι hackers δείχνουν να ενδιαφέρονται να εξαπλωθούν και να ωφεληθούν από αυτή την αγορά. Ο σχεδιασμός μιας λύσης ασφάλειας για τη VoIP τεχνολογία είναι πλέον πρωταρχικός στόχος.

Οι προκλήσεις ασφαλείας που αντιμετωπίζει το VoIP είναι απειλές από πρωτόκολλα διαφορετικών τομέων-για παράδειγμα, επιθέσεις SIP σηματοδοσίας, επιθέσεις RTP μέσων, και επιθέσεις IP τομέα. Οι VoIP προκλήσεις ασφάλειας είναι DoS επιθέσεις, απειλές από ανοιχτή IP υποδομή, και επιθέσεις SIP σηματοδοσίας και ροής μέσων. Αυτές οι απειλές συνοψίζονται παρακάτω:

7.1.1 Απειλές παρεμπόδισης και τροποποίησης

Σε αντίθεση με τις δυσκολίες που συναντιούνται στην παράνομη παρακολούθηση στο πρωτόκολλο PSTN, σε ένα VoIP σύστημα είναι πιθανό να αντιμετωπιστεί χρησιμοποιώντας ροή πακέτων που να μπορεί να καταγραφεί και να αποκωδικοποιηθεί. Ελεύθερο λογισμικό όπως το Vomit1 (Voice over misconfigured internet telephones) υπάρχει ήδη για επιθέσεις σε επιχειρήσεις και είναι και κατάλληλο και για Cisco IP τηλέφωνα.

Παρόμοια εργαλεία έχουν προκύψει και για το SIP και δεν παρουσιάζουν σημαντικές τεχνολογικές δυσκολίες. Ο επιτιθέμενος έχει τη δυνατότητα να μολύνει, να κρυφακούσει ή και να κλέψει ευαίσθητες οικονομικές και εμπορικές πληροφορίες.

7.1.2 Denial of Service και απάτες

Πολλές επιθέσεις στοχεύουν στη σηματοδοσία των δικτύων (π.χ. proxy, gateway κ.λπ.) με σκοπό να προκαλέσουν όλεθρο στο δίκτυο VoIP. Αυτό είναι πολύ εύκολο να επιτευχθεί πλημμυρίζοντας το δίκτυο με μια μεγάλη ποσότητα μηνυμάτων, κακώς δομημένων

μηνυμάτων ή ακόμα και συσκευές που έχουν στόχο να προσβάλλουν συγκεκριμένες ευαισθησίες του συστήματος.

Αυτό παρεμβάλει ραδιοσήματα και πλημμύρες αιτημάτων πιστοποίησης στο PCSCF και άλλες συσκευές. Για παράδειγμα, σε μία REGISTER επίθεση πλημμύρας, ο επιτιθέμενος στέλνει πολλά REGISTER αιτήματα στο P-CSCF με ψεύτικες ή παραπλανητικές διευθύνσεις πηγών (π.χ. SIP URI). Στην περίπτωση διανεμημένης REGISTER πλημμύρας, ο επιτιθέμενος παράγει πολλαπλά REGISTER αιτήματα με διαφορετικές ή παραπλανητικές διευθύνσεις πηγών ώστε να κατακλύσει τους VoIP πόρους. Προκαλεί πτώση των VoIP πόρων και οι νόμιμοι χρήστες δεν μπορούν να λάβουν τις υπηρεσίες.

7.1.3 Κοινωνικές απειλές

Οι κοινωνικές απειλές είναι επιθέσεις που κυμαίνονται από την παραγωγή ενοχλητικών επικοινωνιών για τους χρήστες, μέχρι πιο επικίνδυνες κλοπές δεδομένων. Η απειλή χαρακτηρίζεται ως κοινωνική, αφού είναι αυστηρά συνδεδεμένη με τις προτιμήσεις ειδικά των χρηστών, και αυτό το κάνει πολύ δύσκολο για το σύστημα να αναγνωρίσει το είδος της επίθεσης. Ένα παράδειγμα αυτού είναι μια απειλή που αναφέρεται συνήθως σαν Spam πάνω από την τηλεφωνία μέσω internet και είναι παρόμοια με το Spam στα συστήματα ηλεκτρονικού ταχυδρομείου, αλλά παραδίδεται με τη μορφή τηλεφωνικής κλήσης.

Αυτού του είδους η απειλή αναπτύχθηκε λόγω του φτηνού κόστους που έχει το VoIP αυτή την περίοδο. Υπολογίζεται ότι οι κλήσεις VoIP είναι σε μέγεθος τρεις φορές φτηνότερες από ότι είναι οι κλήσεις του PSTN δικτύου. Οι κλήσεις SPIT μπορεί να είναι κλήσεις που χρησιμοποιούνται για την προώθηση προϊόντων, ή κλήσεις που σε καθοδηγούν να καλέσεις υπηρεσίες με μεγάλη χρέωση. Μια άλλη παραλλαγή των κλήσεων SPIT είναι αυτές που έχουν στόχο να συλλέξουν τα προσωπικά στοιχεία του χρήστη, αποπροσανατολίζοντάς τους χρησιμοποιώντας έναν διαδραστικό αποκριτή φωνής (Interactive Voice Responder) που δίνει την εντύπωση ότι μπορεί να τον εμπιστευθεί ο χρήστης.

Οι περισσότερες από αυτές τις επιθέσεις πρόκειται να παραχθούν από μηχανές προγραμματισμένες για να κάνουν αυτή τη δουλειά. Επικοινωνίες όπως το SPIT είναι τεχνικά σωστές συναλλαγές, από άποψη σηματοδότησης των κλήσεων. Αυτό έχει σαν αποτέλεσμα το SIP να μη μπορεί να διακρίνει από το INVITE που δέχεται, αν αυτό είναι κακόβουλο spam ή όχι. Η πρόκληση είναι ακόμα πιο περίπλοκη δεδομένου ότι το spam περιεχόμενο δεν είναι διαθέσιμο για να ανιχνευθεί παρά μόνο όταν το τηλέφωνο χτυπήσει, ενοχλήσει τον χρήστη και αυτός απαντήσει την κλήση. Έτσι τεχνικές παρόμοιες με το φιλτράρισμα του ηλεκτρονικού ταχυδρομείου είναι σχεδόν βέβαιο ότι δε μπορούν να χρησιμοποιηθούν σ αυτή την περίπτωση. Ακόμα κι αν μια συναλλαγή χαρακτηριστεί σα spam, ο χειρισμός της εξαρτάται έντονα από το νομικό πλαίσιο της κάθε χώρας.

7.1.4 Λοιπές απειλές

- Επίθεση Παραπλάνησης (Spoofing attack)

Ο κακόβουλος κόμβος κρύβει την παρουσία του στο δίκτυο και υποκλέπτει κίνηση, και οι επιτιθέμενοι πλαστογραφούν μηνύματα. Αυτοί οι κόμβοι γίνονται εμπιστευτικοί κόμβοι μέσα στο VoIP δίκτυο.

- Man-in-the-middle attack

Οι hackers ερευνούν τις ρωγμές ασφαλείας και διακόπτουν την διαδικασία πιστοποίησης και προστασίας ακεραιότητας έτσι ώστε να λάβουν VoIP υπηρεσίες δωρεάν.

- Impersonation:

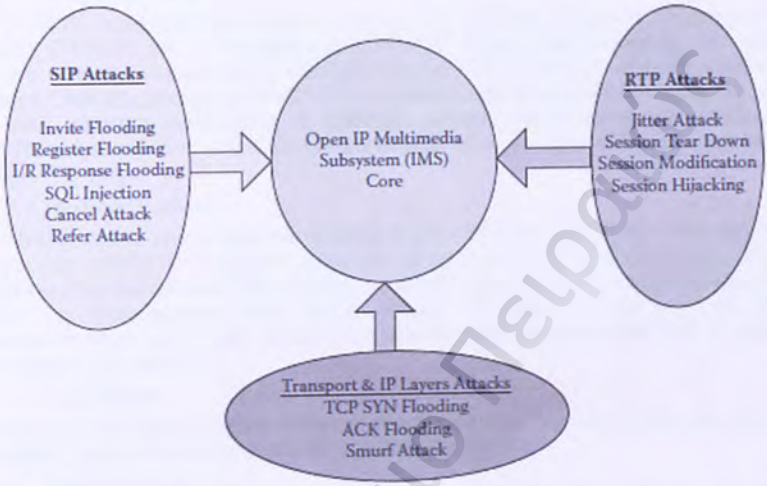
Η απομίμηση ενός εξυπηρετητή προκαλεί λάθος δρομολόγηση των μηνυμάτων. Οι υπάρχουσες διαδικασίες δρομολόγησης είναι ανήμπορες να διακρίνουν μεταξύ του εισβολέα και του νόμιμου χρήστη. Με αυτόν τον τρόπο ο επιτιθέμενος έχει ελεύθερη πρόσβαση στις VoIP υπηρεσίες και το θύμα χρεώνεται για τη χρήση των υπηρεσιών που κάνει ο εισβολέας.

- Eavesdropping:

Οι hackers λαμβάνουν πληροφορίες συνόδου αν τα μηνύματα στέλνονται με καθαρή μορφή κειμένου. Έτσι μπορούν εύκολα να εισάγουν μία ποικιλία πειρατικών επιθέσεων από τις πληροφορίες συνόδου.

- Password guessing attack:

Αυτό μοιάζει με πειρατική επίθεση συνόδου με στόχο να ληφθούν πληροφορίες για το χρήστη. Ακόμα και αν ένας εισβολέας δεν μπορεί να διακόψει την VoIP διαδικασία πιστοποίησης, μπορεί να εισάγει μία επίθεση password guessing έτσι ώστε να κάνει κακή χρήση των νόμιμων λογαριασμών των χρηστών. Ο εισβολέας εισάγει αυτήν την επίθεση στέλνοντας πολλά REGISTER αιτήματα στο P-CSCF και λαμβάνει 401-μη πιστοποιημένα μηνύματα από τον πυρήνα του VoIP. Ο επιτιθέμενος μπορεί να λάβει 200 OK αποκρίσεις σε μία επιτυχής επίθεση.



Εικόνα 24: επιθέσεις

- SQL injection:

Αυτός είναι τύπος της επίθεσης πλαστογράφησης μηνυμάτων. Η βασισμένη σε κείμενο φύση των SIP μηνυμάτων παρέχει μία ευκαιρία για επιθέσεις πλαστογράφησης μηνυμάτων στο VoIP.

Αυτή η επίθεση δεν στοχεύει μόνο στην τροποποίηση δεδομένων αλλά επίσης προκαλεί DoS με κατάρρευση των υπηρεσιών βάσεων δεδομένων. Η χρησιμοποίηση μίας διεπαφής ιστού για την παροχή υπηρεσιών προστιθέμενης αξίας κάνει το VoIP πιο ευαίσθητο σε αυτό το είδος επίθεσης.

Η SQL έγχυση μπορεί να πραγματοποιηθεί εύκολα εισάγοντας μία SQL δήλωση όταν ο UA και ο P-CSCF αρχίσουν τις διαδικασίες πιστοποίησης. Το αρχικό REGISTER αίτημα του UA χρησιμοποιεί την HTTP συνοπτική επικεφαλίδα πιστοποίησης για να μεταφέρει τις ταυτότητες των χρηστών. Όταν ένας κακόβουλος χρήστης προσπαθεί να πραγματοποιήσει μία SQL έγχυση στο IMS, παραπλανεί το SIP μήνυμα και εισάγει τον κακόβουλο SQL κώδικα στην επικεφαλίδα πιστοποίησης. Όταν ο P-CSCF λαμβάνει ένα SIP μήνυμα με μία μολυσμένη επικεφαλίδα πιστοποίησης, παράγει και εκτελεί τη παράνομη SQL δήλωση, η οποία μπορεί να διαγράψει δεδομένα στη βάση δεδομένων. Οι υπάρχουσες λύσεις δεν παρέχουν μετριασμό αυτής της επίθεσης. Το IMS επίσης ενοποιεί το HTTP servlet container και γι' αυτό ένας επιτιθέμενος μπορεί επίσης να χρησιμοποιήσει το HTTP μήνυμα για να πραγματοποιήσει τις επιθέσεις SQL έγχυσης.

- Επίθεση τερματισμού συνόδου μέσων

Το BYE αίτημα χρησιμοποιείται για να τερματίσει μία εγκαθιδρυμένη σύνοδο. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει το BYE αίτημα για να διαλύσει μία σύνοδο. Ο επιτιθέμενος στέλνει

ένα ψεύτικο BYE μήνυμα, το οποίο προωθείται από το P-CSCF στο UA1 και υποθέτει πως αυτό είναι από το UA2, ο οποίος θέλει να διαλύσει την σύνδεση στέλνοντας το BYE μήνυμα. Σαν αποτέλεσμα, ο UA1 σταματάει την RTP ροή αμέσως, ενώ ο UA2 συνεχίζει να στέλνει RTP πακέτα στον UA1 επειδή ο UA2 δεν έχει καταλάβει ότι η σύνδεση πρέπει να έχει τερματιστεί. Για να πραγματοποιήσει αυτού του είδους την επίθεση, ο επιτιθέμενος χρειάζεται να μάθει όλες τις απαραίτητες παραμέτρους συνόδου. Αυτό μπορεί να επιτευχθεί είτε ψάχνοντας στο δίκτυο είτε εκτελώντας μία επίθεση τερματισμού συνόδου μέσων για να εισάγει ένα BYE αίτημα στην σύνοδο.

- CANCEL Attack:

Το CANCEL τερματίζει ένα εκκρεμές αίτημα. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τη μέθοδο CANCEL για να ακυρώσει ένα INVITE αίτημα που παράγεται από έναν νόμιμο χρήστη. Πριν η τελική απόκριση παραχθεί για ένα INVITE αίτημα, ο επιτιθέμενος στέλνει ένα ψεύτικο CANCEL μήνυμα στο P-CSCF, το οποίο υποθέτει ότι είναι από έναν νόμιμο χρήστη. Το VoIP σύστημα αναγνωρίζει το CANCEL μήνυμα και διακόπτει την επεξεργασία του INVITE αιτήματος. Ένα CANCEL αίτημα μπορεί μόνο να χρησιμοποιηθεί για να ακυρώσει ένα INVITE αίτημα.

- Re-INVITE attack:

Το INVITE αίτημα εγκαθιδρύει μία σύνοδο ή έναν διάλογο μεταξύ δύο user agents (UA). Ο στόχος του reINVITE μηνύματος είναι για να τροποποιήσει τις πραγματικές πληροφορίες συνόδου. Για παράδειγμα, αλλάζοντας τις διευθύνσεις ή θύρες, προσθέτοντας ένα ρεύμα μέσων, ή διαγράφοντας ένα ρεύμα μέσων. Γι' αυτό, ο επιτιθέμενος μπορεί να πραγματοποιήσει μία DoS επίθεση στέλνοντας ένα πλαστό reINVITE μήνυμα για να τροποποιήσει τη σύνοδο.

- Repudiation:

Ο χρήστης ή το δίκτυο αρνείται ενέργειες που έχουν γίνει. Μη αποκήρυξη είναι μία υπηρεσία ασφαλείας που υπολογίζει τις απειλές της αποκήρυξης.

- Masquerading:

Ένας εισβολέας παρουσιάζεται ως ένας πιστοποιημένος χρήστης για να πάρει απόρρητες πληροφορίες και να λάβει υπηρεσίες του συστήματος.

- IP multimedia services identity module (ISIM) cloning:

Αυτή η διαδικασία αλλάζει την ταυτότητα μιας οντότητας σε μια οντότητα ίδιου τύπου. Το ISIM μπορεί να κλωνοποιηθεί αφαιρώντας το μυστικό κλειδί (K) και το international mobile subscriber identity (IMSI) από ένα ISIM και αλλάζοντάς το σε ένα άλλο ISIM χρησιμοποιώντας διαφορετικές τεχνικές επίθεσης.

7.2 ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΣΥΣΧΕΤΙΣΕΙΣ ΑΣΦΑΛΕΙΑΣ VoIP

Ο στόχος των VoIP λύσεων ασφαλείας είναι η ανάπτυξη ενός πλαισίου εργασίας VoIP ασφάλειας για να βεβαιώνει το απόρρητο του χρήστη και τη προστασία του δικτύου εναντίον κακών χρήσεων.

7.2.1 Μηχανισμοί ασφάλειας VoIP

Σημαντικά χαρακτηριστικά ασφαλείας και υπηρεσίες ασφαλείας παρέχονται από τις παρακάτω λύσεις:

- User confidentiality:

Παρέχει απόρρητη ταυτότητα χρήστη, απόρρητη τοποθεσία χρήστη, και ιχνηλασιμότητα χρήστη. Για να πετύχει αυτά τα χαρακτηριστικά, ανατίθεται στον χρήστη μία προσωρινή ταυτότητα έτσι ώστε η μόνιμη ταυτότητα χρήστη στην οποία οι υπηρεσίες παραδίδονται να μη μπορεί να υποκλαπεί μέσω της ραδιοσύνδεσης πρόσβασης.

- Entity authentication:

Βασίζεται στην πιστοποίηση χρήστη και δικτύου και πρέπει να εφαρμόζεται στην εγκαθίδρυση σύνδεσης μεταξύ του χρήστη και του δικτύου. Περιλαμβάνει έναν μηχανισμό πιστοποίησης χρησιμοποιώντας ένα διάνυσμα πιστοποίησης που παραδίδεται από το

περιβάλλον του χρήστη (Home Environment, HE) στο δίκτυο που υπηρετεί έναν τοπικός μηχανισμό, χρησιμοποιώντας την εγκαθίδρυση του κλειδιού ακεραιότητας μεταξύ του χρήστη και του υπηρετούμενου δικτύου.

- Data confidentiality:

Παρέχει εμπιστευτικότητα των δεδομένων του χρήστη και των δεδομένων σηματοδοσίας. Πραγματοποιείται με τη χρήση κρυπτογραφικών αλγορίθμων και συμφωνία κλειδιού.

- Data integrity:

Παρέχει ακεραιότητα δεδομένων και πιστοποίηση προέλευσης των δεδομένων σηματοδοσίας. Η ακεραιότητα δεδομένων πραγματοποιείται με αλγόριθμους ακεραιότητας και συμφωνία κλειδιού ακεραιότητας.

- Network and services availability:

Καθιστά σίγουρο ότι οι πόροι και υπηρεσίες δικτύου είναι διαθέσιμα όλη την ώρα στους χρήστες. Για να εξασφαλίσει τη διαθεσιμότητα των υπηρεσιών και πόρων, το δίκτυο πρέπει να προστατεύεται από τις DoS επιθέσεις.

- Fraud Control:

Προστατεύει τα πολύτιμα περιουσιακά στοιχεία και υπηρεσίες προστιθέμενης αξίας από παράνομους χρήστες και hackers. Στο VoIP, αυτές οι υπηρεσίες μπορούν να προστατευτούν από AS ασφαλείας. Η 3GPP και 3GPP2 έχουν προτυποποιήσει την VoIP ασφάλεια σε διαφορετικές εκδόσεις. Η ασφάλεια αυτή βασίζεται στην πρώιμη IMS ασφάλεια (early IMS security) και ολοκληρωμένη IMS ασφάλεια (complete IMS security). .

IMS Ασφάλεια (IP Multimedia Subsystem)

Η πρώιμη λύση IMS ασφάλειας που προτυποποιήθηκε στην 3GGP, release 5, παρέχει περιορισμένη λειτουργικότητα ασφαλείας και σκοπεύει να προστατεύει την πρώιμη ανάπτυξη IMS ασφαλείας. Παρέχει πιστοποίηση των συνδρομητών για πρόσβαση υπηρεσιών και εμπιστευτικότητα στην ραδιοδιεπαφή, καθώς επίσης και κρυπτογράφηση.

Η ολοκληρωμένη λύση IMS ασφαλείας προτυποποιήθηκε στην 3GPP, release 6, με πλήρη λειτουργικότητα ασφαλείας. Προσφέρει καινούργια χαρακτηριστικά ασφαλείας , βελτιώνει τα υπάρχοντα και ασφαλίζει καινούργιες υπηρεσίες ώστε να προστατεύσει δίκτυα και τερματικά με προστασία δεδομένων. Αποτελείται από ασφάλεια δικτυακού τομέα και πρόσβασης που ορίζει την SIP ασφάλεια με hop-by-hop τρόπο. Η end-to-end ασφάλεια δεν υποστηρίζεται.

7.2.2 Συσχετίσεις ασφάλειας VoIP

Η συνολική ασφάλεια για τα VoIP συστήματα αποτελείται από μηχανισμούς όπως την πιστοποίηση και συμφωνία κλειδιού μεταξύ ενός VoIP συνδρομητή και του δικτύου, τη συμφωνία μηχανισμού ασφαλείας μεταξύ του VoIP πελάτη και του δικτύου επίσκεψης, την προστασία ακεραιότητας και εμπιστευτικότητας, την ασφάλεια δικτυακού τομέα μεταξύ διαφορετικών επικρατειών και την υπάρχουσα ασφάλεια GPRS/UMTS πρόσβασης.

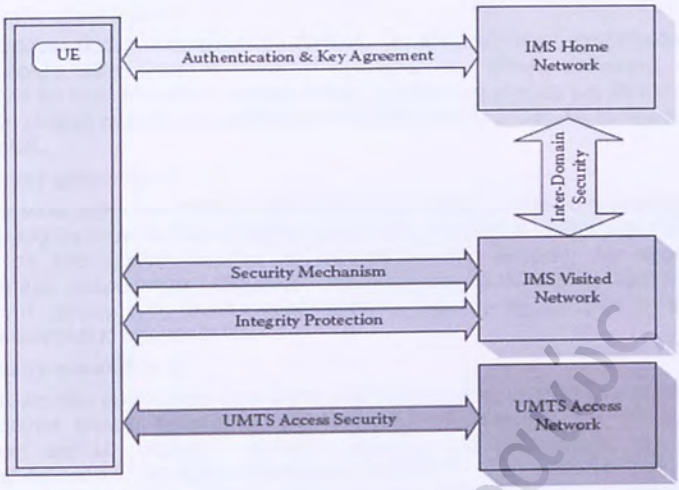
Οι VoIP μηχανισμοί ασφαλείας πραγματοποιούνται από τις παρακάτω συσχετίσεις:

- Security association 1

Παρέχει αμοιβαία πιστοποίηση χρήστη και δικτύου. Το HSS είναι υπεύθυνο για τη παραγωγή κλειδιών και στη συνέχεια αναθέτει τη πιστοποίηση του χρήστη στο S-CSCF.

- Security association 2

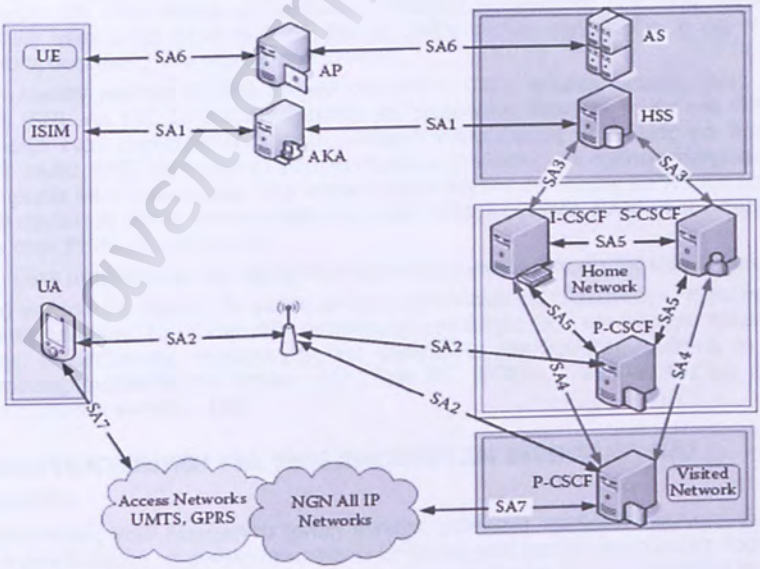
Παρέχει μία ασφαλισμένη σύνδεση και μία συσχέτιση ασφαλείας μεταξύ του UE και του P-CSCF για τη προστασία του Gm σημείου αναφοράς. Στο VoIP, η ασφάλεια του δικτυακού τομέα χρησιμοποιείται για τη προστασία της SIP σηματοδοσίας, αλλά η SIP επικοινωνία στην Gm διεπαφή μεταξύ του UE και του P-CSCF είναι έξω από το πλαίσιο του NDS/IP και χρειάζεται επιπρόσθετα μέτρα ασφαλείας.



Εικόνα 25: Security associations

- Security association 3

Παρέχει ασφάλεια μέσα στο δικτυακό τομέα εσωτερικά για την Cx διεπαφή. Το HSS αποθηκεύει μόνιμα τα δεδομένα συνδρομητών και υπηρεσιών. Αυτά τα κεντρικά δεδομένα χρησιμοποιούνται από το I-CSCF και S-CSCF όταν ο χρήστης εγγράφεται ή λαμβάνει συνόδους μέσω της Cx διεπαφής και το επιλεγόμενο πρωτόκολλο είναι το DIAMETER. Τα DIAMETER μηνύματα πάνω από τις Cx και Dx διεπαφές χρησιμοποιούν το πρωτόκολλο SCTP (Stream Control Transmission Protocol) με IPsec (IP security) για ασφαλή επικοινωνία.



Εικόνα 26: Security associations

- Security association 4

Παρέχει ασφάλεια μεταξύ διαφορετικών δικτύων για κόμβους που υποστηρίζουν SIP και είναι εφαρμόσιμο μόνο όταν το P-CSCF βρίσκεται στο δίκτυο επίσκεψης. Αυτό που συμβαίνει είναι ότι παρ' όλο που η πιστοποίηση χρειάζεται να γίνει σε ένα δίκτυο επίσκεψης, συγκεκριμένη ευθύνη πρέπει να ανατεθεί στο P-CSCF διότι το IPSec SA υπάρχει μεταξύ του P-CSCF και UE.

- Security association 5

Παρέχει ασφάλεια μέσα στο δίκτυο εσωτερικά μεταξύ κόμβων που υποστηρίζουν SIP και επίσης εφαρμόζεται όταν το PCSCF βρίσκεται στο ίδιο δίκτυο. Το VoIP προστατεύει όλη την IP κίνηση σε ένα δίκτυο πυρήνα με τη χρήση του NDS/IP, το οποίο παρέχει εμπιστευτικότητα, ακεραιότητα δεδομένων, πιστοποίηση και antireplay προστασία για τη κίνηση, με τη χρήση ενός συνδυασμού κρυπτογραφικών μηχανισμών ασφαλείας και μηχανισμών ασφαλείας πρωτοκόλλου.

- Security association 6

Τα πρωτόκολλα που δουλεύουν κατά μήκος της Ut διεπαφής εκτελούν λειτουργικότητα για να διαχειρίζονται κίνηση δεδομένων για εφαρμογές βασισμένες στο HTTP. Γι' αυτό, ασφαλίζοντας μία Ut διεπαφή σημαίνει επιτυχής εμπιστευτικότητα και προστασία ακεραιότητας δεδομένων για κίνηση βασισμένη στο HTTP. Η πιστοποίηση και η συμφωνία κλειδιού για την Ut διεπαφή βασίζονται επίσης στο AKA, το οποίο παράγει κλειδιά συνόδου.

Το VoIP ορίζει γενικά bootstrapping αρχιτεκτονική (Generic Boostrapping Architecture, GBA), η οποία χρησιμοποιεί αρχιτεκτονική πιστοποίησης (Generic Authentication Architecture, GAA) η οποία πραγματοποιεί αμοιβαία πιστοποίηση πριν τη πρόσβαση στις υπηρεσίες. Η πιστοποίηση στην Ut διεπαφή πραγματοποιείται από τον proxy πιστοποίησης (authentication proxy). Η κίνηση στην Ut διεπαφή περνάει από τον proxy server αυτόν και ασφαλίζεται χρησιμοποιώντας το boostrapped κλειδί συνόδου. Η Ut διεπαφή χρησιμοποιεί την ασφάλεια επιπέδου μεταφοράς (Transport Layer Security, TLS) για εμπιστευτικότητα και για προστασία ακεραιότητας.

- Security association 7

Καταφέρνει να προστατεύσει τον χρήστη και τις πληροφορίες χρήστη στα δίκτυα πρόσβασης (π.χ. UMTS, GSM, GPRS, WLAN, DSL και VoIP). Η συσχέτιση ασφαλείας πραγματοποιείται ανεξάρτητα είτε στον τομέα υπηρεσιών μεταγωγής κυκλώματος (CS) είτε στον τομέα υπηρεσιών μεταγωγής πακέτου (PS). Για τα UMTS δίκτυα πρόσβασης, η αρχιτεκτονική διαχείρισης ασφαλείας αποτελείται από το user

Service identity module (USIM), mobile equipment (ME), access network (AN), service network (SN), και HE. Το USIM απαιτείται για πρόσβαση στον PS τομέα στο GPRS και αναγνωρίζει έναν συγκεκριμένο χρήστη. Περιέχει παραμέτρους ασφαλείας για πρόσβαση στον PS τομέα, IMSI, λίστα από επιτρεπτά σημεία πρόσβασης, και σχετικές πληροφορίες με την υπηρεσία MMS μηνυμάτων. Στο υπηρετούμενο δίκτυο, το serving GPRS support node (SGSN) συνδέει το δίκτυο ραδιοπρόσβασης (radio access network, RAN) με τον πυρήνα του δικτύου στον PS τομέα υπηρεσιών.

Είναι υπεύθυνο για την πραγματοποίηση λειτουργιών διαχείρισης ελέγχου και κίνησης για τον PS τομέα. Το μέρος ελέγχου ασχολείται με διαχείριση κινητικότητας και διαχείριση συνόδων. Το SGSN επίσης βεβαιώνει κατάλληλο QoS και παράγει πληροφορίες χρέωσης. Η διαδικασία πιστοποίησης και συμφωνίας κλειδιού περιλαμβάνει το κέντρο πιστοποίησης (authentication center, AUC) στο HE, SGSN, ή VLR καθώς και κινητούς σταθμούς (mobile stations - MS).

7.3 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΓΙΑ ΤΗΝ ΑΝΙΧΝΕΥΣΗ ΕΙΣΒΟΛΕΑ ΚΑΙ ΠΡΟΛΗΨΗ

Οι αρχιτεκτονικές VoIP διανέμονται (proxy servers, gateways, application servers, terminals, κλπ) και έτσι δύσκολο να αντιμετωπιστούν οι επιθέσεις από μια συγκεντρωμένη προσέγγιση ασφάλειας. Η αρχιτεκτονική για την ανίχνευση και την πρόληψη κάποιου εισβολέα θα πρέπει να διανέμεται, εκτός αν το δίκτυο έχει σχεδιαστεί με κάποιο συγκεκριμένο τρόπο.

Το πιο κάτω σχήμα απεικονίζει τη γενική αρχιτεκτονική όπου το VoIPspecific Honeypot (παγίδα) είναι χωρισμένο από την πραγματική περιοχή υποδομής. Ο διανεμημένος έλεγχος εφαρμογών επιτυγχάνεται επεκτείνοντας την ασφάλεια VoIP και στα στοιχεία υποδομής (SIP Proxy Servers, Terminals κ.α.).

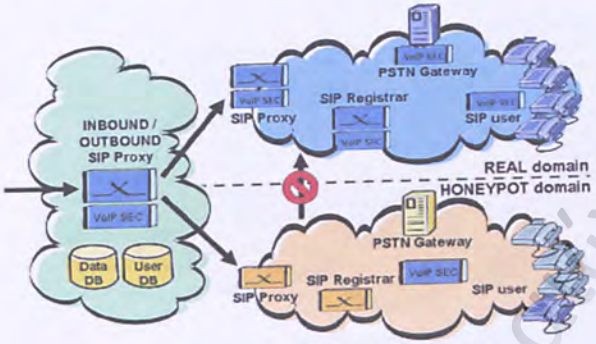


Figure 1: Network Architecture

Εικόνα 27: αρχιτεκτονική προτεινόμενου δικτύου

Προκειμένου να προσαρμοστεί το VoIPspecific Honeypot στην αρχιτεκτονική ανίχνευσης και πρόληψης του εισβολέα, εισήχθη ένας πρόσθετος μηχανισμός. Ο στόχος αυτός του μηχανισμού είναι να γεφυρώσουν με διαφάνεια τις πραγματικές περιοχές και τις περιοχές της παγίδας με τις εξωτερικές περιοχές, έτσι ώστε να δρομολογούνται σωστά τα πραγματικά αιτήματα στην πραγματική περιοχή ενώ τα spam στο Honeypot.

Στην αρχιτεκτονική που απεικονίζεται στο παραπάνω σχήμα, το domain απεικονίζεται από έναν outbound/inbound proxy σε ένα δημόσιο πραγματικό δίκτυο. Η πραγματική περιοχή και το honeypot αποσυνδέονται αυστηρά το ένα από το άλλο, έτσι ώστε να αποτραπούν τα backdoors στο παραγόμενο περιβάλλον.

Κατά συνέπεια μια βάση δεδομένων με τους κανονικούς χρήστες και μια με τους χρήστες που έχουν χαρακτηριστεί ως κακόβουλοι, καταγράφονται στον proxy ως πληροφορίες που μοιράζονται το μέσο εσωτερικό domain. Το χαρακτηριστικό τέτοιων βάσεων δεδομένων είναι να υπάρχει διανομή των πληροφοριών μεταξύ της περιοχής Honeypot και της πραγματικής περιοχής, για να βελτιώσει τις μεθόδους ανίχνευσης και πρόληψης και σχέδια βασισμένα στις παρατηρήσεις του VoIPspecific Honeypot.

7.3.1 VOIP-SPECIFIC HONEYPOT

Το Honeypot είναι μια παγίδα που έχει στόχο να ανιχνεύσει, να εκτρέψει και να ελέγξει επιθέσεις σε συστήματα πληροφοριών. Γενικά αυτό το Honeypot αποτελείται από έναν υπολογιστή, από δεδομένα ή δίκτυα που εμφανίζονται να είναι μέρος ενός δικτύου αλλά που στην πραγματικά είναι απομονωμένο και ελεγχόμενο.

Ένα Honeypot έχει συγκεκριμένη αξία στην ανίχνευση επίθεσης και εκτροπής. Είναι συνήθως συγκεκριμένο σύστημα που κανονικά δεν πρέπει να αντιμετωπίζει οποιαδήποτε κίνηση ή δραστηριότητα. Οποιαδήποτε δραστηριότητα φαίνεται σε ένα Honeypot μπορεί να ερμηνεύεται σαν κακόβουλη ή αναρμόδια. Το Honeypot μπορεί να γίνει πολύ χρήσιμο σαν συγκεκριμένο συστατικό μιας αρχιτεκτονικής που ελέγχει τις VoIP εισβολές και προλήψεις.

Η έννοια του Honeypot μπήκε στο VoIP κόσμο αναπτύσσοντας μια πλήρη παράλληλη υποδομή VoIP εντελώς λογική και φυσικά χωρισμένη από τον πραγματικό κόσμο, όπου παρατηρούμε συνεχώς την κινητικότητα. Ο φυσικός χωρισμός είναι απαραίτητος προκειμένου να αποφύγουμε ότι ένας επιτιθέμενος που εισβάλει στο VoIP-specific Honeypot, είναι ικανός να επιτεθεί από κει και στην πραγματική υποδομή VoIP.

Τα κύρια χαρακτηριστικά του VoIP-specific Honeypot είναι ο μετριασμός της SPIT απειλής με μιας χαμηλού κόστους υποδομή και το γεγονός ότι μια τέτοια υποδομή συμπληρώνει καλά την πιθανή ανίχνευση εισβολής και πρόληψη με τη συλλογή χρήσιμων πληροφοριών ώστε να βελτιωθεί το οποιοδήποτε ποσοστό λάθους άλλων μεθοδολογιών.

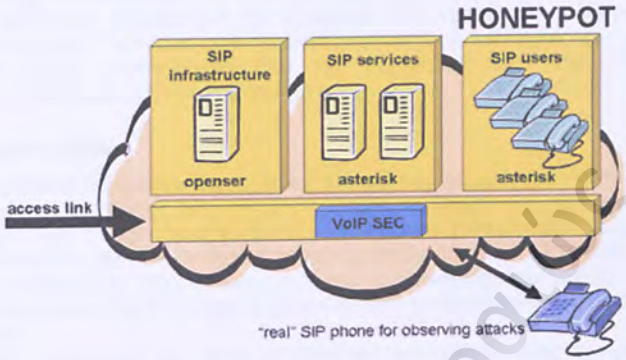


Figure 2: Honeypot Architecture

Εικόνα 28: Αρχιτεκτονική VoIPspecific "παγίδας"

Για την εφαρμογή του VoIP-specific Honeypot χρησιμοποιήθηκε ένα μίγμα γνωστού λογισμικού:

- Openser2: ένας ανοικτού λογισμικού SIP proxy server Η προηγμένη openser λογική δρομολόγησης επιτρέπει τη διαμόρφωση σύνθετων σχεδίων δρομολόγησης.
- Asterisk3: ένας PBX ανοικτού λογισμικού που προσφέρει ένα ευρύ φάσμα υπηρεσιών και εφαρμογών (π.χ. λειτουργίες πυλών, ταχυδρομικές θυρίδες (mailboxes)) .

Το VoIP-specific Honeypot μιμείται ένα πραγματικό δίκτυο VoIP ως εξής:

• η υποδομή SIP μιμείται από Openser.

Μια περίπτωση του Openser διαμορφώνεται στον VoIP-specific Honeypot. Πολλές τέτοιες περιπτώσεις μπορούν να χρησιμοποιηθούν για να χτίσουν πιο σύνθετα SIP δίκτυα. Το Openser διαμορφώνεται με έναν τυχαίο call-dispatcher για το χειρισμό άγνωστων καλούμενων.

• οι SIP υπηρεσίες μιμούνται από τον Asterisk.

Με αριθμούς (που είναι extensions του Asterisk) ο επιτιθέμενος δρομολογείται στα mailboxes.

• τους SIP χρήστες τους μιμούνται από τα mailboxes του Asterisk.

Τα προαιρετικά SIP τηλέφωνα μπορούν να εφαρμοστούν στον "καθρέφτη" κάθε εισερχόμενης κλήσης για λόγους παρατήρησης.

7.4 ΑΛΛΕΣ ΣΧΕΤΙΚΕΣ ΛΥΣΕΙΣ

Τα συστήματα ανίχνευσης εισβολέων είναι μια δεύτερη γραμμή άμυνας πίσω από τους μηχανισμούς πρόληψης εισβολέων, όπως η αυθεντικοποίηση κωδικών πρόσβασης και τα firewalls. Σε άλλη υλοποίηση συστήματος ασφάλειας παρουσιάζεται η ανάγκη της γνώσης περιοχών σε συγκεκριμένα IDSs, βασισμένα σε WEB εφαρμογές.

Η ασφάλεια των συστημάτων έχει μεγάλο ενδιαφέρον για τη VoIP τεχνολογία, για το λόγο αυτό προτείνονται διάφορες προσεγγίσεις ανίχνευσης εισβολέων σαν απαντήσεις σε διαφορετικές απειλές.

Το Scidive χρησιμοποιεί μεθόδους βασισμένες στην ΄υπογραφή΄ και σε πρότυπα σχέδια πρωτοκόλλου. Προτάθηκε επίσης ένα στατιστικό πλαίσιο βασισμένο στο πρότυπο Bayes ώστε να αναγνωρίζει τα κανονικά από τα κακόβουλα SIP μηνύματα.

Το SEC προτάθηκε ως ένας ΄ελαφρύς΄ συσχετιστής των γεγονότων (events) που μπορεί να εξυπηρετήσει τις διαφορετικές εφαρμογές, από τον έλεγχο log αρχείων και συστημάτων μέχρι την ανίχνευση της απάτης και της εισβολής.

Πιο πρόσφατα έγγραφα για την ανίχνευση των κοινωνικών επιθέσεων πρότειναν λύσεις που περιείχαν ΄blacklist΄ και ΄greylist΄ τύπους και οντότητες κεντρικοποιημένων δικτύων. Τέλος, μια ενδιαφέρουσα ιδέα της ανίχνευσης SPIT είναι βασισμένη στη δακτυλοσκοπία συσκευών (device fingerprinting).

7.5 ΣΥΜΠΕΡΑΣΜΑ

Έχουμε παρουσιάσει παραπάνω μια ολιστική προσέγγιση για ελέγχους VoIP ασφάλειας. Τα βασικά συστατικά της λύσης μας είναι ένα VoIP honeypot (παγίδα για αμιγώς VoIP συστήματα) και ένας συσχετισμός γεγονότος (events) σε επίπεδο SIP. Αυτή η λύση είναι ικανή να υπερασπίσει και DoS επιθέσεις, αλλά και επιθέσεις τύπου SPIT και Vishing.

Οι ικανότητες του SEC το κάνουν ικανό να αποτελέσει το τεχνικό εργαλείο στην οικοδόμηση αποδοτικών VoIP IDS και παρουσιάζεται η δυνατότητα που έχει αναπτύσσοντας ένα πρωτότυπο.

Ακόμα, επεκτείναμε σε αυτό το έγγραφο την έννοια ενός honeypot προς τις εφαρμογές VoIP και δείξαμε πώς οι κοινωνικές επιθέσεις μπορούν να μετριαστούν. Τα παραπάνω εφαρμόστηκαν και εξετάστηκαν σε δοκιμαστικό περιβάλλον, αλλά πρέπει να γίνουν περισσότερες δοκιμές σε πραγματικό περιβάλλον σε VoIP δίκτυα. Μελλοντικά θα πρέπει να εξεταστεί επίσης η επέκταση των τεχνικών συσχετισμού γεγονότων σε σχέση με παραδείγματα από τη μηχανική μάθηση.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία παρουσιάσθηκαν εκτενώς τα πρωτόκολλα που χρησιμοποιούνται στις VoIP επικοινωνίες και η συμβολή τους στην επίτευξη ενός ασφαλούς περιβάλλοντος για τηλεπικοινωνίες. Έγινε λόγος για τις υπάρχουσες τεχνικές επίλυσης κοινών προβλημάτων και τέλος, παρουσιάστηκε μια αρχιτεκτονική επίλυσης του προβλήματος της ασφάλειας κυρίως για προβλήματα DoS επιθέσεων, αλλά και επιθέσεων τύπου SPIT.

Οι υπάρχουσες τεχνικές, ναι μεν, εξυπηρετούν τις σημερινές ανάγκες για καλύτερη ποιότητα και εξυπηρέτηση, αλλά υπάρχουν σίγουρα κενά τα οποία πρέπει να καλυφθούν. Οι καινούριες τεχνικές που αναπτύσσονται σε περιορισμένα περιβάλλοντα και εργαστήρια θα πρέπει να μεταφερθούν και να δοκιμαστούν σε πραγματικά περιβάλλοντα, όπου και η κίνηση των VoIP δικτύων είναι περισσότερο αυξημένη και άρα και οι κίνδυνοι που υπονομεύουν.

Το γεγονός ότι στα επόμενα χρόνια αναμένεται «εκτόξευση» της χρήσης των VoIP τεχνολογιών, λόγω των πολλών πλεονεκτημάτων τους, σίγουρα θα υπάρξει και αύξηση των απειλών. Ίσως εμφανιστούν και απειλές που αυτή τη στιγμή, στο επίπεδο που είμαστε, ακόμα δεν τις έχουμε λάβει υπόψη μας ώστε να αναπτύξουμε τους κατάλληλους μηχανισμούς ασφαλείας.

Συμπερασματικά λοιπόν, νέες τεχνικές θα χρηστούν αναγκαίες και απαραίτητες για την όλο και μεγαλύτερη ικανοποίηση των χρηστών, την καλύτερη ποιότητα υπηρεσιών και τη διασφάλιση της ασφάλειας και της ιδιωτικότητας των πελατών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Voice Over IP Reference Page
2. "H.323.Packet-based multimedia communications systems", ITU-T, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU (06/2006)
3. RFC 791 - IP protocol
4. "RFC 2543, SIP: Session Initiation Protocol". Handley, Schulzrinne, Schooler, Rosenberg
5. "Social Security to Build "World's Largest VOIP" Government Technology
6. "H.323". Voice over IP fundamentals. Jonathan Davidson, James Peters, Jim Peters, Brian Gracely.
7. "RFC 3525, *Gateway Control Protocol Version 1*", C. Groves, M. Pantaleo, T. Anderson, T. Taylor (editors), The Internet Society (June 2003)
8. "RFC 5125, *Reclassification of RFC 3525 to Historic*", T. Taylor, The IETF Trust (February 2008)
9. "RFC 3261, SIP: Session Initiation Protocol"
10. "Holistic VoIP Intrusion Detection and Prevention System", Mohamed Nassar, Saverio Niccolini, Radu State
11. "Security Considerations for Voice Over IP Systems", National Institute of standards and technology