128

Α.Τ.Ε.Ι. ΚΑΛΑΜΑΤΑΣ - ΠΑΡΑΡΤΗΜΑ ΣΠΑΡΤΗΣ

Τμήμα Τεχνολογίας Πληροφορικής &
Τηλεπικοινωνιών

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΥΓΚΡΙΤΙΚΗ ΜΕΛΕΤΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΡΩΤΟΚΟΛΛΩΝ ΚΑΙ ΤΩΝ ΕΡΓΑΛΕΙΩΝ ΤΗΛΕΔΙΑΣΚΕΨΗΣ

Επιβλέπων Καθηγητής: Μποζαντζής Βασίλειος

Φοιτήτρια:

Σουρέλη Ασπασία *ΑΜ: 2008046*

Σπάρτη, Μάιος 2013

Copyright © Ασπασία Σπ. Σουρέλη, 2013

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Α.Τ.Ε.Ι. Καλαμάτας.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ	ΥΠΟΓΡΑΦΕΣ
1. ΠΑΝ. Ι. ΦΙΛΙΠΠΟΠΟΥΛΟΣ	
2. ΛΙΑΠΕΡΔΟΣ Σ.	
3. ΜΠΟΖΑΝΤΖΗΣ Β.	

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς, είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας.

Η συγγραφέας,

Σουρέλη Α

Σουρέλη Ασπασία

Ευχαριστίες

Έχοντας φτάσει στο τέλος της πτυχιακής μου εργασίας, αισθάνομαι υποχρεωμένη να μιλήσω για κάποιους ανθρώπους, που ο καθένας με τον δικό του τρόπο σηματοδότησε την πορεία των χρόνων μου στις προπτυχιακές σπουδές μου και να τους ευχαριστήσω.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω τον επιβλέποντα μου, κύριο Βασίλειο Μποζαντζή, Επιστημονικό Συνεργάτη του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών του Α.Τ.Ε.Ι. Καλαμάτας, διότι η συνεργασία μαζί του ήταν ένας καταλύτης για την ολοκλήρωση των προπτυχιακών σπουδών μου. Τα αποτελέσματα της εργασίας αυτής είναι από τη συνεργασία με τον κ. Μποζαντζή. Η συνεργασία μας ξεκίνησε όταν ήμουν προπτυχιακός φοιτήτρια στο χειμερινό εξάμηνο του 2011 - 2012, στο μάθημα «Επικοινωνίες Δεδομένων». Από τη συνεργασία αυτή, είχα την πρώτη εμπειρία στις επικοινωνίες. Η πλήρη ηθική στήριξή του και η εμπιστοσύνη του στο πρόσωπό μου, με όπλισαν με κουράγιο, δύναμη και μου έδωσε το θάρρος να αναλάβω την προσπάθεια για τη σύγκριση των δύο διαφορετικών πρωτοκόλλων και δύο εργαλείων τηλεδιάσκεψης.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου Σπήλιο Σουρέλη και Μαρία Σουρέλη για την αμέριστη υποστήριξή τους όλα αυτά τα χρόνια, των προπτυχιακών σπουδών μου. Αφιερώνω αυτή την εργασία στους γονείς μου, ως ελάχιστη ευγνωμοσύνη για την κατανόηση και την υπομονή τους όλα αυτά τα χρόνια.

Σουρέλη Ασπασία

Σπάρτη, Μάιος 2013

Περιεχόμενα

Περιεχόμενα εικόνων

Ορισμοί

Ακεραιότητα έχουμε όταν τα δεδομένα μας δεν αλλοιώνονται με μη εξουσιοδοτημένο τρόπο.

Ανωνυμία ορίζεται η κατάσταση εκείνη στην οποία είσαι μη αναγνωρίσιμος μέσα σε ένα σύνολο οντοτήτων, το ανώνυμο σύνολο.

Ασφάλεια είναι το σύνολο όλων μέτρων που λαμβάνονται για να αποτραπούν απώλειες κάθε είδους. Η απώλεια μπορεί να συμβεί λόγω σφάλματος του χρήστη, προβλημάτων στον κώδικα, κακόβουλων ενεργειών, αποτυχιών υλικού και ενεργειών της φύσης. Η ασφάλεια διακρίνεται σε επιμέρους κομμάτια, στην διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα, την ιδιωτικότητα και την ανωνυμία.

Διαθεσιμότητα έχουμε όταν τα δεδομένα (ή υπηρεσία) είναι διαθέσιμα προς χρήση όταν αυτό απαιτηθεί.

Εμπιστευτικότητα έχουμε όταν στα δεδομένα μας έχουν πρόσβαση (ανάγνωση, εμφάνιση κτλ) μόνο εξουσιοδοτημένα άτομα.

Εργαλεία τηλεδιάσκεψης είναι εργαλείο όπου με τη χρήση του πραγματοποιείται η τηλεδιάσκεψη.

Ιδιωτικότητα είναι ότι συνίσταται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτήν την έννοια η ιδιωτικότητα προσβάλλεται με την αποκάλυψη της απόρρητης πληροφορίας.

Πρωτόκολλο επικοινωνίας ορίζεται ένα σύνολο κανόνων συμφωνημένων και από τα δυο επικοινωνούντα μέρη και που εξυπηρετούν την μεταξύ τους ανταλλαγή πληροφοριών. Το πρωτόκολλο επικοινωνίας είναι δηλαδή μια δέσμη κανόνων στους οποίους στηρίζεται η επικοινωνία των συσκευών (συνήθως, αλλά όχι πάντα, υπολογιστών) σε ένα δίκτυο. Οι κανόνες αυτοί καθορίζουν τη μορφή, το χρόνο και τη σειρά μετάδοσης των πληροφοριών στο δίκτυο. Εκτελούν, επίσης, έλεγχο και διόρθωση σφαλμάτων στη διάρκεια μετάδοσης των πληροφοριών.

Τηλεδιάσκεψη είναι η επικοινωνία, μέσω υπολογιστών, δύο ή περισσοτέρων ατόμων ή ομάδων ατόμων, που βρίσκονται σε απόσταση μεταξύ τους. Κατά την τηλεδιάσκεψη γίνεται συγχρόνως οπτική και ακουστική επαφή των μετεχόντων (τηλεδιάσκεψη μπορούμε να έχουμε και με ακουστική επαφή μόνο). Η τηλεδιάσκεψη γίνεται σε πραγματικό χρόνο και επιτρέπει να γίνει ομιλία, συζήτηση, ερωτήσεις και απαντήσεις με ομιλητές και ακροατές σε απόσταση. Η οθόνη του υπολογιστή είναι εκείνη που κάνει δυνατή την οπτική και την ακουστική επαφή.

Voice over IP ή VoIP (VVOIP ή Video and Voice over IP αποτελεί την επέκταση του VoIP ώστε να περιλαμβάνει και την αποστολή εικόνας) ή τηλεφωνία μέσω διαδικτύου ή σωστότερα ΦεΔΠ, δηλαδή «Φωνή επί Διαδικτυακού Πρωτοκόλλου», χαρακτηρίζει μια ομάδα πρωτοκόλλων - τεχνολογιών (H.323, SIP), η οποία προσφέρει φωνητική συνομιλία σε πραγματικό χρόνο με σχετικά καλή ποιότητα πλέον και στην ουσία χωρίς κόστος.

Περίληψη

Στην σημερινή εποχή όπου όλο και περισσότερες επιχειρήσεις επιδιώκουν την μείωση των λειτουργικών εξόδων από την μετακίνηση των υπαλλήλων στις διάφορες περιοχές όπου στεγάζονται τα τμήματα της επιχείρησης, είναι περισσότερο αναγκαίο από ποτέ η χρήση ειδικών εργαλείων τηλεδιάσκεψης. Για την υποστήριξη των εργαλείων αυτών έχουν αναπτυχθεί συγκεκριμένα πρωτόκολλα επικοινωνίας. Όμως, επειδή η κοινωνία που ζούμε δεν είναι αγγελικά πλασμένη, και υπάρχουν αρκετοί κακόβουλοι χρήστες, είτε λόγω διασκέδασης είτε για επαγγελματικούς λόγους, υπάρχουν αρκετά προβλήματα και στα πρωτόκολλα και στα εργαλεία τηλεδιάσκεψης.

Στα πλαίσια της πτυχιακής αυτής εργασίας γίνεται προσπάθεια για την περιγραφή των πρωτοκόλλων και των εργαλείων τηλεδιάσκεψης και την αποτίμηση αυτών στα θέματα ασφαλείας που αντιμετωπίζουν.

Στο πρώτο κεφάλαιο περιγράφεται η έννοια της τηλεδιάσκεψης και σε ποιους τομείς της ζωής μας εφαρμόζεται. Ακόμη, γίνεται μία εκτενής αναφορά στα προβλήματα ασφαλείας που έχουν ανακύψει στα διάφορα συστήματα τηλεδιάσκεψης.

Στο δεύτερο κεφάλαιο γίνεται μια προσπάθεια ανάλυσης των δύο βασικότερων πρωτοκόλλων, SIP και H.323. Συγκεκριμένα, αναλύεται η αρχιτεκτονική τους, η λειτουργία τους, καθώς και τα θέματα ασφαλείας που αντιμετωπίζουν.

Στο τρίτο κεφάλαιο γίνεται μια προσπάθεια ανάλυσης των δύο βασικότερων εργαλείων, NetMeeting και Asterisk. Συγκεκριμένα, αναλύεται η αρχιτεκτονική τους, η λειτουργία τους, καθώς και τα θέματα ασφαλείας που αντιμετωπίζουν.

Στο τέταρτο κεφάλαιο υλοποιείται και παρατίθενται τα αποτελέσματα μιας από τις πιο γνωστές επιθέσεις, επίθεση μη – εξουσιοδοτημένης πρόσβασης, σε ένα από τα ευρέως διαδεδομένα εργαλεία τηλεδιάσκεψης, στο Asterisk.

Στο πέμπτο κεφάλαιο καταγράφονται τα συμπεράσματα από την συνολική μελέτη σύγκρισης των πρωτοκόλλων και των εργαλείων τηλεδιάσκεψης, λαμβάνοντας υπόψιν και την υλοποίηση της επίθεσης του τετάρτου κεφαλαίου.

Κεφάλαιο 1: Η τηλεδιάσκεψη χθες και σήμερα

1.1 Ιστορική ανασκόπηση της τηλεδιάσκεψης

Η τηλεδιάσκεψη έγινε δυνατή μετά τη δημιουργία της τηλεόρασης. Δεν ήταν δημοφιλής στη χρήση ως εργαλείο επικοινωνίας μέχρι πρόσφατα, λόγω των υψηλών δαπανών. Η χρήση της, όμως, αυξήθηκε επειδή υπάρχει η δυνατότητα να εμφανίζει γραφικά και ήχο μέσω ενός σωλήνα για ψυχαγωγία, και η ίδια τεχνολογία είναι ήδη σε θέση να χρησιμοποιηθεί ως μέσο επικοινωνίας.

Μια τηλεδιάσκεψη μπορεί να είναι μια απλή συνάντηση μεταξύ δύο συμμετεχόντων ή μπορεί να αφορά περισσότερα άτομα από πολλές διαφορετικές τοποθεσίες. Όταν υπήρξε η δυνατότητα να έχουν αυτό το είδος επικοινωνίας, τότε που τέθηκε για πρώτη φορά σε διάθεση, το κόστος ήταν πολύ υψηλό. Ως εκ τούτου, δεν μπορούσε να χρησιμοποιηθεί για τους λόγους που χρησιμοποιείται σήμερα. Οι πρώτες προσπάθειες να πραγματοποιηθεί επικοινωνία μέσω βίντεο είχαν πολύ κακή ποιότητα εικόνας και ήταν σχεδόν άχρηστες ως εργαλείο των μέσων επικοινωνίας.

Στη δεκαετία του 1980, αυτό το είδος της επικοινωνίας έγινε περισσότερο γνωστό από απλά μια δυνατότητα που παρείχε η τεχνολογία. Μέσα από μελέτες δοκιμών και τη δημιουργία της πιο προηγμένης τεχνολογίας, οι πρώτες υπηρεσίες τηλεδιάσκεψης κατέστησαν διαθέσιμες στη δεκαετία του 1990. Τα πρωτόκολλα του διαδικτύου και το προηγμένο λογισμικό συμπίεσης χρησιμοποιούνταν σε αυτά τα συστήματα τηλεδιάσκεψης και ήταν διαθέσιμα μέσω της χρήσης του επιτραπέζιου υπολογιστή ως μέσο. Το 1992, ο Tim Dorcey σχεδίασε την τεχνολογία που γρήγορα χρησιμοποιήθηκε όπως στο MSN Messenger και σε παρόμοια συστήματα με τη χρήση του υπολογιστή.

Η ψηφιακή συμπίεση ήχου και βίντεο, που έχουν ροές σε πραγματικό χρόνο, είναι αυτό που κάνει η τηλεδιάσκεψη δυνατή.

Η δημιουργία της ψηφιακής τεχνολογίας ήταν πράγματι το κλειδί για την τελική λήψη της τηλεδιάσκεψης. Μέσω αυτής της δημιουργίας οι άνθρωποι δεν χρειάζονται πλέον να μετακινηθούν μακριά από το σπίτι, προκειμένου να δραστηριοποιηθούν. Οι εταιρείες δεν θα πρέπει να αναλάβουν το βάρος της αποστολής των συνεργατών σε

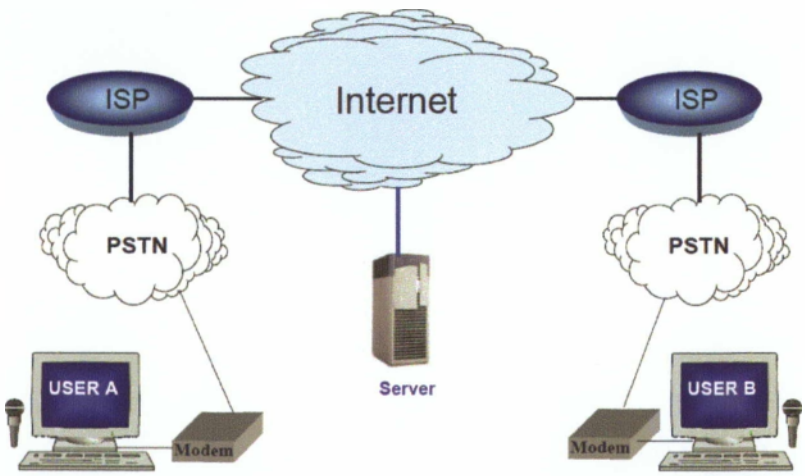
άλλα κράτη. Η τηλεδιάσκεψη έχει διανύσει πολύ δρόμο στην πάροδο του χρόνου, αξιοποιώντας ότι έχει να προσφέρει.[1][18][20]

1.2 Διαχρονική εξέλιξη της τηλεδιάσκεψης

Σήμερα η τηλεφωνία, που πραγματοποιείται στο Internet, περιέχει τηλεδιασκέψεις πάνω από το Internet ή πάνω από ένα WAN (Wide Area Network).

Η τεχνολογία αιχμής αποτελεί το VoIP. Υπάρχουν πολλά λογισμικά τα οποία προορίζονται για προσωπική χρήση. Ενδεικτικά προϊόντα είναι το Netmeeting και το Asterisk που θα αναλύσουμε στο Κεφάλαιο 3. Ακόμα υπάρχουν τα Skype, Google Talk, Windows Live Messenger, Yahoo Messenger, OpenH.323 Project, OpenAM, SIP/SER και OpenSer. Μια τηλεδιάσκεψη μπορεί να είναι απλή και να βασίζεται σε μια απλή τηλεφωνική κλήση, αλλά μπορεί όμως να είναι πιο σύνθετη και να περιέχει και μετάδοση κινούμενης εικόνας και δεδομένων σε μεγάλους χώρους που υπάρχουν οθόνες και ανεπτυγμένα οπτικοακουστικά μέσα.

Με τον καιρό όμως, οι τηλεδιασκέψεις γίνονται όλο και πιο σύγχρονες και μπορούν να εφαρμοστούν σε προσωπικούς υπολογιστές αλλά και σε κινητά τηλέφωνα.



Εικόνα 1: Η χρήση της τηλεδιάσκεψης

Υπάρχουν πολλά πλεονεκτήματα για την χρήση της τηλεδιάσκεψης σε σχολικά περιβάλλοντα και χώρους εργασίας. Εξοικονομείται χρόνος, που θα διέθετε κανείς για να παραστεί φυσικά σε ένα χώρο, όπως, επίσης, εξοικονομούνται χρήματα

προκειμένου να καταφέρουν να έρθουν όσοι επιθυμούν να συμμετάσχουν στην τηλεδιάσκεψη και να βρίσκονται στον ίδιο φυσικό χώρο.

Επίσης, αποφάσεις που διαφορετικά θα χρειαζόταν περισσότερος χρόνος για να ληφθούν, τώρα με την τηλεδιάσκεψη ολοκληρώνονται σε πολύ μικρότερο χρονικό διάστημα. Με την χρήση τεχνικών απόκρυψης, μπορεί να επιτευχθεί υψηλή ποιότητα όσον αφορά την ασφάλεια των τηλεπικοινωνιών.

Βασικό κομμάτι στην ποιότητα μιας τηλεδιάσκεψης αποτελεί και ο εξοπλισμός προκειμένου αυτή να πραγματοποιηθεί. Για την καλύτερη εξέλιξη μιας τηλεδιάσκεψης, οι συμμετέχοντες ακολουθούν κανόνες, που βοηθούν στην καλύτερη οργάνωση της.[1][18][20]

1.3 Η χρήση της τηλεδιάσκεψης

1.3.1 Ανάγκη για τηλεδιάσκεψη

Η έκρηξη στην τεχνολογία που συμβαίνει σε ότι αφορά τα συστήματα τηλεδιάσκεψης είναι αποτέλεσμα των χρήσιμων χαρακτηριστικών που προσφέρουν αυτά τα συστήματα. Ορισμένα από αυτά τα χαρακτηριστικά είναι η επικοινωνία σε πραγματικό χρόνο, η ανταλλαγή οπτικών δεδομένων, η ανταλλαγή δεδομένων. Τα χαρακτηριστικά αυτά έκαναν τον χώρο των εταιρειών να ενδιαφερθούν σε αυτού του είδους την επικοινωνία. Τα συστήματα δηλαδή αυτά εξυπηρετούν συγκεκριμένες ανάγκες των εταιρειών όπως είναι η ανάγκη για συγχρονισμό με την ανάπτυξη, την συνεργασία ατόμων που δεν βρίσκονται στο ίδιο φυσικό σημείο και η επικοινωνία με πελάτες που βρίσκονται σε απομακρυσμένα σημεία. Η τηλεδιάσκεψη έρχεται να ξεπεράσει όλες αυτές τις ανάγκες και να προσφέρει λύσεις, που είναι σύγχρονες, έγκυρες και έγκαιρες.[17][18][20]

1.3.2 Η χρήση της τηλεδιάσκεψης

Η τηλεδιάσκεψη έχει πολλές χρήσεις σε διάφορους τομείς της ζωής και αφορά αρκετά διαφορετικά επαγγέλματα. Εφαρμογές της είναι η τηλεϊατρική, η τηλεεκπαίδευση, η τηλεεργασία, η επικοινωνία ατόμων με προβλήματα ακοής και άλλες.

Τηλεϊατρική

Μεγάλο ενδιαφέρον παρουσιάζει η εφαρμογή της τεχνολογίας στην από απόσταση διαγνωστική - συμβουλευτική ιατρική. Με τη χρήση της τηλεδιάσκεψης, άνθρωποι που δεν μπορούν να μετακινηθούν εύκολα λόγω κινητικών προβλημάτων, υγείας ή μεγάλης απόστασης, μπορούν να επικοινωνήσουν και να συμβουλευθούν το γιατρό ή το νοσηλευτικό προσωπικό.

Τηλεεκπαίδευση

Η τηλεδιάσκεψη παρέχει τη δυνατότητα σε καθηγητές να διδάξουν σε απομακρυσμένες αίθουσες ή ταυτόχρονα σε περισσότερες από μία αίθουσες. Επίσης, μαθητές από σχολεία, χωρίς μεγάλες οικονομικές δυνατότητες, μπορούν να παρακολουθήσουν ακριβά ή εξειδικευμένα μαθήματα ή να κάνουν εικονικά εκπαιδευτικά ταξίδια σε μουσεία, όπερες, πανεπιστήμια κ.λπ.

Τηλεεργασία

Πολύ μεγάλο ενδιαφέρον παρουσιάζουν οι εφαρμογές της τηλεδιάσκεψης στο χώρο της εργασίας. Η πιο συνηθισμένη εφαρμογή είναι η συνδιάσκεψη δύο ή περισσότερων στελεχών μιας επιχείρησης που δεν βρίσκονται στο ίδιο δωμάτιο, μπορεί ούτε καν στην ίδια ήπειρο. Επιπλέον, παρέχεται στους συμμετέχοντες η δυνατότητα για ταυτόχρονη επεξεργασία ενός κειμένου, λογιστικού πίνακα ή άλλης εφαρμογής, δίνοντας προστιθέμενη αξία στην έννοια της συνεργασίας.

Επικοινωνία Ατόμων με Προβλήματα Ακοής

Ιδιαίτερη εφαρμογή βρίσκουν τα συστήματα τηλεδιάσκεψης σε ανθρώπους με έλλειψη ή απώλεια ακοής. Μέσω της μετάδοσης της εικόνας και της χρήσης της νοηματικής γλώσσας μπορούν να υποκαταστήσουν την επικοινωνία τους χρησιμοποιώντας απλές, point-to-point συνδέσεις.[18][20][22]

1.3.3 Πλεονεκτήματα

Τα οφέλη για την αποδοτικότερη οργάνωση γραφείου μιας επιχείρησης, με την τεχνολογία της τηλεδιάσκεψης είναι τα παρακάτω:

- Αυξάνει την παραγωγικότητα της επιχείρησης, επικοινωνώντας αποδοτικότερα και πιο ολοκληρωμένα με τους προμηθευτές και τους πελάτες της.

- Μειώνει το χρόνο λήψης αποφάσεων.
- Μειώνει το κόστος και αυξάνει τα έσοδα, μέσω των επικοινωνιακών διασυνδέσεων.
- Δημιουργεί μια αλλαγή στην κουλτούρα της εταιρίας, για να μπορεί να υλοποιεί μια συνεχή βελτίωση, μέσω της τεχνολογίας.
- Προσδίδει μια διεθνή εικόνα στην εταιρία.
- Αναπτύσσει νέες διαδικασίες που οδηγούν σε αλλαγή των δομών λειτουργίας της εταιρίας.
- Ενεργοποιεί το προσωπικό της για να αναπτύξει νέες επιδεξιότητες.[18][20]

1.3.4 Μειονεκτήματα

Η τεχνολογία της τηλεδιάσκεψης επηρεάζεται από πολλές παραμέτρους. Τα πακέτα δεδομένων IP που ταξιδεύουν από έναν υπολογιστή μέσω διαφόρων δικτύων στον προορισμό τους, μπορεί να φτάσουν καθυστερημένα, με διαφορετική σειρά ή ακόμα και να χάνονται.

Σημαντικό ρόλο στην ποιότητα, παίζουν ο λόγος της συμπίεσης που εφαρμόζει ο κωδικοποιητής καθώς και η ταχύτητα και η διαθέσιμη χωρητικότητα στο δίκτυο μεταφοράς δεδομένων. Συγκεκριμένα:

- Απαιτείται υψηλή ταχύτητα διαδικτύου (Internet) για να πραγματοποιηθεί μια τηλεδιάσκεψη.
- Η ποιότητα της φωνής είναι χαμηλότερη από ότι στα παραδοσιακά τηλέφωνα.
- Η υπηρεσία δεν λειτουργεί όταν υπάρχει διακοπή ρεύματος.
- Δεν υπάρχει άμεση σύνδεση με τους αριθμούς έκτακτης ανάγκης.
- Υπάρχει πιθανότητα κλοπής των αποθηκευμένων φωνητικών δεδομένων από κακόβουλους χρήστες (hackers).
- Η υπηρεσία τηλεδιάσκεψης είναι επιρρεπής στους ιούς.[18][20]

1.4 Η ασφάλεια στην τηλεδιάσκεψη

Η πρώτη γενιά εργαλείων τηλεδιάσκεψης δούλευαν σωστά σε ομογενή και ειδικά περιβάλλοντα, αλλά υπήρξαν προβλήματα όταν αναπτύχθηκαν τα ετερογενή δημόσια δίκτυα. Κατά συνέπεια, το τοπίο της τηλεδιάσκεψης σήμερα απαιτεί προετοιμασία

και σκέψη γύρω από την συνδεσιμότητα και ιδίως στην ασφάλεια του περιβάλλοντος του δικτύου. Προετοιμάζοντας και πραγματοποιώντας ένα ασφαλές περιβάλλον, πρέπει να έχουμε στο μυαλό μας όλα τα μέρη ενός οργανισμού. Αυτό εμπεριέχει τους τελικούς χρήστες να έχουν την ελευθερία της χρήσης της τηλεδιάσκεψης ως σημαντικό επικοινωνιακό εργαλείο, επιτρέποντας τους να συνδέονται όπου και όποτε χρειάζονται. Επί προσθέτως, οι διαχειριστές του δικτύου πρέπει να αισθάνονται εμπιστοσύνη ότι τα αρχεία τους είναι ασφαλή από τους εισβολείς. Η κατανόηση των προκλήσεων και η εφαρμογή των λύσεων είναι το μεγαλύτερο εμπόδιο όταν εφαρμόζεται μια λύση τηλεδιάσκεψης.

Στα πλαίσια του Vampire Project χρηματοδοτούμενο από το Γαλλικό Εθνικό Γραφείο Έρευνας (ANR) για την καλύτερη κατανόηση της ευρύτερης ασφάλειας της τηλεδιάσκεψης, πραγματοποιήθηκε μια έρευνα που περιλάμβανε 221 επιθέσεις που έλαβαν χώρα από το 1999 έως το Νοέμβριο του 2009. Τα προβλήματα ασφαλείας αυτά περιλαμβάνουν επιθέσεις σχετικά απλές, όπως άρνηση εξυπηρέτησης υπηρεσιών (DoS), ως και σοβαρότερες, όπως υποκλοπή στις τηλεπικοινωνίες, απομακρυσμένη διαχείριση εξυπηρετητών ή ακουστικών, αποφυγή πληρωμών ή χρέωση άλλου χρήστη.

Παρατηρείται ότι τα περισσότερα προβλήματα αφορούν επιθέσεις, συνήθως μέσω του εξυπηρετητή ή του εξοπλισμού του χρήστη. Στο σημείο αυτό πρέπει να σημειωθεί ότι και οι λιγότερο προφανείς επιθέσεις, τις οποίες οι χρήστες και οι διαχειριστές δεν αντιλήφθησαν αμέσως, έχουν επίσης καταγραφεί. Θα πρέπει να αναφέρουμε ότι στην κατάταξη των απειλών, δεν υπολογίζεται σωστά ο πιθανός αριθμός των σοβαρότερων επιθέσεων, γιατί σε πολλές από τις περιπτώσεις όπου έχει καταγραφεί επίθεση DoS, οι επιτιθέμενοι θα μπορούσαν επίσης να έχουν προβεί σε επίθεση υπερχείλισης, αλλά δεν ακολουθήθηκε κάποια λεπτομερής ανάλυση.

Σήμερα, αν και θεωρητικά υπάρχει η γνώση για την προστασία των εφαρμογών του εξυπηρετητή, είναι λιγότερο σαφές πως μπορούν να προστατευτούν οι τελικές συσκευές. Την κατάσταση χειροτερεύει το γεγονός ότι, σπάνια γίνεται αναβάθμιση στο υλικό του εξοπλισμού της τηλεδιάσκεψης, έξω από επιχειρηματικά περιβάλλοντα.

Μέχρι στιγμής, και παρά το γεγονός ότι τα ζητήματα ασφάλειας στη μεταφορά δεδομένων και στη μεταφορά της φωνής έχουν αρκετές ομοιότητες, στη συνείδηση των χρηστών έχουν σε μεγάλο βαθμό εκληφθεί ως εντελώς διαφορετικά ζητήματα. Για παράδειγμα, παρόλο που οι χρήστες κατανοούν εύκολα ότι στην ανταλλαγή δεδομένων μέσω του διαδικτύου ελλοχεύουν αρκετοί κίνδυνοι, έχουν την αίσθηση ότι οι τηλεφωνικές τους συνδιαλέξεις δεν είναι τόσο ευπαθείς και μάλιστα είναι αυστηρά εμπιστευτικές. Με την ενοποίηση των δύο αυτών κόσμων, οι ομοιότητες στα θέματα ασφαλείας αρχίζουν να γίνονται φανερές. Οι τρέχουσες υλοποιήσεις IP τηλεφωνίας, όσον αφορά στη σηματοδοσία των κλήσεων (SIP) και στη μεταφορά των μηνυμάτων φωνής (RTP), δεν παρέχουν επαρκή αυθεντικοποίηση των κλήσεων, ούτε και end-to-end μέτρα ακεραιότητας και εμπιστευτικότητας. Αν αυτά τα χαρακτηριστικά ασφαλείας δεν υλοποιηθούν, τότε θα παρουσιαστούν πολλά κενά ασφαλείας ικανά για κακόβουλη εκμετάλλευσή τους. Επιπλέον, η ασφάλεια στην τηλεδιάσκεψη είναι ένα πολύπλοκο ζήτημα, λόγω των πολλών παραμέτρων και συστατικών που το απαρτίζουν. Παρακάτω, παρατίθενται σε γενικές γραμμές κάποια πιθανά προβλήματα που μπορούν να παρουσιαστούν.

Ενισχυμένη επίθεση μη-ανωνυμοποίησης

Η πιο άμεση επίθεση σε τηλεδιασκέψεις είναι η αναγνώριση της γεωγραφικής τοποθεσίας του χρήστη. Χρησιμοποιώντας μια κατάλληλη βάση δεδομένων αναζήτησης IP και τεχνολογία, οι κακόβουλοι είναι ικανοί να εντοπίσουν την γεωγραφική τοποθεσία του χρήστη.

Επίθεση Ψαρέματος

Σε αυτό τον τύπο της επίθεσης, ένας κακόβουλος εκθέτει ένα ελκυστικό άτομο να ζητήσει ενδεχομένως ευαίσθητες πληροφορίες από άλλους χρήστες, όπως το όνομά τους, τηλεφωνικούς αριθμούς, λογαριασμούς στα εργαλεία τηλεδιάσκεψης, κτλ. Σε αντίθεση με τις παραδοσιακές επιθέσεις ψαρέματος, οι οποίες τυπικά πραγματοποιούνται μέσω ηλεκτρονικού μηνύματος (email) ή με άμεσα μηνύματα (chat messages), ένας κακόβουλος στη τηλεδιάσκεψη μπορεί απλά να αναπαραγάγει ένα βίντεο, που έχει ετοιμάσει εκ των προτέρων για να δελεάσει ανυποψίαστους χρήστες με σκοπό να συνομιλήσουν μαζί του και ενδεχομένως να αποκαλυφθούν ευαίσθητες πληροφορίες.

Επίθεση Man-in-the-Middle

Παρατηρείται ότι οι χρήστες της τηλεδιάσκεψης είναι ευάλωτοι σε επιθέσεις man-in-the-middle (MITM). Ενώ δύο χρήστες πιστεύουν ότι συνομιλούν απευθείας ο ένας με τον άλλον, είναι πιθανό να εισαχθεί ένας τρίτος στη μέση ο οποίος θα παρακολουθεί την συζήτηση χωρίς οι δύο τελικοί χρήστες να το γνωρίζουν ότι η συνομιλία τους παρακολουθείται ή καταγράφεται. Σε συνδυασμό με τις επιθέσεις μη-ανωνυμοποίησης, είναι δυνατό να εκτεθεί η ταυτότητα του χρήστη και να απειληθεί, όπως οι καταγεγραμμένοι χρήστες με εκβιασμό.

Παρακάτω θα παρουσιαστούν επιγραμματικά κάποιες γενικές αρχές που θα πρέπει να ισχύουν σε κάθε σύστημα τηλεδιάσκεψης προκειμένου να πληροί ένα βασικό πλαίσιο ασφαλείας.

Αντίμετρα μη-ανωνυμοποίησης

Η επίθεση μη-ανωνυμοποίησης κυρίως χρησιμοποιεί την IP διεύθυνση του θύματος με το όνομα και το βίντεο του θύματος να μεταφέρουν κακόβουλο υλικό. Η πιο έξυπνη άμυνα σε αυτή την επίθεση είναι να θολωθούν τα πρόσωπα ώστε να προστατέψουν την ταυτότητά τους.

Αντίμετρα ψαρέματος

Διαισθητικά, οι επιθέσεις ψαρέματος μπορούν εύκολα να ανιχνευθούν και να αντιμετωπιστούν. Για παράδειγμα, ένας χρήστη μπορεί να ζητήσει από το συνομιλητή του να αποδείξει ότι το βίντεο που παρακολουθεί είναι πραγματικό ζητώντας να σηκώσει το χέρι η να ανοιγοκλείσει τα μάτια του, κτλ.

Αντίμετρα Man-in-the-Middle

Στη παρούσα κατάσταση, η οποία δεν υποστηρίζει ανώνυμες IP διευθύνσεις, μια προσέγγιση για τις επιθέσεις MITM είναι να γίνει προσπάθεια ελέγχου των μεταξύ τους διευθύνσεων.

Πολιτική Ασφαλείας

Θα πρέπει να υλοποιείται κάποια συγκεκριμένη πολιτική ασφαλείας. Μια πολιτική ασφαλείας θα πρέπει να καθορίζει:

- Ποια ομάδα ή ποιο άτομο είναι υπεύθυνο για την εφαρμογή της πολιτικής ασφαλείας.

- Ρόλους και ευθύνες.
- Διαχείριση Κινδύνων.
- Ταξινόμηση της πληροφορίας.
- Φυσική Ασφάλεια.
- Έλεγχο Πρόσβασης.
- Κανόνες Συμμόρφωσης.

Από τα παραπάνω, γίνεται κατανοητό ότι θα πρέπει να προσεχθεί ιδιαιτέρως το κομμάτι της ασφαλούς επικοινωνίας με την χρήση των κατάλληλων πρωτοκόλλων, τα οποία πρόκειται να αναλυθούν στο Κεφάλαιο 2.[3][8][26][33]

1.5 Ζητήματα ασφαλείας στην τηλεδιάσκεψη

Παρακάτω θα γίνει παρουσίαση των κυριότερων επιθέσεων χρησιμοποιώντας την ταξινόμηση του VoIP Security Alliance (VoIPSA).

1.5.1 Κοινωνικές απειλές

1.5.1.α SPIT

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

Στις κλασικές τηλεπωλήσεις, χρησιμοποιούνται auto - dialers, οι οποίοι καλούν νούμερα μέχρι να σηκώσει το τηλέφωνο κάποιος. Το SPIT είναι σαν τις τηλεπωλήσεις, αλλά με αρκετά μεγαλύτερη συχνότητα και μπορεί να συγκριθεί με την συχνότητα του SPAM. Οι τηλεπωλήσεις είναι ενοχλητικές, αλλά η συχνότητα των τηλεφωνημάτων συγκρινόμενη με το SPAM είναι πολύ μικρή.[3][8]

1.5.1.β Email spam (spam) εναντίον voice spam (spit).

Κοινά χαρακτηριστικά:

- Κοινά κίνητρα, π.χ. αναζήτηση οικονομικού κέρδους ή άσκησης επιρροής.
- Κοινές τεχνικές δημιουργίας, π.χ. αυτόματη παραγωγή μαζικών μηνυμάτων / κλήσεων χαμηλού κόστους, χρήση πραγματικών διευθύνσεων τελικών χρηστών, συλλογή διευθύνσεων κλπ.

Διαφορές:

- Η επικοινωνία με ηλεκτρονικό μήνυμα είναι ουσιαστικά ασύγχρονη, ενώ η VoIP επικοινωνία είναι κυρίως σύγχρονη στις διάφορες φάσεις των συνόδων.
- Στο περιβάλλον VoIP, μη εύλογες καθυστερήσεις δεν είναι (ούτε) τεχνικά αποδεκτές.
- Το email spam αποτελείται κυρίως από κείμενο, ίσως και εικόνες, ενώ το SPIT κυρίως από ήχο και εικόνα και πολύ λιγότερο από κείμενο.
- Μια SPIT κλήση συχνά δημιουργεί εντονότερη ενόχληση στο χρήστη.[3][8]

1.5.2 Υποκλοπές

Σε αυτή την επίθεση χρησιμοποιούνται τα εργαλεία σύλληψης και ανάλυσης της κίνησης του δικτύου, όπως το Ethereal, για να κάνει εξέταση στα μηνύματα σηματοδοσίας και τα πολυμεσικά ρεύματα σε μια συνομιλία. Τα συλληφθέντα RTP πακέτα, που ανταλλάσσονται από τα UDP ή TCP πρωτόκολλα, αποκωδικοποιούνται και μετατρέπονται σε αρχεία ήχου. Η διαδικασία που ακολουθείται για την σύλληψη και την αποκωδικοποίηση των πακέτων φωνής είναι η εξής:

- Πρώτα συλλαμβάνονται και αποκωδικοποιούνται τα RTP πακέτα.
- Έπειτα, η σύνοδος αναλύεται με την επιλογή ενός ρεύματος προς ανάλυση και επανασυναρμολόγηση με το κατάλληλο εργαλείο ανάλυσης.
- Τέλος το ρεύμα μπορεί τώρα να μετατραπεί σε αρχείο ήχου.

Υπάρχουν 4 βασικές επιθέσεις υποκλοπής, οι οποίες θα αναλυθούν στην συνέχεια, είναι οι: εξέταση του αρχείου διαμόρφωσης TFTP, εύρεση αριθμού, αναζήτηση αναγνώρισης κλήσης και παρακολούθησης συνομιλίας. Για να πραγματοποιηθούν αυτές οι επιθέσεις, ο επιτιθέμενος χρειάζεται να αποκτήσει πρόσβαση στο σημείο του δικτύου που βρίσκεται η VoIP κίνηση. Αυτό μπορεί να γίνει από παντού, από ένα

τελικό σημείο VoIP (υπολογιστή με softphone ή τηλέφωνο) μέχρι και μέσω πρόσβασης στο VoIP proxy / gateway μέσω ασύρματου δικτύου.[3][8]

1.5.2.α Εξέταση του αρχείου διαμόρφωσης TFTP

Τα περισσότερα IP τηλέφωνα βασίζονται σε ένα TFTP εξυπηρετητή για να κατεβάσουν το αρχείο ρυθμίσεων τους όταν ενεργοποιούνται. Αυτό συχνά περιέχει κωδικούς για να συνδεθούμε απευθείας στο τηλέφωνο (με telnet, web interface κ.α.) και να το διαχειριστούμε. Ο επιτιθέμενος που παρακολουθεί την κίνηση όταν ένα τηλέφωνο κατεβάζει αυτό το αρχείο μπορεί να μάθει αυτούς τους κωδικούς ώστε να ρυθμίσει εκ νέου και να ελέγξει το IP τηλέφωνο.[3][8]

1.5.2.β Εύρεση αριθμού

Ο επιτιθέμενος παρακολουθεί παθητικά όλες τις εισερχόμενες και εξερχόμενες κλήσεις για να δημιουργήσει μια βάση δεδομένων με τους τηλεφωνικούς αριθμούς ή τις επεκτάσεις τους σε ένα οργανισμό. Αυτή η βάση μπορεί να χρησιμοποιηθεί για πιο προχωρημένες επιθέσεις VoIP, όπως χειρισμό σηματοδότησης.[3][8]

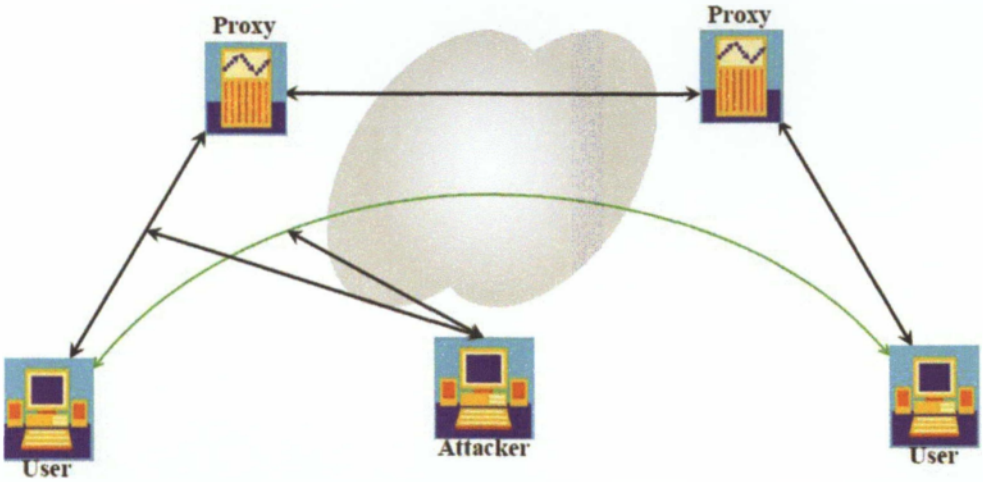
1.5.2.γ Αναζήτηση αναγνώρισης κλήσης

Αυτή η επίθεση πάει ένα βήμα παραπέρα από την εύρεση αριθμού για να δει ποιος μιλάει με ποιόν, ακόμα και αν η συνομιλία είναι κρυπτογραφημένη.[3][8]

1.5.2.δ Παρακολούθηση συνομιλίας και ανάλυση

Αυτή η επίθεση περιγράφει έναν επιτιθέμενο, ο οποίος ηχογραφεί έναν ή και τους δύο συνομιλητές σε μια συνομιλία. Πέρα από ότι μπορεί απλά να ακούσει τη συνομιλία, μπορεί με τη χρήση κατάλληλων εργαλείων να μεταφράσει τους ηχητικούς τόνους που πατήθηκαν στη κλήση. Συλλαμβάνοντας αυτή τη πληροφορία, ο επιτιθέμενος θα

είναι σε θέση να χρησιμοποιήσει αυτούς τους αριθμούς για να αποκτήσει πρόσβαση σε αυτόν τον λογαριασμό μέσω τηλεφώνου.[3][8][25]

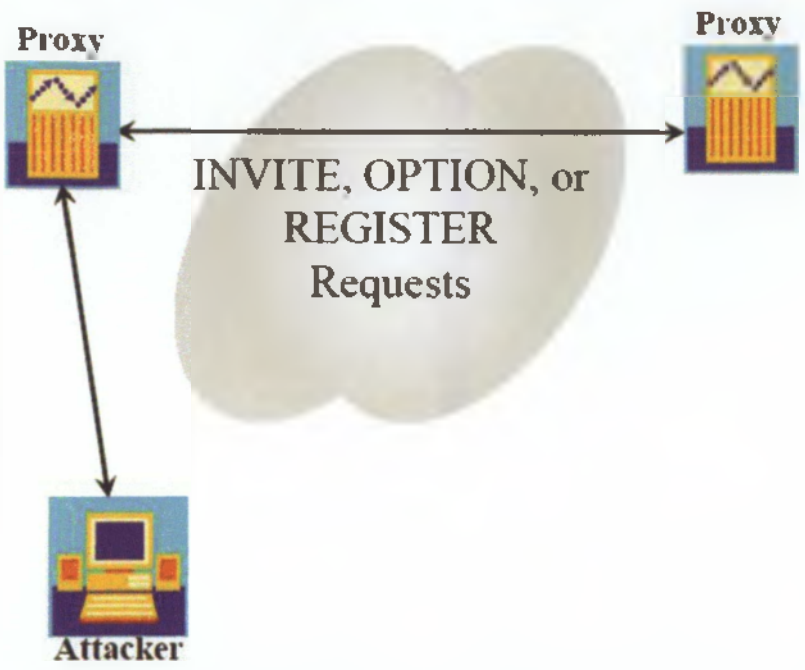


Εικόνα 2: Σχεδιάγραμμα παρακολούθησης συνομιλίας

1.5.3 Σκόπιμη διακοπή υπηρεσιών

1.5.3.α Άρνηση εξυπηρέτησης υπηρεσιών

Οι επιτιθέμενοι μπορούν να κάνουν κακή χρήση του πρωτοκόλλου σηματοδοσίας για να διεξάγουν επιθέσεις άρνησης εξυπηρέτησης υπηρεσιών. Στην πρώτη περίπτωση, οι επιτιθέμενοι μπορούν να δημιουργήσουν ένα μεγάλο αριθμό αιτημάτων εγκατάστασης κλήσης, που θα καταναλώνουν τη δύναμη επεξεργασίας του ενδιάμεσου διακομιστή. Στη δεύτερη περίπτωση, οι επιτιθέμενοι χρησιμοποιούν την ακύρωση των εκκρεμών σημάτων εγκατάστασης κλήσης συμπεριλαμβανομένης της αποστολής των CANCEL, GOODBYE ή PORT UNREACHABLE μηνυμάτων. Αυτό καθιστά το τηλέφωνο να μην είναι σε θέση να ολοκληρώσει τις κλήσεις ή να κλείσει. Ο συγκεκριμένος τύπος επίθεσης βοηθιέται από την πολυπλοκότητα των πρωτοκόλλων σηματοδοσίας.



Εικόνα 3: Σχεδιάγραμμα επίθεσης διακοπής υπηρεσιών

Επιθέσεις κατακλυσμού UDP

Λόγω του ότι η διεύθυνση της πηγής του UDP πακέτου μπορεί να πλαστογραφηθεί, αυτή η επίθεση προτιμάται για να πραγματοποιηθεί κατακλυσμός εύρους ζώνης. Η πλαστογράφηση επιτρέπει στον επιτιθέμενο να προσπεράσει τα τείχη προστασίας και άλλες συσκευές φιλτραρίσματος.

Επιθέσεις κατακλυσμού TCP SYN

Οι επιθέσεις κατακλυσμού TCP SYN καταστρέφουν τη χειραψία τριπλής κατεύθυνσης για να κατακλύσει ένα στόχο με διαχείριση σύνδεσης. Σε αυτή την επίθεση, ο επιτιθέμενος στέλνει έναν κατακλυσμό από πακέτα SYN με πλαστογραφημένη IP διεύθυνση πηγής. Το θύμα απαντάει με ένα SYN-ACK στον αποστολέα (ο οποίος δεν υπάρχει). Για να μπορέσει να ολοκληρωθεί η TCP σύνδεση, το θύμα περιμένει για μια χρονική περίοδο για ένα ACK πακέτο από τη πηγή. Αυτό το πακέτο δε στέλνεται ποτέ με αποτέλεσμα ο πίνακας συνδέσεων του θύματος να γεμίζει και να καταναλώνει όλους τους διαθέσιμους πόρους με αυτές τις άκυρες αιτήσεις. Σαν αποτέλεσμα έχουμε έναν διακομιστή, τηλέφωνο ή δρομολογητή που δε μπορεί να ξεχωρίσει τα DoS πακέτα από τα γνήσια SYN για τις πραγματικές VoIP συνδέσεις.

Επιθέσεις κατακλυσμού ICMP και Smurf

Μια πιο κακή χρήση του είναι η πλαστογράφηση της ταυτότητας την IP διεύθυνσης της πηγής και τον έλεγχο διευθύνσεων εκπομπής σε μια ποικιλία δικτύων που επιτρέπουν εκπομπές οδηγούμενες από IP. Αυτό ονομάζεται επίθεση smurf και περιλαμβάνει έναν κατακλυσμό από γνήσιες ICMP απαντήσεις από αυτά τα δίκτυα στο θύμα που πλαστογραφήθηκε. Κατακλύζοντας το εύρος ζώνης του δικτύου του θύματος με πλαστές ICMP απαντήσεις, οι περισσότερες εφαρμογές Internet θα καταρρεύσουν υπό αυτήν την επίθεση.

Σκουλήκια Και Ιοί υπερκάλυψης

Υπερκάλυψη σημαίνει ότι οι ανάγκες των εφαρμογών για εύρος ζώνης έχουν υπερβεί τις δυνατότητες του δικτύου. Αυτό μπορεί να προκύψει από επιθέσεις κατακλυσμού DoS ή φτωχή διαχείριση QoS. Το ξέσπασμα των σκουληκιών και των ιών στο δίκτυο μπορεί να καταναλώσει όλο το διαθέσιμο εύρος ζώνης σαν παρενέργεια του σαρώματος για άλλους ευαίσθητους πελάτες προκειμένου να τους μολύνει.[3][8][25]

1.5.3.β Επιθέσεις παράνομης εγγραφής

Η επίθεση παράνομης εγγραφής συμβαίνει όταν ένας επιτιθέμενος μιμείται έναν έγκυρο χρήστη σε έναν αιτούντα και αντικαθιστά τη νόμιμη εγγραφή με τη δική του διεύθυνση. Αυτή η επίθεση αναγκάζει τις εισερχόμενες κλήσεις προοριζόμενες για τον χρήστη να σταλθούν στον απατεώνα.[3][8][30]

1.5.3.γ Επιθέσεις υπογραφής μηνύματος

Η επίθεση υπογραφής μηνύματος πραγματοποιείται όταν ένας επιτιθέμενος παρεμποδίζει και τροποποιεί τα πακέτα που ανταλλάσσονται μεταξύ των SIP τμημάτων. Η υπογραφή μηνύματος μπορεί να πραγματοποιηθεί μέσω της παράνομης εγγραφής, της ενδιάμεσης πλαστογραφίας, ή μιας επίθεσης σε οποιοδήποτε έμπιστο συστατικό που επεξεργάζεται τα μηνύματα, όπως ο ενδιάμεσος διακομιστής, η πύλη πολυμέσων, ή το τείχος προστασίας.[3][8]

1.5.3.δ Επιθέσεις κατάρρευσης συνεδρίας

Η επίθεση κατάρρευσης συνεδρίας πραγματοποιείται όταν ένας επιτιθέμενος παρατηρεί τη σηματοδοσία για μια κλήση, και έπειτα στέλνει παραποιημένα BYE αιτήματα στους συμμετέχοντες χρήστες. Οι περισσότεροι χρήστες δεν απαιτούν ισχυρή αυθεντικοποίηση, γεγονός που επιτρέπει σε έναν επιτιθέμενο να στείλει κατάλληλα επεξεργασμένα BYE αιτήματα στους δύο χρήστες, τερματίζοντας βιαίως την κλήση.[3][8]

1.5.4 Παρακολούθηση και τροποποίηση

1.5.4.α Επιθέσεις ενδιάμεσης πλαστογραφίας

Η επίθεση ενδιάμεσης πλαστογραφίας εμφανίζεται όταν ένας επιτιθέμενος εξαπατά έναν από τους χρήστες ή τους ενδιάμεσους διακομιστές ώστε να επικοινωνήσουν με ένα διακομιστή απατεώνων.[3][8]

1.5.4.β Επίθεση επανεκπομπής

Μια επίθεση με τη βοήθεια των εργαλείων εξέτασης πάνω στα πακέτα ενός δικτύου μπορεί να πραγματοποιήσει επιθέσεις επανεκπομπής με τη σύλληψη πληροφοριών σε μια σύνοδο επικοινωνίας. Οι πληροφορίες που συλλαμβάνονται μπορούν να αναμεταδοθούν άθικτες ή τροποποιημένες για να επιτύχουν έναν σκοπό.[3][8]

Κεφάλαιο 2: Πρωτόκολλα τηλεδιάσκεψης

Τα πρωτόκολλα που αναπτύχθηκαν και καθιερώθηκαν και προσφέρουν την δυνατότητα για τηλεδιασκέψεις και όχι μόνο είναι το SIP και το H.323. Κάθε ένα από αυτά διαθέτει την δική του ανάλυση και τους δικούς του όρους επικοινωνίας. Είναι γραμμένο αναλυτικά, ενώ συνεχώς ορισμένα από αυτά ενημερώνονται και αναπτύσσονται. Η επίτευξη μετάδοσης του ήχου σίγουρα και προαιρετικά της εικόνας και των δεδομένων δεν γίνεται πάντα με τους ίδιους τρόπους, ενώ υπάρχει περίπτωση όπου τα πρωτόκολλα αυτά να μην είναι ανοιχτά προς την επιστημονική κοινότητα αλλά διατηρούν κλειστό τον πηγαίο κώδικά τους.

2.1 SIP

2.1.1 Παρουσίαση-Ανάλυση

Το Session Initiation Protocol (SIP), το οποίο δημιουργήθηκε από την IETF, είναι ένα πρωτόκολλο σηματοδοσίας που χρησιμοποιείται για τη δημιουργία συνόδων σε ένα IP δίκτυο. Η σύνοδος θα μπορούσε να είναι μια απλή αμφίδρομη τηλεφωνική κλήση ή θα μπορούσε να είναι μια συνδιάσκεψη συνόδου πολυμέσων. Η ικανότητα για τη δημιουργία αυτών των συνόδων, σημαίνει ότι μια σειρά από καινοτόμες υπηρεσίες μπορούν να καταστούν δυνατές.

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

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

Το SIP είναι ένα ερωτο - απόκριση πρωτόκολλο, που μοιάζει με δύο άλλα πρωτόκολλα του διαδικτύου, τα HTTP και SMTP, με συνέπεια να ταιριάζει άνετα δίπλα σε άλλες εφαρμογές διαδικτύου. Χρησιμοποιώντας το SIP, η τηλεφωνία γίνεται άλλη μια Web εφαρμογή και ενσωματώνεται εύκολα σε άλλες υπηρεσίες του διαδικτύου. Το SIP είναι μια απλή εργαλειοθήκη όπου οι πάροχοι υπηρεσιών

μπορούν να χρησιμοποιήσουν για την οικοδόμηση υπηρεσιών φωνής και πολυμέσων. Τέλος για να καταστεί δυνατή η τηλεφωνική επικοινωνία, το SIP χρειάζεται να συνεργαστεί με άλλα πρωτόκολλα όπως:

- για την εξασφάλιση μεταφοράς (RTP),
- για την συμφωνία των παραμέτρων της κλήσης (SDP),
- για τον έλεγχο ταυτότητας των χρηστών (ακτίνα, διάμετρος),
- να παρέχουν καταλόγους (LDAP),
- να είναι σε θέση να εγγυάται ποιότητα φωνής (RSVP, YESSIR) και διασυνεργασίας με τη σημερινή του τηλεφωνικού δικτύου.[9][10][15][23][24]

2.1.2 Λειτουργία

Διευθυνσιοδότηση SIP και εύρεση διακομιστή (server)

Το SIP χρησιμοποιεί διευθύνσεις σαν του email με τη μορφή user@domain, user@host, user@ip_address, phonenumber@gateway επειδή είναι η πιο κοινή μορφή διευθυνσιοδότησης στο διαδίκτυο. Με μια σειρά από DNS ελέγχους όπως αναζήτηση υπηρεσίας (searching of service, SRV), όπου βρίσκεται ο διακομιστής στον οποίο «ανήκει» ο κληθείς χρήστης. Ένα ακόμα πλεονέκτημα της μορφής αυτής, είναι ότι εύκολα μπορεί να μετατραπεί σε URI (uniform resource identifier), όπως sip:mkour@auth.gr. Το πλεονέκτημα είναι ότι με τον τρόπο αυτό μπορεί εύκολα να ενσωματωθεί σε μια ιστοσελίδα, έτσι ώστε ενεργοποιώντας μια σύνδεση να ξεκινάει η κλήση, όπως γίνεται στο mailto:URL.

Ο διακομιστής μπορεί να είναι είτε ενδιάμεσος είτε επανακατευθυνόμενος ανακατευθύνοντας την κλήση. Η διαδικασία εύρεσης του επόμενου διακομιστή είναι γνωστή σαν δρομολόγηση επόμενου βήματος. Υπάρχει περίπτωση κατά τη διαδικασία αυτή, ένας διακομιστής να βρει ότι πολλοί διακομιστές σε απόσταση ενός βήματος μπορούν να επικοινωνήσουν με το χρήστη που καλείται. Το SIP δίνει τη δυνατότητα σε έναν ενδιάμεσο διακομιστή να στείλει παράλληλα το ίδιο εισερχόμενο αίτημα σε πολλούς διακομιστές σε απόσταση ενός βήματος.

Συναλλαγές SIP

Αφού βρεθεί ποιος είναι ο τερματικός πομπός του κληθέντος χρήστη, όλα τα αιτήματα στέλνονται εκεί. Όπως αναφέραμε, κάθε αίτημα μαζί με τις αποκρίσεις που προκαλεί σχηματίζουν μια συναλλαγή SIP. Τα αιτήματα μπορούν να σταλούν είτε μέσω TCP είτε μέσω UDP.

Αν χρησιμοποιηθεί ένα αξιόπιστο πρωτόκολλο (TCP), τότε όλα τα μηνύματα της ίδιας συναλλαγής μεταφέρονται μέσω της ίδιας σύνδεσης. Αν όμως χρησιμοποιηθεί το UDP, ο δέκτης user agent στέλνει την απόκριση με βάση τις πληροφορίες που περιέχει το πεδίο Via στην επικεφαλίδα του αιτήματος. Σε πρωτόκολλα με την τεχνική αυτοτελών πακέτων πληροφορίας, η αξιοπιστία επιτυγχάνεται μέσω επαναποστολής.

Πρόσκληση SIP

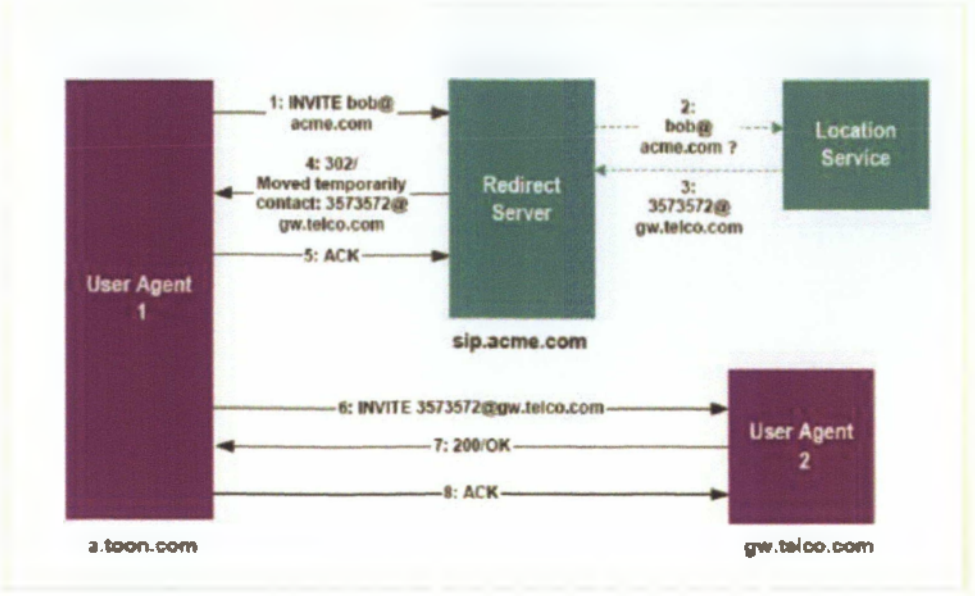
Μια πετυχημένη πρόσκληση αποτελείται από δυο αιτήματα, ένα INVITE ακολουθούμενο από ACK. Το INVITE ζητά από το χρήστη που καλείται να πάρει μέρος σε μια διάσκεψη ή σε μια απλή συνομιλία. Αφού συμφωνήσει να λάβει μέρος, ο χρηστής που έκανε την κλήση επιβεβαιώνει ότι έλαβε την απάντηση στέλνοντας ένα μήνυμα ACK. Το μήνυμα INVITE περιέχει μια περιγραφή της συνόδου ώστε να παρέχει τις απαραίτητες πληροφορίες στο χρήστη που καλείται για να συμμετάσχει στη σύνοδο. Αν ο καλούμενος χρήστης θέλει να δεχτεί την κλήση στέλνει ένα μήνυμα με μια παρόμοια περιγραφή.

Εντοπισμός Χρηστή

Η τοποθεσία του καλούμενου χρήστη μπορεί να αλλάζει με το χρόνο. Αυτές οι τοποθεσίες μπορούν να εγγράφονται δυναμικά σε ένα SIP διακομιστή. Όταν θα ερωτηθεί για κάποιο χρήστη, επιστρέφει μια λίστα με όλες τις πιθανές τοποθεσίες. Το τμήμα που επιτελεί αυτή τη λειτουργία μέσα σε ένα διακομιστή (server) λέγεται διαχειριστής θέσης.

Αλλαγή υπάρχουσας συνόδου

Σε κάποιες περιπτώσεις μπορεί να χρειαστεί να αλλάξουν κάποιες παράμετροι μιας συνόδου. Αυτό γίνεται στέλνοντας ένα νέο μήνυμα INVITE με το ίδιο call-id και με περιεχόμενο τις νέες παραμέτρους. Το μήνυμα αυτό πρέπει να έχει μεγαλύτερο CSeq από κάθε προηγούμενο αίτημα του πελάτη στο διακομιστή.[10][19][23][24]



Εικόνα 4 :Λειτουργία του SIP

2.1.3 Ασφάλεια

Τα μηνύματα SIP μπορεί να περιέχουν ευαίσθητες πληροφορίες. Ακόμα, στο σώμα του μηνύματος μπορεί να υπάρχει το κλειδί της κωδικοποίησης της συνόδου. Το SIP υποστηρίζει δύο συμπληρωματικές υπηρεσίες για την προστασία των δεδομένων:

Κρυπτογράφηση για όλη τη διαδρομή

Η κρυπτογράφηση βασίζεται σε κλειδιά που έχουν οι χρήστες. Κάθε μήνυμα στέλνεται κωδικοποιημένο με το κλειδί του παραλήπτη, έτσι ώστε μόνο αυτός να μπορεί να το διαβάσει. Πρέπει να σημειωθεί ότι δεν κωδικοποιείται ολόκληρο το μήνυμα. Κάποια πεδία της επικεφαλίδας πρέπει να είναι «ελευθέρα», γιατί τα δεδομένα που περιέχουν είναι απαραίτητα στους ενδιάμεσους διακομιστές. Όλες οι υλοποιήσεις πρέπει να υποστηρίζουν κωδικοποίηση PGP (pretty good privacy).

Κρυπτογράφηση ανά βήμα

Με τη μέθοδο αυτή, μπορούμε να κωδικοποιήσουμε ολόκληρο το μήνυμα. Έτσι, κανονικά, δεν αποκαλύπτονται σε κακόβουλους χρήστες οι διευθύνσεις των ατόμων που συνομιλούν. Αλλά αυτό δεν συμβαίνει. Τα δεδομένα αυτά είναι γνωστά στους ενδιάμεσους διακομιστές (για να γίνει η δρομολόγηση) και συνεπώς μπορούν βρεθούν μέσω της ανάλυσης της κίνησης που περνάει από το διακομιστή. Ακόμα και έτσι όμως, η παρεχόμενη ασφάλεια είναι ικανοποιητική. Η μέθοδος αυτή μπορεί να

χρησιμοποιηθεί ακόμα και αν το μήνυμα έχει αρχικά κωδικοποιηθεί με βάση την κρυπτογράφηση για όλη τη διαδρομή.[16][19][20][27]

2.1.4 Αναφορές Προβλημάτων

Το SIP είναι ένα βασικό πρωτόκολλο για δίκτυα πραγματικού χρόνου επικοινωνίας, συμπεριλαμβανόμενων VoIP και IMS δικτύων. Είναι βασισμένο σε IP, οπότε είναι εξίσου ευπαθή σε επιθέσεις άρνησης εξυπηρέτησης υπηρεσιών που δέχονται οι SIP διακομιστές.

Βομβαρδισμός

Η επίθεση αυτή περιλαμβάνει τη διαβίβαση μιας μεγάλης ποσότητας από πλαστά SIP μηνύματα σε ένα στοχοθετημένο σύστημα. Η τηλεφωνία μέσω IP είναι πολύ ευαίσθητη σε θέματα διαθεσιμότητας. Μια μεγάλη ποσότητα από ψεύτικα SIP μηνύματα απαιτεί την κατανομή των υπολογιστικών πόρων για την αποκωδικοποίηση και την ερμηνεία τους. Καθώς το σύστημα είναι απασχολημένο με την επεξεργασία και την αντιμετώπιση των ψεύτικων μηνυμάτων, τα έγκυρα μηνύματα θα επεξεργάζονται με χαμηλότερο ρυθμό από τον οποίο θα έπρεπε να επεξεργάζονται από το σύστημα. Αυτός ο τύπος επίθεσης έχει ήδη δοκιμαστεί με επιτυχία σε VoIP συσκευές.

SIP μηνύματα και επιθέσεις πλημμύρας

Το SIP πρωτόκολλο είναι βασισμένο σε κείμενο, οπότε υπάρχουν αρκετά είδη επίθεσης μηνυμάτων πλημμύρας. Οι πιο σημαντικές από αυτές είναι: η πρόσκληση πλημμύρας, η εγγραφή πλημμύρας και η εγγραφή απάντηση πλημμύρας. Σύμφωνα με την πρώτη, ο επιτιθέμενος στέλνει ένα μεγάλο αριθμό SIP μηνυμάτων με μία πλαστή IP διεύθυνση προς το θύμα αναγκάζοντας τον να καταναλώσει πόρους για την επεξεργασία των εισερχόμενων μηνυμάτων. Η επίθεση εγγραφής λειτουργεί παρόμοια με την προηγούμενη επίθεση, αλλά χρησιμοποιεί αντί για μηνύματα πρόσκλησης, μηνύματα εγγραφής. Σύμφωνα με την τελευταία επίθεση, ο επιτιθέμενος στέλνει ένα μεγάλο ποσό εγγραφής μηνύματα με λάθος τα διαπιστευτήριά του προς πληρεξούσιο διακομιστή για να το συντρίψει. Υπάρχουν τρεις κύριες πηγές που μπορούν να στοχευθούν από μια SIP επίθεση πλημμύρας: το εύρος, η ΚΜΕ και η μνήμη.

Εύρος

Ο στόχος είναι πλημμυρισμένος με περισσότερα μηνύματα από ότι το δίκτυο μπορεί να χειριστεί, π.χ. ο εισβολέας καταφέρνει να δημιουργήσει μια επίθεση με ποσοστό 10 GB/s, ενώ ο στόχος είναι συνδεδεμένος με διαδίκτυο μέσω γραμμής 1 GB/s.

KME

Ο στόχος είναι πλημμυρισμένος με περισσότερα μηνύματα από ότι μπορεί να επεξεργαστεί σε μία δεδομένη χρονική στιγμή, καθότι το SIP είναι πρωτόκολλο βασισμένο σε κείμενο, πρέπει να αναλύσει κάθε εισερχόμενο μήνυμα.

Μνήμη

Πολλές SIP αιτήσεις δημιουργούν καταστάσεις λειτουργίας στον στόχο. Ένα μήνυμα πρόσκλησης στέλνεται στον ενδιάμεσο διακομιστή και περιμένει μερικά δευτερόλεπτα για μια απάντηση. Κατά τη διάρκεια αυτής της κατάστασης καταναλώνεται μνήμη στον ενδιάμεσο. Εάν λοιπόν ο ενδιάμεσος αντιμετωπίζει μια πληθώρα τέτοιων μηνυμάτων κάποια στιγμή θα εξαντληθεί η μνήμη που έχει στη διάθεση του, με αποτέλεσμα να υπολειτουργήσει αν όχι να καταρρεύσει. Μια πλημμύρα μπορεί να επιτευχθεί με διαφορετικά SIP μηνύματα.

TCP SYN και TCP/ACKs πλημμύρας

Η γνωστή κατηγορία των επιθέσεων επιτυγχάνει τους στόχους της, με το να δημιουργεί μισάνοιχτες συνδέσεις στο θύμα. Μια τέτοια κατάσταση εμφανίζεται, όταν ο διακομιστής στείλει ένα μήνυμα SYN - ACK, αλλά ποτέ δεν λαμβάνει ένα μήνυμα ACK από τον χρήστη. Συγκεκριμένα, ο εισβολέας στέλνει ένα πλαστό SYN πακέτο με μία απρόσιτη IP διεύθυνση προέλευσης. Κατά την υποδοχή, το θύμα θα απαντήσει με ένα μήνυμα SYN - ACK, αλλά το δίκτυο δεν είναι σε θέση να το δρομολογήσει. Ως εκ τούτου, το θύμα δεν λαμβάνει ποτέ ACK μήνυμα που να ανταποκρίνεται στο δικό του SYN - ACK. Ακόμα χειρότερα, η μνήμη που διατίθεται για αναμονή της σύνδεσης μπορεί να αποδεσμευτεί μόνο όταν η TCP σύνδεση γίνει timeout. Μια παρόμοια επίθεση με TCP SYN είναι το TCP / ACKs πλημμύρα. Για την μεγιστοποίηση των συνεπειών μπορεί ο κακόβουλος να χρησιμοποιήσει και τις δύο επιθέσεις παράλληλα.

Επιθέσεις προς αναλυτές μηνυμάτων

Καθώς το SIP πρωτόκολλο είναι βασισμένο σε απλό κείμενο με ένα υψηλό βαθμό ελευθερίας, ένας αποτελεσματικός αναλυτής αναλύει τα μηνύματα που λαμβάνει μέχρι το σημείο των πληροφοριών που απαιτούνται. Ωστόσο, ακόμη και ένα πλήρες SIP μήνυμα μπορεί να κατασκευαστεί με τρόπο που να παρεμποδίζει την ορθή ανάλυση. Για παράδειγμα, ένας εισβολέας μπορεί να δημιουργήσει αδικαιολόγητα μεγάλα μηνύματα με απλό τρόπο, με την προσθήκη επιπλέον κεφαλίδων, σε συνδυασμό με ένα μεγάλο μήνυμα - σώματος. Έτσι, αντί να καταστρέφουν μόνο την ενέργεια του επεξεργαστή, τα μεγάλα μηνύματα αυξάνουν σε χρόνο την χρήση του δικτύου και του καταναλώνουν περισσότερη μνήμη.[4][14]

2.2 H.323

2.2.1 Παρουσίαση-Ανάλυση

Η σειρά συστάσεων H.323 καθορίζει τις τερματικές συσκευές, τον εξοπλισμό και τις υπηρεσίες που απαιτούνται για την επικοινωνία με χρήση πολυμέσων σε πραγματικό χρόνο, πάνω από τοπικά δίκτυα τα οποία δεν παρέχουν εξασφαλισμένη ποιότητα επικοινωνίας, ή δίκτυα μεταγωγής πακέτων. Το τοπικό δίκτυο μπορεί να είναι απλό τμήμα (π.χ. δακτύλιος), ή μια πιο σύνθετη τοπολογία που αποτελείται από πολλά τμήματα διαφόρων ειδών (ακόμα και όλο το διαδίκτυο), και αυτός είναι και ο λόγος της αδυναμίας εξασφάλισης μιας ελάχιστης ποιότητας επικοινωνίας. Οι τερματικές συσκευές που ακολουθούν τη σύσταση H.323 μπορεί να είναι ενσωματωμένες σε ένα προσωπικό υπολογιστή, ή να είναι ανεξάρτητες (π.χ. βιντεοτηλέφωνα).

Η υποστήριξη φωνής είναι απαραίτητη, ενώ η υποστήριξη μετάδοσης δεδομένων και κινούμενης εικόνας είναι προαιρετική, αλλά από τη στιγμή που θα υποστηρίζονται θα πρέπει να ακολουθείται κάποια κοινή μέθοδος λειτουργίας για τη συνεργασία των τερματικών συσκευών που παρέχουν τη δυνατότητα αυτή. Η σειρά συστάσεων H.323 επιτρέπει τη χρήση περισσότερων του ενός καναλιών επικοινωνίας, για κάθε είδος πληροφορίας που μεταδίδεται.

Η έκδοση 4 του H.323 περιέχει βελτιώσεις στην αξιοπιστία, τις δυνατότητες κλιμάκωσης και την ευελιξία του. Επίσης, εισήγαγε νέα χαρακτηριστικά, τα οποία

βοηθούν τη διευκόλυνση περισσότερο κλιμακούμενων λύσεων Gateway και MCU, ώστε να υπάρξει ανταπόκριση στις αυξανόμενες απαιτήσεις.

Επιπλέον, έχει δημοσιευτεί ένας αριθμός παραρτημάτων αναφορικά με το H.323. Το H.323 παραμένει το κύριο πρωτόκολλο για τηλεδιάσκεψη.[9][11][12][15][20]

2.2.2 Λειτουργία

Η είσοδος του H.323 αποτέλεσε λοιπόν μία ολοκληρωμένη πρόταση για τη δημιουργία ενός δικτυακού περιβάλλοντος που ενσωματώνει πολλαπλές παλαιές και νέες τεχνολογίες από διαφορετικούς κατασκευαστές σε ένα ενιαίο πλαίσιο διαχείρισης πληροφορίας φωνής και εικόνας. Το πρωτόκολλο αποτελείται από τέσσερα διαφορετικά κομμάτια:

1. Τερματικό

Πρόκειται για τα τελικά σημεία χρηστών, που υποστηρίζουν αμφίδρομη επικοινωνία, υποχρεωτικά επικοινωνιών φωνής και προαιρετικά εικόνας και δεδομένων. Το H.323 καθορίζει τον τρόπο με τον οποίο διαφορετικοί τερματικοί σταθμοί είναι δυνατό να επικοινωνήσουν. Τα τερματικά θα πρέπει συμπληρωματικά να υποστηρίζουν το H.245 που κατευθύνει τη χρήση των καναλιών επικοινωνίας μεταξύ τερματικών σταθμών, το Q.931 για κλήση και σηματοδότησης εγκατάστασης, το Registration / Admission / Status (RAS) για επικοινωνία με το Gatekeeper, καθώς επίσης και το Real Time Protocol (RTP) / Real-Time Control Protocol (RTCP) για την εν σειρά αποστολή και λήψη των πακέτων φωνής. Ειδικά για την περίπτωση της επικοινωνίας με φωνή, το πρότυπο G.711 για συμπίεση και απόδοση πακέτων με ρυθμούς 54 ή 64 kbps σε ένα τοπικό δίκτυο δεδομένων.

2. Gateway

Είναι το μοναδικό προαιρετικό στοιχείο του H.323 και παρέχει τόσο το φυσικό, όσο και η λογική διεπαφή μεταξύ των τηλεφωνικών συσκευών και του επικοινωνιακού δικτύου.

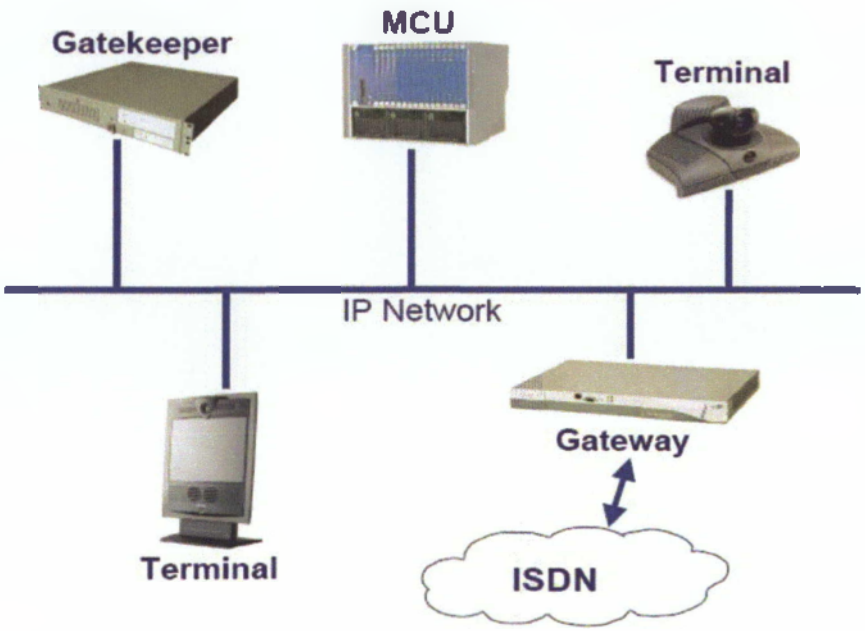
Χρησιμοποιείται συνήθως για τους παρακάτω λόγους:

- την επικοινωνία μεταξύ αναλογικών PSTN τερματικών,

- την επικοινωνία με απομακρυσμένους H.320 σταθμούς ISDN δικτύων,
- την επικοινωνία με απομακρυσμένους H.323 σταθμούς PSTN δικτύων.

Παρέχει συγκεκριμένες διεπαφές προς την PSTN υπηρεσία και χρησιμοποιεί CODECs για τη μετατροπή τηλεφωνικών κυκλωμάτων σε πακέτα δεδομένων, τα οποία σε συνεργασία με τον gatekeeper μέσω του RAS δρομολογεί στο δίκτυο όπου είναι βασισμένο σε IP.

Όπως προαναφέρθηκε, η ύπαρξη του Gateway δεν είναι υποχρεωτική στην περίπτωση που οι τερματικοί σταθμοί θέλουν να επικοινωνούν μεταξύ τους εντός του τοπικού και μόνο δικτύου και δεν ενδιαφέρονται για πρόσβαση εκτός αυτού.



Εικόνα 5:Οντότητες στο H.323

3. Gatekeeper

Η gatekeeper είναι ένα πολύ χρήσιμο, αλλά προαιρετικό στοιχείο ενός H.323 δικτύου. Οι gatekeepers εξασφαλίζουν ασφαλείς και εμπορικά εφικτές επικοινωνίες. Συχνά μία gatekeeper αναφέρεται ως ο εγκέφαλος του H.323 δικτύου, εξαιτίας της κεντρικής διαχείρισης και των υπηρεσιών ελέγχου που επιτελεί. Όταν υπάρχει μια gatekeeper όλες οι απολήξεις (τερματικά, gateways και MCUs) πρέπει να έχουν

καταγραφεί σε αυτή. Η gatekeeper και οι απολήξεις, τις οποίες διαχειρίζεται, σχηματίζουν μία ζώνη διαχείρισης. Κάθε gatekeeper παρέχει αρκετές υπηρεσίες σε όλες τις απολήξεις της ζώνης της. Αυτές οι υπηρεσίες περιλαμβάνουν:

Μετάφραση διεύθυνσης: μία gatekeeper διατηρεί μία βάση δεδομένων για μετάφραση ψευδωνύμων, όπως διεθνείς τηλεφωνικούς αριθμούς και δικτυακές διευθύνσεις.

Έλεγχο αποδοχής και πρόσβασης στις απολήξεις : αυτός ο έλεγχος μπορεί να βασίζεται στο διαθέσιμο εύρος ζώνης, στους περιορισμούς που υπάρχουν ως προς την ταυτόχρονη κλήση H.323 κλήσεων, ή στα προνόμια και τις προτεραιότητες των απολήξεων.

Διαχείριση εύρους ζώνης : Οι διαχειριστές του δικτύου μπορούν να διαχειρίζονται το εύρος ζώνης ορίζοντας συγκεκριμένους περιορισμούς στον αριθμό των παράλληλων κλήσεων, και περιορίζοντας συγκεκριμένα τερματικά από το να πραγματοποιούν κλήσεις σε συγκεκριμένα χρονικά διαστήματα.

Η ικανότητα δρομολόγησης : Μία gatekeeper μπορεί να δρομολογεί όλες τις κλήσεις που ξεκινούν ή τερματίζουν στη ζώνη της. Αυτή η δυνατότητα προσφέρει πολλά πλεονεκτήματα. Πρώτον, το γεγονός ότι "κρατά λογαριασμό" για πληροφορίες που αφορούν τις κλήσεις, μπορεί να φανεί χρήσιμο σε ότι αφορά τη χρέωση αλλά και την ασφάλεια του συστήματος. Δεύτερον, μία gatekeeper μπορεί να επανακατευθύνει μία κλήση στην κατάλληλη gateway ανάλογα με το διαθέσιμο εύρος ζώνης. Τρίτον, η επαναδρομολόγηση μπορεί να χρησιμοποιηθεί για την ανάπτυξη προχωρημένων υπηρεσιών, όπως η προώθηση γραμμής, και η εκτροπή φωνητικού ταχυδρομείου.

4. Multipoint Conference Unit (MCU)

Καθορίζει και ελέγχει την ταυτόχρονη διασύνδεση (συνεδρία) περισσότερων των δύο τερματικών σταθμών. Αποτελείται από δύο διακριτά τμήματα, τον Multipoint Controller (MC), η ύπαρξη του οποίου είναι αναγκαστική και κανένα ή περισσότερους του ενός Multipoint Processors (MP). Ο MC ελέγχει την H.245 συνεννόηση μεταξύ των τερματικών προκειμένου να καθοριστούν οι κοινές τους δυνατότητες για επικοινωνία, ενώ συμπληρωματικά ανακαλύπτει τους αποστολείς πολλαπλής εκπομπής πακέτων. Ο MP από την άλλη πλευρά είναι αυτός που

ασχολείται με την πραγματική ροή της φωνής ή του βίντεο, υλοποιώντας τεχνικές για ένωσης και προώθησης.

Πώς γίνεται η επικοινωνία

Το πρότυπο ορίζει, ότι τα απαραίτητα στοιχεία για την ύπαρξη επικοινωνίας με χρήση του Η.323 είναι η δυνατότητα παραγωγής και ελέγχου φωνής, το Q.931 εγκατάστασης κλήσης, η ύπαρξη RAS και η Η.245 σηματοδοσία.

Έλεγχος (Control)

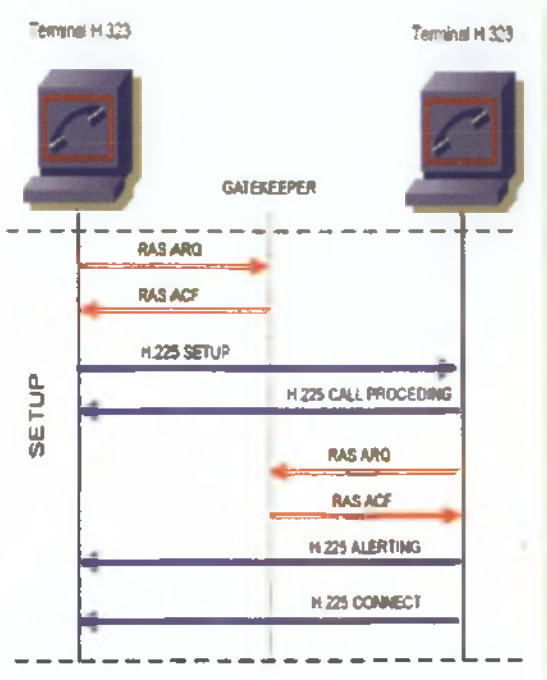
Είναι ίσως το πλέον ουσιαστικό από τα χαρακτηριστικά γνωρίσματα κάθε πρωτοκόλλου, γιατί περιλαμβάνει μία σειρά από διαδικασίες σηματοδοσίας που αφορούν εγκαθίδρυση και τερματισμό της επικοινωνίας και διερεύνηση των δυνατοτήτων που διαθέτει κάθε ένα εκ των συμμετεχόντων μελών. Το ουσιαστικό όμως είναι ότι όλες οι υπηρεσίες ελέγχου αποτελούν ένα ανεξάρτητο στρώμα (επίπεδο ελέγχου) υπό την καθοδήγηση του οποίου πραγματοποιούνται μία σειρά από αποφασιστικής σημασίας διεργασίες, όπως είναι αυτές της διαμόρφωσης, της σειριακής αριθμοδότησης, διόρθωσή σφαλμάτων και ανάγνωση σφαλμάτων.

Οι παραπάνω υπηρεσίες ελέγχου, εξυπηρετούνται όπως προαναφέρθηκε από τις παρακάτω τρεις διακριτές διαδικασίες ελέγχου.

α) Η.245 κανάλι ελέγχου: Είναι το κανάλι επικοινωνίας που συντονίζει όλες τις λειτουργίες ελέγχου μεταξύ των Η.323 τερματικών με δυνατότητα εγκατάστασης και τερματισμού ενός λογικού καναλιού επικοινωνίας, μεταφορά των μηνυμάτων ελέγχου ροής πακέτων και πάνω από όλα ικανότητα για υποστήριξη της βασικής λειτουργίας "ανταλλαγής ικανοτήτων" των τερματικών.

β) Q.931: Χρησιμοποιείται αποκλειστικά στην πρώιμη φάση εγκαθίδρυσης της επικοινωνίας μεταξύ των τερματικών σταθμών.

γ) RAS: Εκτελεί διαδικασίες που αφορούν σε εγγραφή, αποδοχή, περιγραφή κατάστασης και καθορισμού μεταβολής ρυθμού αποστολής/λήψης πακέτων μεταξύ των τερματικών και του gatekeeper.[20][37]



Εικόνα 6: Λειτουργία του H.323

2.2.3 Ασφάλεια

Το H.235 ασχολείται με την ασφάλεια και την κρυπτογράφηση του H.323 πρωτοκόλλου και χρησιμοποιεί αλγορίθμους προκειμένου να πετύχει την ασφάλεια στην μετάδοση δεδομένων ήχου και εικόνας.

Το H.235 είναι η σύσταση ασφαλείας για τα συστήματα πρωτοκόλλων της σειράς H.3XX. Ειδικά, το H.235 παρέχει διαδικασίες ασφάλειας για τα συστήματα που βασίζονται στα πρωτόκολλα H.323, H.225.0, H.245 και το H.460. Μπορεί να εφαρμοστεί σε απλή point-to-point τηλεδιάσκεψη καθώς και σε πολλαπλών σημείων σε οποιοδήποτε τερματικό που χρησιμοποιεί το H.245 ως πρωτόκολλο ελέγχου.

Στόχος του είναι να παρέχει αυθεντικοποίηση, ιδιωτικότητα και ακεραιότητα για τα συστήματα όπου βασίζονται στο H.323. Παρέχει δυνατότητα σε ένα άτομο, παρά σε μια συσκευή, να ταυτοποιηθεί. Τα προφίλ ασφάλειας περιλαμβάνουν:

1. Ένα απλό προφίλ ασφάλειας βασισμένο σε κωδικό πρόσβασης,
2. Ένα προφίλ που χρησιμοποιεί ψηφιακά πιστοποιητικά και εξαρτώμενο πλήρως από την χρήση της υποδομής δημοσίου κλειδιού, και
3. Το προφίλ που συνδυάζει τα δύο παραπάνω.

Η χρήση αυτών των προφίλ ασφάλειας είναι προαιρετική.

Το Η.235 περιέχει την δυνατότητα να διαπραγματεύεται υπηρεσίες και λειτουργικότητα σε γενικό τρόπο και μπορεί να είναι επιλέξιμο λαμβάνοντας υπόψιν τις τεχνικές και τις ικανότητες κρυπτογράφησης που χρησιμοποιούνται. Ο ειδικός τρόπος στον οποίο χρησιμοποιούνται συσχετίζει τις ικανότητες των συστημάτων, τις απαιτήσεις εφαρμογών και τους ειδικούς περιορισμούς της πολιτικής ασφαλείας. Το Η.235 υποστηρίζει διάφορους αλγορίθμους κρυπτογράφησης με κατάλληλες πολλαπλές επιλογές για διάφορους σκοπούς. Ορισμένοι αλγόριθμοι κρυπτογράφησης μπορούν να βρίσκονται σε συγκεκριμένες υπηρεσίες ασφαλείας.

Το Η.235 υποστηρίζει την σηματοδότηση των πολύ γνωστών αλγορίθμων καθώς και των μη καθορισμένων ή κατάλληλων κρυπτογραφικών αλγορίθμων. Δεν υπάρχουν ειδικά χρησιμοποιούμενοι αλγόριθμοι, παρόλα αυτά ισχυρά προτείνεται ότι τα σημεία τερματισμού υποστηρίζουν τους περισσότερους αλγορίθμους που εφαρμόζονται όσο το δυνατό περισσότερο με στόχο να επιτύχουν διαλειτουργικότητα. Αυτό συμβαδίζει με την έννοια ότι η υποστήριξη του Η.245 δεν εγγυάται την διαλειτουργικότητα μεταξύ δύο κωδικοποιητών οντοτήτων.

Δομή πρωτοκόλλου Η.235

Το Η.235 απαιτεί πολλά μηνύματα, διαδικασίες, δομές και αλγορίθμους για τα προβλήματα ασφαλείας της σηματοδότησης, του ελέγχου και των επικοινωνιών κάτω από την δομή του Η.323. Παρακάτω παρατίθεται μια περίληψη των ορισμών:

- Το κανάλι σηματοδότησης της κλήσης μπορεί να είναι ασφαλές χρησιμοποιώντας το TLS ή το IPSEC σε μία ασφαλή και γνωστή πύλη.
- Οι χρήστες μπορούν να αυθεντικοποιούνται είτε κατά την αρχική σύνδεση της κλήσης στην διαδικασία ασφάλειας του καναλιού Η.245 είτε στην ανταλλαγή πιστοποιητικών του Η.245.
- Οι ικανότητες κρυπτογράφησης ενός καναλιού ενημέρωσης καθορίζεται από την ύπαρξη ικανοτήτων του μηχανισμού διαπραγμάτευσης.
- Η αρχική κατανομή του υλικού των κλειδιών για το κύριο κλειδί είναι μέσω του Η.245 OpenLogicalChannel ή των μηνυμάτων OpenLogicalChannelAck.

- Η επαναδημιουργία κλειδιών μπορεί να επιτευχθεί στο H.245 με τις εντολές EncryptionUpdateCommand, EncryptionUpdateRequest, EncryptionUpdate και EncryptionUpdateAck
- Η κατανομή του υλικού των κλειδιών είναι προστατευμένη είτε με την χρήση του καναλιού H.245 ως ιδιωτικό κανάλι είτε με ειδική προστασία του υλικού των κλειδιών με την χρήση επιλεγμένων πιστοποιητικών ανταλλαγής.

Τα πρωτόκολλα ασφαλείας παρουσιάστηκαν σε συμμόρφωση με τα δημοσιευμένα διεθνή πρότυπα ή με τα προτεινόμενα πρότυπα.[20][31][37][38][39]

2.2.4 Αναφορές Προβλημάτων

Το H.323 είναι πολύ απαιτητικό στις θύρες (ports) απαιτώντας τέσσερις ροές UDP, δύο για RTP και δύο για RTCP, και επίσης υπάρχουν συγκεκριμένες κατευθυντήριες γραμμές για το που πρέπει να είναι οι θύρες αυτές. Οι θύρες RTP πρέπει να είναι σε θύρες με ζυγό αριθμό ενώ το RTCP σε μονό.

Το πρότυπο αυτό έχει ως στόχο να χειριστεί την διασύνδεση με αξιόπιστων δικτύων. Τα δίκτυα έχουν διαφοροποίηση βάσει του proxy που χρησιμοποιούν, δηλαδή SOCKS και FWTK. Όταν ένα δίκτυο χρησιμοποιεί proxy FWTK τότε το πρωτόκολλο H.323 μπορεί να χρησιμοποιηθεί με μεγαλύτερη ασφάλεια. Ενώ αντιθέτως, αν ένα δίκτυο χρησιμοποιεί το proxy SOCKS είναι περισσότερο ευπαθές. Για την αντιμετώπιση αυτού του θέματος, συστήνεται η χρήση τοίχους προστασίας (Firewall).

Η ομάδα ασφαλούς προγραμματισμού του πανεπιστημίου του Oulu έλεγξε τις δυνατότητες ασφάλειας της μεταφοράς πακέτων δεδομένων στο H.323 με την χρήση του πρωτοκόλλου H.225 για την μεταφορά και του H.245 για την ασφάλεια. Μετά την έρευνα, δημοσιοποίησαν ότι στο H.323 μπορούν να τροποποιηθούν τα πακέτα που στέλνονται και να είναι ευπαθή στα θέματα ασφαλείας, καθώς το πρωτόκολλο αυτό υλοποιείται σε εφαρμογές που είναι εγκατεστημένες στο εκάστοτε υπολογιστικό σύστημα. Τα υπολογιστικά συστήματα αυτά εξαρτώνται απόλυτα από τον χρήστη. Για τον λόγο αυτό η εγκατάσταση του πρωτοκόλλου H.323 θα πρέπει να γίνεται σε συστήματα τα οποία καλύπτουν τους βασικούς κανόνες ασφαλείας.[2][31][32]

2.3 Σύγκριση SIP και H.323

Στις προηγούμενες παραγράφους αναλύσαμε τα δύο πιο κύρια πρωτόκολλα που χρησιμοποιούνται σήμερα για VoIP κλήσεις και δυνητικά αυτά τα δύο έχουν τις δυνατότητες για πραγματοποίηση και video κλήσεων. Τα δυο πρωτόκολλα μονοπωλούν τον κόσμο του ίντερνετ και παρουσιάζουν αρκετές ομοιότητες αλλά επίσης και αρκετές διαφορές. Άρα η σύγκριση αυτών τον δύο είναι αναπόφευκτη προκειμένου να σκιαγραφήσει τα δύο πρωτόκολλα στα βασικά αλλά και στα λιγότερο κύρια σημεία τους.

Το H.323 είναι πρότυπο της ITU, οπότε προέρχεται από τον χώρο της παραδοσιακής τηλεφωνίας, είναι στην 5η έκδοση, άρα είναι ώριμο. Η κωδικοποίηση του είναι σε μορφή ASN και άρα είναι δυσανάγνωστο χωρίς ειδικά εργαλεία. Επίσης, αποτελείται από ομπρέλα πρωτοκόλλων και είναι ιδιαίτερα βαρύ στην υποστήριξή του και περίπλοκο στη λειτουργία του. Η μεγάλη εγκατεστημένη βάση ειδικού εξοπλισμού τηλεδιάσκεψης που χρησιμοποιούν το H.323 και η χρήση του στις πρώτες υπηρεσίες VoIP παραγωγής είναι οι λόγοι που παραμένει δημοφιλές.

Το SIP είναι πρότυπο της IETF, οπότε προέρχεται από τον χώρο του Internet και μοιάζει πολύ περισσότερο με τα άλλα πρωτόκολλα υπηρεσιών στο Internet, η ανάπτυξή του είναι ακόμα σε εξέλιξη, η κωδικοποίηση του είναι σε μορφή ASCII και άρα είναι εξαιρετικά ευανάγνωστο (όσο και το HTTP, SMTP), είναι απλό πρωτόκολλο σηματοδοσίας, εξαιρετικά ελαφρύ, απλό και επεκτάσιμο. Το SIP διαρκώς κερδίζει έδαφος, αλλά δεν είναι σαφές πότε και αν θα αντικαταστήσει πλήρως το H.323.

Το SIP προέρχεται από τα HTTP και SMTP ενώ το H.323 έχει εξαχθεί από το Q.931. Το SIP είναι βασισμένο σε κείμενο (text-based) πρωτόκολλο (ASCII) ενώ το H.323 είναι βασισμένο σε ASN.1. Η μετάδοση γίνεται μέσω TCP/ SCCP/ UDP στο SIP ενώ στο H.323 η μετάδοση γίνεται μόνο διαμέσου TCP. Η διευθυνσιοδότηση στο H.323 γίνεται διαμέσου ενός E.164 αριθμού ή με ένα e-mail alias που είναι λιγότερο ευέλικτο την στιγμή που το SIP κάνει τη διευθυνσιοδότηση μέσω κάποιου URL ή ενός E.164 αριθμού πολύ ευέλικτου.

Ο Gatekeeper είναι σταθερή κλήση στο H.323 ενώ το Proxy στο SIP μπορεί να είναι ασταθής, ή εκτελούμενο σταθερό . Στο H.323 η διαδικασία για την εγκατάσταση μιας

κλήσης είναι αρκετά πολύπλοκη ενώ αντίθετα αυτή η διαδικασία για το SIP πρωτόκολλο είναι αρκετά απλή. Ο Gatekeeper εμπλέκεται καθ όλη τη διάρκεια κλήσης στο H.323 πρωτόκολλο ενώ στο SIP πρωτόκολλο ο Proxy χρησιμοποιείται μόνο για την εγκατάσταση της κλήσης (SIP = Session Initiation Protocol).

Η διαπραγμάτευση με πολυμέσα είναι πολύπλοκη όσον αφορά το H.323 ενώ στην περίπτωση του SIP είναι απλή. Η ευκινησία δεν είναι τμήμα της αρχιτεκτονικής του H.323 αλλά είναι όμως αναπόσπαστο κομμάτι στην αρχιτεκτονική του SIP πρωτοκόλλου.

Η ενσωμάτωση του SIP σε IP δίκτυα γίνεται εύκολα ενώ η συνεργασία με τα PSTN δίκτυα είναι εύκολο για το H.323. Όσον αφορά την χρέωση της υπηρεσίας στην H.323 αρχιτεκτονική υπάρχει σημείο αναφοράς για αυτό ενώ στο SIP πρωτόκολλο όχι ιδιαίτερα ξεκάθαρα.

Το H.323 πρωτόκολλο είναι ιδιαίτερα «ώριμο» πρωτόκολλο αλλά το SIP ακόμη εξελίσσεται. Επίσης τα δύο πρωτόκολλα διαθέτουν διαφορετικούς οπαδούς στον κόσμο.

Το μέλλον ανήκει σίγουρα στο SIP, οπότε στο προσεχές διάστημα συσκευές που υποστηρίζουν dual-mode, SIP και H.323 κλήσεις, θα γίνουν δημοφιλείς, ενώ εξυπηρετητές που υποστηρίζουν τουλάχιστον αυτά τα δύο πρωτόκολλα θα παίξουν σημαντικό ρόλο. Τα δημοφιλέστερα H.323 και SIP τερματικά, σήμερα, είναι «συσκευές» βασισμένες σε λογισμικό μόνο, που μπορούν να χρησιμοποιήσουν το μικρόφωνο, ηχεία και απλή κάμερα ενός προσωπικού υπολογιστή για τηλεδιασκέψεις.

Το H.323 υπάρχει από το 1996. Η ομάδα Internet Engineering Task Force (IETF) εργάζεται με παράλληλα Στάνταρτ για την τεχνολογία IP. Το Session Initiation Protocol (SIP), είναι ένα πρωτόκολλο σε επίπεδο εφαρμογής (application level) για πολυμεσικές επικοινωνίες. Όσοι προτείνουν το SIP βλέπουν τα παρακάτω ως πλεονεκτήματα του SIP έναντι του H.323 :

- Βασισμένο σε IP (IP based): Το IP είναι το κυρίαρχο πρωτόκολλο τόσο για τις άκρες (edges) όσο και για την καρδιά (core) του Internet. Ως αποτέλεσμα, δεν υπάρχει κανένα πρόβλημα, όσον αφορά τη συνλειτουργία του με το ATM και ISDN.

- Το H.323 «κουβαλάει» πολλά έξτρα προκειμένου να εξασφαλίσει τη δυνατότητα συνλειτουργίας του με άλλα Στάνταρτ της σειράς, ενώ το SIP είναι απαλλαγμένο από όλο αυτό το περιττό «βάρος», είναι λιγότερο περίπλοκο, εύκολο για να αποκωδικοποιηθεί, παρέχει αρχιτεκτονική client - server, ευκολότερη firewall / proxy σχεδίαση, ενώ επίσης επιδέχεται αναβάθμιση και βελτίωση.[6]

2.4 Συμπεράσματα

Έχοντας παρουσιάσει και έχοντας κάνει σύγκριση των δύο βασικότερων πρωτοκόλλων που χρησιμοποιούνται στη τηλεδιάσκεψη, θα γίνει εξαγωγή των συμπερασμάτων για την χρήση τους.

Οι εφαρμογές, που υιοθετούν είτε το ένα είτε το άλλο πρωτόκολλο, υλοποιούνται σε συστήματα που κάνουν χρήση μεγάλης υπολογιστικής ισχύος μεταφέροντας τα δεδομένα τους με μεγάλη ταχύτητα. Τα δύο αυτά πρωτόκολλα έχουν αρκετές ομοιότητες και αρκετές διαφορές.

Όσον αφορά το θέμα ασφάλειας, δεν μπορεί να εξαχθεί συγκεκριμένο αποτέλεσμα. Οι λόγοι που μας οδηγούν σε αυτή την απάντηση είναι ότι από μόνα τους τα πρωτόκολλα αυτά δεν μπορούν να παρέχουν τη μέγιστη δυνατή ασφάλεια, καθώς έχουν άμεση αλληλεξάρτηση με τις εφαρμογές που υλοποιούνται. Επίσης, τα διεθνή πρότυπα, στα οποία πρέπει να υπακούουν, τροποποιούνται συνεχώς.

Το H.323 είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται εδώ και χρόνια και η ασφάλεια του ενδυναμώνεται μέσω της χρήσης του πρωτοκόλλου H.245. Όμως, αυτό το κάνει ταυτόχρονα και ευάλωτο σε διάφορες επιθέσεις ασφαλείας, καθώς οι κακόβουλοι χρήστες γνωρίζουν τις ευπάθειες του και τα τρωτά σημεία του κώδικά του και μπορούν να τα εκμεταλλευτούν καταλλήλως.

Το SIP είναι ένα πρωτόκολλο το οποίο συνεχώς αναπτύσσεται και εξελίσσεται. Αυτό το κάνει ταυτόχρονα και ευάλωτο στις επιθέσεις αλλά και ικανό να αντιμετωπίζει τις συνεχείς προκλήσεις. Χαρακτηρίζεται ως ευάλωτο, διότι δεν έχει χρησιμοποιηθεί για αρκετά μεγάλο χρονικό διάστημα και συνεπώς δεν έχει δοκιμαστεί αρκετά και δεν έχει μία γνωσιακή βάση με τα πιθανά προβλήματα που μπορεί να αντιμετωπίσει. Από

την άλλη χαρακτηρίζεται ως ικανό να αντιμετωπίζει τις προκλήσεις καθώς οι δημιουργοί του συνεχώς ενδυναμώνουν το πρωτόκολλο σύμφωνα με τις νέες απαιτήσεις των διεθνών προτύπων ασφαλείας.

Βάσει όλων όσων ερευνήθηκαν και έγιναν μελέτη στην παρούσα εργασία, κατά την προσωπική μου άποψη το πιο ασφαλές πρωτόκολλο, αν μπορεί κάποιος να το πει αυτό, είναι το SIP. Οι λόγοι που με οδηγούν σε αυτό το συμπέρασμα είναι ότι το SIP είναι ένα πρωτόκολλο το οποίο ακόμα εξελίσσεται και συνεπώς αυξάνονται τα δεδομένα της ασφάλειας του. Επίσης, είναι ένα πρωτόκολλο το οποίο προέρχεται από τα HTTP και SMTP, το οποίο σημαίνει ότι ενδυναμώνεται η ασφάλειά του μέσω αυτών.

Κεφάλαιο 3: Εργαλεία τηλεδιάσκεψης

Τα προϊόντα που είναι εφαρμογές που βασίζονται πάνω στα πρωτόκολλα είναι σίγουρα πολλά και συνεχώς ανανεώνονται, μετατρέποντας αυτά που σήμερα θεωρούνται κορυφαία αύριο να είναι απλώς ξεπερασμένα. Οι ομάδες των χρηστών είναι σίγουρα πολλές και διαφορετικές μεταξύ τους με διαφορετικές απαιτήσεις και ανάγκες. Το ίδιο συμβαίνει και με τα προϊόντα που έρχονται να προσφέρουν λύσεις στις απαιτήσεις αυτές.

3.1 NetMeeting

Το NetMeeting είναι ένα πρόγραμμα που μας προσφέρει έναν εντελώς νέο τρόπο επικοινωνίας. Με το NetMeeting, μπορούμε να συμμετέχουμε σε τηλεδιασκέψεις, να συνεργαζόμαστε σε αρχεία, χρησιμοποιώντας τις δυνατότητές του, και να χρησιμοποιούμε από κοινού πληροφορίες μέσω του διαδικτύου ή του εταιρικού μας δικτύου (Intranet).

3.1.1 Παρουσίαση-Ανάλυση

Η τελευταία έκδοση του NetMeeting περιέχει περισσότερες νέες δυνατότητες και βελτιωμένες λειτουργίες σε σχέση με τις παλαιότερες.

Μπορούμε με ευκολότερους τρόπους να αναζητούμε και να καλούμε άτομα. Μπορούμε, επίσης, να χρησιμοποιούμε βιβλία διευθύνσεων και καταλόγους που βρίσκονται στον τοπικό μας υπολογιστή, σε διακομιστές δικτύου καθώς και στο διαδίκτυο, για να καλούμε άλλα άτομα. Ακόμη, μπορούμε να χρησιμοποιούμε τον κατάλογο του διαδικτύου της Microsoft, προσαρμοσμένο με τη λίστα των επαφών μας, για την πραγματοποίηση κλήσεων με χρήση της υπηρεσίας MSN Messenger. Εάν η εταιρεία χρησιμοποιεί πύλες ή ελεγκτές πύλης για την πραγματοποίηση κλήσεων, μπορεί να πραγματοποιήσει κλήσεις NetMeeting σε τηλέφωνα καθώς και βιντεοσκοπικά συστήματα διάσκεψης.[21][29]

3.1.1.α Καλύτερη προβολή των κοινόχρηστων προγραμμάτων

Τα κοινόχρηστα προγράμματα εμφανίζονται σε ξεχωριστά παράθυρα στην επιφάνεια εργασίας, διευκολύνοντας έτσι τη διάκριση μεταξύ των κοινόχρηστων προγραμμάτων και των προσωπικών μας. Έχουμε τη δυνατότητα να εναλλασσόμαστε με ευκολία μεταξύ των προγραμμάτων και να τα ελαχιστοποιούμε χωρίς να επηρεάζουμε την επιφάνεια εργασίας των άλλων συμμετεχόντων.[21][29]

3.1.1.β Απομακρυσμένη κοινή χρήση της επιφάνειας εργασίας

Έχουμε τη δυνατότητα πρόσβασης και χρήσης ενός υπολογιστή από κάποιον άλλον μέσω της κοινόχρηστης επιφάνειας εργασίας. Αυτή η δυνατότητα είναι εξαιρετικά χρήσιμη, όταν θέλουμε να χρησιμοποιήσουμε αρχεία και προγράμματα από τον υπολογιστή του γραφείου μας όταν βρισκόμαστε σε κάποια άλλη τοποθεσία. Επιπλέον, επιτρέπει σ' έναν τεχνικό να εργαστεί και να διορθώσει ένα πρόβλημα στον υπολογιστή μας, χωρίς να είναι απαραίτητο να έλθει στο γραφείο μας.[21][29]

3.1.2 Λειτουργία

Οι δυνατότητες του NetMeeting μάς επιτρέπουν να πραγματοποιούμε κλήσεις χρησιμοποιώντας διακομιστές καταλόγου χρηστών, διακομιστές διασκέψεων καθώς και ιστοσελίδες. Το NetMeeting διευκολύνει την πραγματοποίηση κλήσεων μέσω του διαδικτύου, του εσωτερικού δικτύου της εταιρείας μας καθώς και των τηλεφώνων. Εύκολη συνεργασία με άλλους συμμετέχοντες στη τηλεδιάσκεψη μέσω της κοινής χρήσης των προγραμμάτων. Μόνο ένας υπολογιστής είναι απαραίτητο να διαθέτει το πρόγραμμα και έτσι όλοι οι άλλοι συμμετέχοντες να εργάζονται ταυτόχρονα στο έγγραφο. Επιπλέον, είναι δυνατή η αποστολή και η λήψη αρχείων από τους χρήστες για να εργαστούν σ' αυτά.

Οι δυνατότητες ήχου και βίντεο του NetMeeting μάς επιτρέπουν να δούμε και να ακούσουμε άλλα άτομα. Ακόμα και αν δεν έχουμε τη δυνατότητα μετάδοσης βίντεο, μπορούμε να λαμβάνουμε κλήσεις βίντεο στο παράθυρο βίντεο του NetMeeting. Μέσω της δυνατότητας της συνομιλίας, μπορούμε να ομιλούμε με πολλά άτομα.

Επιπλέον, οι κλήσεις συνομιλίας είναι δυνατό να κρυπτογραφηθούν, εξασφαλίζοντας έτσι την εμπιστευτικότητα των τηλεδιασκέψεών μας.

Με τη βοήθεια του πίνακα, μπορούμε να εξηγήσουμε έννοιες, δημιουργώντας διαγράμματα πληροφοριών, χρησιμοποιώντας σχέδια ή εμφανίζοντας γραφικά. Έχουμε επίσης τη δυνατότητα να αντιγράψουμε περιοχές της επιφάνειας εργασίας μας ή των παραθύρων μας και να τις επικολλήσουμε μετά στον πίνακα.

Το Microsoft NetMeeting προσφέρει σε όλον τον κόσμο έναν ολοκληρωτικά νέο τρόπο ομιλίας, διάσκεψης, εργασίας, καθώς και κοινής χρήσης προγραμμάτων στο διαδίκτυο.[21][29]

3.1.2.α Δυνατότητες με τη χρήση του NetMeeting

- Πραγματοποιούμε κλήσεις σ' όσους χρησιμοποιούν διαδίκτυο ή τοπικό δίκτυο (intranet).
- Με το NetMeeting, μπορούμε να καλούμε άτομα σ' άλλους υπολογιστές μέσω ενός τοπικού δικτύου (LAN), μέσω του διαδικτύου ή με modem. Μπορούμε να συνδεθούμε μαζί τους, αν διαθέτουν το NetMeeting ή κάποιο από τα λογισμικά διασκέψεων που βασίζονται σε πρότυπα.
- Για συζητήσεις μέσω του Internet, θα πρέπει υπολογιστής μας να διαθέτει κάρτα ήχου συνδεδεμένη με μικρόφωνο και ηχεία.
- Βλέπουμε τα άτομα που καλούμε
- Με το NetMeeting, μπορούμε να στέλνουμε μια εικόνα βίντεο. Είναι απαραίτητο να διαθέτουμε μια κάρτα καταγραφής βίντεο και μια βιντεοκάμερα ή μια βιντεοκάμερα με υποστήριξη Video for Windows ή και μια απλή web camera. Μπορούμε να λαμβάνουμε βίντεο ακόμη κι αν δεν διαθέτουμε εξοπλισμό βίντεο.
- Συνεργαζόμαστε μ' άλλους σε κοινόχρηστες εφαρμογές
- Μπορούμε να ανοίξουμε μια από τις εφαρμογές και να την θέσετε σε κοινή χρήση, ώστε οι άλλοι συμμετέχοντες να μπορούν να την βλέπουν, καθώς εμείς εργαζόμαστε.
- Χρησιμοποιούμε τον πίνακα για να σχεδιάζουμε κατά τη διάρκεια μιας ηλεκτρονικής διάσκεψης.

- Κατά τη συνεργασία σε μια κοινόχρηστη εφαρμογή, μόνο ένα άτομο μπορεί να έχει τον έλεγχο του δρομέα τη φορά. Συχνά προκύπτει η ανάγκη για κάποιο περιβάλλον διάσκεψης όπου ο καθένας να έχει τη δυνατότητα εργασίας ταυτόχρονα με τους άλλους συμμετέχοντες. Ο πίνακας είναι η απάντηση - παρέχει τη δυνατότητα στους συμμετέχοντες σε μια ηλεκτρονική διάσκεψη να σχεδιάζουν, να πληκτρολογούν καθώς και να βλέπουν τα αποτελέσματα ταυτόχρονα.
- Ελέγχουμε τη λίστα με τις μνήμες για να δούμε ποιοι «φίλοι» μας είναι συνδεδεμένοι.
- Η λίστα με τις μνήμες για τους «φίλους» και συνεργάτες μας, μας ενημερώνει ποιοι απ' αυτούς είναι συνδεδεμένοι κάθε στιγμή.
- Πληκτρολογούμε μηνύματα και τα στέλνουμε με τη συνομιλία.
- Η συνομιλία επιτρέπει στους συμμετέχοντες σε μια ηλεκτρονική διάσκεψη να πληκτρολογούν και να ανταλλάσσουν μηνύματα σε πραγματικό χρόνο. Όταν ένα άτομο σε μια τηλεδιάσκεψη αρχίζει να χρησιμοποιεί τη συνομιλία, αυτή εμφανίζεται στις οθόνες όλων. Εφόσον μόνο δύο άτομα μπορούν να χρησιμοποιούν ήχο και βίντεο κάθε στιγμή, η συνομιλία είναι ιδιαίτερα χρήσιμη όταν υπάρχουν πολλοί συμμετέχοντες στην ίδια τηλεδιάσκεψη.
- Στέλνουμε αρχεία σε άλλους, που συμμετέχουν σε μια τηλεδιάσκεψη.
- Μπορούμε να στείλουμε ένα αρχείο σε όλους τους συμμετέχοντες σε μια τηλεδιάσκεψη, σύροντας απλά το αρχείο πάνω στα ονόματά τους, στην καρτέλα τρέχουσας κλήσης.
- Μπορούμε να χρησιμοποιήσουμε το NetMeeting για να καλούμε άτομα μέσω του διαδικτύου, ενός εταιρικού δικτύου ή απευθείας χρησιμοποιώντας μια σύνδεση modem. Πρέπει να έχουμε υπόψη μας ότι το άτομο που καλούμε δεν είναι απαραίτητο να διαθέτει το NetMeeting. Πολλά προϊόντα λογισμικού που βασίζονται σε πρότυπα διαφορετικά από αυτά του NetMeeting μπορούν να λαμβάνουν κλήσεις NetMeeting.[21][29]

3.1.2.β Δυνατότητες πραγματοποίησης κλήσης με το NetMeeting

Απευθείας

Το NetMeeting συνδέεται απευθείας με έναν διακομιστή καταλόγου διαδικτύου ή με έναν άλλον υπολογιστή. Για να πραγματοποιήσουμε μια κλήση, μπορούμε είτε να επιλέξουμε ένα από τα άτομα που είναι συνδεδεμένα σε έναν διακομιστή ή να καλέσουμε έναν άλλον υπολογιστή πληκτρολογώντας το όνομα ή τη διεύθυνσή του.

Κατάλογος Internet της Microsoft

Τα άτομα που προσθέτουμε στη λίστα επαφών της υπηρεσίας MSN Messenger εμφανίζονται ως επαφές στον κατάλογο διαδικτύου της Microsoft του NetMeeting. Οι επαφές μας είναι άλλα άτομα που έχουν λογαριασμούς Hotmail. Μπορούμε να πραγματοποιήσουμε κλήσεις NetMeeting σε άτομα από τη λίστα επαφών μας που έχουν λογαριασμό Hotmail είτε από την υπηρεσία MSN Messenger είτε από τον κατάλογο διαδικτύου της Microsoft.

Χρήση μιας πύλης

Το NetMeeting έχει τη δυνατότητα να χρησιμοποιήσει μια πύλη του δικτύου μας, για να συνδεθεί με ένα τηλέφωνο ή με ένα βιντεοσκοπικό σύστημα τηλεδιάσκεψης.

Χρήση ελεγκτή πύλης

Το NetMeeting χρησιμοποιεί έναν υπολογιστή του δικτύου μας με τη βοήθεια του οποίου μπορούμε να αναζητήσουμε και να συνδεθούμε με άλλα άτομα, υπολογιστές και πύλες. Οι διαχειριστές πύλης ελέγχουν την πρόσβαση στο δίκτυο, επιτρέποντας ή απορρίπτοντας κλήσεις και ελέγχοντας την ταχύτητα σύνδεσης μιας κλήσης. Επιπλέον, προσφέρουν βοήθεια για την ανάλυση διευθύνσεων, μετατρέποντας τις ηλεκτρονικές διευθύνσεις στις κατάλληλες διευθύνσεις δικτύου.

Μεταφορά τηλεφωνικών κλήσεων στο NetMeeting

Οι τηλεφωνικές κλήσεις μπορούν να μεταφερθούν στο NetMeeting, με την προϋπόθεση ότι υπάρχουν δυνατότητες ήχου και βίντεο. Κατά τη μεταφορά της κλήσης είναι διαθέσιμες μόνον οι δυνατότητες ήχου και βίντεο. Οι δυνατότητες τηλεδιάσκεψης με δεδομένα του NetMeeting, όπως η συνομιλία, ο πίνακας, η κοινή χρήση προγραμμάτων και η μεταφορά αρχείων δεν είναι διαθέσιμες.[21][29]

3.1.3 Ασφάλεια

Στο NetMeeting, η ασφάλεια, που παρέχεται, επιτρέπει να αποστείλουμε και να λαμβάνουμε κρυπτογραφημένα δεδομένα, να ελέγχουμε την ταυτότητα των συμμετεχόντων στη τηλεδιάσκεψη, καθώς και να την προστατεύουμε με την χρήση κωδικού πρόσβασης.

Το NetMeeting παρέχει τη δυνατότητα να επιλέξουμε αν η κλήση ή η τηλεδιάσκεψη θα είναι ασφαλής ή όχι και πραγματοποιεί μη ασφαλείς κλήσεις από προεπιλογή. Μέσω μιας ασφαλούς κλήσης του NetMeeting, είναι δυνατή η κρυπτογράφηση δεδομένων και ο έλεγχος της ταυτότητας των συμμετεχόντων σε μια τηλεδιάσκεψη, οι οποίοι διαθέτουν πιστοποιητικά ελέγχου ταυτότητας με προστασία κωδικού πρόσβασης.

Κατά την ανταλλαγή δεδομένων σε μια ασφαλή κλήση ή τηλεδιάσκεψη, τα δεδομένα κρυπτογραφούνται, έτσι ώστε μόνο οι παραλήπτες για τους οποίους προορίζονται αυτά να έχουν τη δυνατότητα να τα διαβάσουν. Το NetMeeting παρέχει ένα πιστοποιητικό εμπιστευτικότητας, μέσω του οποίου οι πληροφορίες κρυπτογραφούνται κατά την αποστολή τους και μετά αποκρυπτογραφούνται στον υπολογιστή του παραλήπτη.

Με τον έλεγχο ταυτότητας, γίνεται επαλήθευση των στοιχείων του ατόμου με το οποίο πιστεύουμε ότι επικοινωνούμε. Η πιο κοινή μέθοδος ελέγχου ταυτότητας είναι η χρήση πιστοποιητικών. Ένα πιστοποιητικό ελέγχου ταυτότητας είναι ένα σύνολο δεδομένων το οποίο προσδιορίζει ένα άτομο. Ένας αξιόπιστος οργανισμός ή οντότητα, γνωστή ως αρχή έκδοσης πιστοποιητικών, εκδίδει το πιστοποιητικό μετά από την επαλήθευση της ταυτότητας του ατόμου.

Τα πιστοποιητικά ελέγχου ταυτότητας μπορούν να χρησιμοποιηθούν επίσης για την κρυπτογράφηση πληροφοριών, εξασφαλίζοντας έτσι τη χρήση του ίδιου κλειδιού κρυπτογράφησης από τον αποστολέα και από τον παραλήπτη, δηλαδή χρησιμοποιείται η συμμετρική κρυπτογράφηση.

Ασφαλείς κλήσεις είναι αυτές που χρησιμοποιούν μόνο δεδομένα. Σε μια ασφαλή κλήση μπορούμε να χρησιμοποιούμε τη συνομιλία και τον πίνακα με τα κοινόχρηστα προγράμματα καθώς και να μεταφέρουμε αρχεία, αλλά χωρίς να μπορούμε να

χρησιμοποιήσουμε τον ήχο και το βίντεο, γιατί αυτές οι μεταδόσεις δεν είναι κρυπτογραφημένες. Δεν είναι δυνατό να υπάρχουν ασφαλείς και μη ασφαλείς κλήσεις ταυτόχρονα σε μια τηλεδιάσκεψη. Όλες οι κλήσεις πρέπει να είναι της ίδιας κατηγορίας.

Μπορούμε να χρησιμοποιήσουμε έναν κωδικό πρόσβασης για να προστατέψουμε το απόρρητο των ηλεκτρονικών μας τηλεδιασκέψεων. Κατά τον προγραμματισμό της, επιλέγουμε έναν κωδικό πρόσβασης και δίνουμε τον κωδικό στους άλλους συμμετέχοντες. Κατά την έναρξη της, για να συμμετέχει ο κάθε χρήστης είναι υποχρεωμένος να παρέχει τον κωδικό πρόσβασης. Η χρήση του κωδικού πρόσβασης είναι ένας εύχρηστος και εύκολος τρόπος για την παρακολούθηση συμμετοχή σε αυτή.

Το NetMeeting χρησιμοποιεί το δικό του πιστοποιητικό για την κρυπτογράφηση δεδομένων, αλλά χωρίς να έχει τη δυνατότητα επαλήθευσης των στοιχείων της ταυτότητας.[21][40]

3.1.4 Αναφορές Προβλημάτων

Το NetMeeting είναι ένα εργαλείο τηλεδιάσκεψης το οποίο χρησιμοποιείται από τις πιο μικρές επιχειρήσεις έως τις πιο μεγάλες. Προσφέρει πολλά πλεονεκτήματα, αλλά έχει και κάποια σοβαρά μειονεκτήματα. Εξαιτίας πολλών αλλαγών, επηρεάστηκε η ασφάλεια, το τείχος προστασίας και ο απομακρυσμένος έλεγχος κατά την διάρκεια των τηλεδιασκέψεων. Για τους λόγους αυτούς το 2003 το NetMeeting σταμάτησε να αναπτύσσεται περαιτέρω και αντικαταστάθηκε από το Meeting Space και άλλα παρόμοια προγράμματα, και εσχάτως από το Skype (Δεκέμβριος 2012).

Ένα από τα πλεονεκτήματα του NetMeeting, είναι ο διαμοιρασμός των πληροφοριών με άλλους εξατομικευμένα. Διαμοιράζοντας μια εφαρμογή μόνο για ανάγνωση προστατεύει την τροποποίηση της. Παρ' όλα αυτά, εάν ο χρήστης δίνει απομακρυσμένο έλεγχο της εφαρμογής σε συνεργατικό περιβάλλον και εάν η εφαρμογή είναι ικανή να επανεγγράψει το δίσκο, ο χρήστης κινδυνεύει από την τροποποίηση του υλικού του και πιθανώς η πληροφορία να διαγραφεί ή να καταστραφεί. Άλλα ευπαθή σημεία μπορεί να είναι όπως οι εκτελέσεις του ActiveX ή των Macros.

Η χρήση της κοινωνικής δικτύωσης μπορεί να επιτρέψει σε άτομα εκτός του τείχους προστασίας και της ασφάλειας της επιχείρησης να αποκτήσουν πρόσβαση σε εσωτερικές πληροφορίες. Εάν κάποιος θεωρείται έμπιστος και μπορεί να έχει πρόσβαση μέσω του NetMeeting, μπορεί να είναι ικανός όχι μόνο να αποκτήσει πρόσβαση στην εφαρμογή αλλά και σε ζωτικά σημεία του δικτύου της επιχείρησης. Μια άλλη απειλή είναι ότι το έμπιστο άτομο μπορεί να στείλει ένα πρόγραμμα που θα επέτρεπε την πρόσβαση στο δίκτυο της εταιρίας σε μια επόμενη ημερομηνία χρησιμοποιώντας κάποιον Δούρειο Ίππο ή παρόμοιο πρόγραμμα. Πιστοποιητικά ταυτοποίησης και αυθεντικοποίησης δεν εγκαθίσταται μέσω αυτού του προγράμματος, με αποτέλεσμα αυτό να δημιουργεί ανασφάλεια στο αν οι χρήστες συνδέονται με τα σωστά άτομα.

Στο NetMeeting υλοποιούνται και άλλες απειλές – επιθέσεις, οι οποίες μπορούν να προκαλέσουν την δυσλειτουργία του. Η πλειονότητα αυτών δεν υλοποιείται στο πρόγραμμα NetMeeting, αλλά στο δίκτυο μέσω του οποίου ο χρήστης πραγματοποιεί την τηλεδιάσκεψη.

Επειδή το NetMeeting είναι ένα από τα προγράμματα που έχει αναπτύξει η Microsoft, μπορεί να συνεργαστεί με άλλα προγράμματα της εταιρίας αυτής. Τα προγράμματα αυτά δεν είναι πάντοτε ασφαλή και ενδυναμωμένα με τις τελευταίες ενημερώσεις. Έτσι, ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση μέσω αυτών στο NetMeeting, και κατ' επέκταση στο δίκτυο της επιχείρησης.[28][40]

3.2 Asterisk

Στην κοινότητα του Asterisk έχει επιχειρηθεί αρκετές φορές να δοθεί ένας περιεκτικός ορισμός του τι ακριβώς είναι το Asterisk και ποιες είναι οι δυνατότητες του. Οι δημιουργοί του, θέλοντας να απλοποιήσουν την έννοια του Asterisk και να το κάνουν ποιο ελκυστικό στο ευρύ κοινό, συχνά χρησιμοποιούν τη φράση: «Είναι απλά λογισμικό». Στην πραγματικότητα όμως, είναι πολλά περισσότερα.

Κάποιος μπορεί να καταλάβει τι είναι το Asterisk κοιτάζοντας την ετοιμολογία του ονόματός του. Ο ειδικός χαρακτήρας του αστερίσκου (*) είναι συγχρόνως ένα πλήκτρο του τηλεφωνικού πληκτρολογίου καθώς επίσης και ένας ειδικός χαρακτήρας στα λειτουργικά συστήματα UNIX και DOS που μπορεί να συμβολίσει οποιοδήποτε

αλφαριθμητικό χαρακτήρα. Έτσι και το Asterisk, έχει σχεδιαστεί ώστε να μπορεί να διασυνδεθεί με οποιοδήποτε τηλεφωνικό υλικό ή λογισμικό απρόσκοπτα και με συνέπεια.[5][13][23][24]

3.2.1 Παρουσίαση-Ανάλυση

Το Asterisk έχει σχεδιαστεί με κύρια προτεραιότητα την ευελιξία και τη συνδεσιμότητα, όπου συγκεκριμένα APIs ορίζουν τον πυρήνα του PBX συστήματος. Η εξελιγμένη αρχιτεκτονική του Asterisk του επιτρέπει να χειρίζεται τις εσωτερικές διασυνδέσεις με πλήρη διαφάνεια, ανεξαρτήτως πρωτοκόλλων, κωδικοποιήσεων, και τηλεφωνικού υλικού. Με αυτόν τον τρόπο το Asterisk είναι σε θέση να χρησιμοποιήσει όλα τα κατάλληλα υλικά και τις τεχνολογίες που είναι διαθέσιμες σήμερα ή ακόμα και μελλοντικά, για να εκτελέσει τις βασικές του λειτουργίες, συνδέοντας υλικό και λογισμικό. [5][13][23][24]

3.2.1.α Ο πυρήνας του Asterisk

Μεταγωγέας PBX

Η πρωταρχική λειτουργία του Asterisk όπως φαίνεται και από την πρώτη ονομασία του (Asterisk the Free PBX) είναι να λειτουργεί σαν σύστημα PBX, συνδέοντας κλήσεις μεταξύ χρηστών και ενεργειών. Ο πυρήνας μεταγωγής συνδέει χρήστες από διάφορες διεπαφές λογισμικού ή υλικού.

Εκτελεστής Εφαρμογών

Εκτελεί εφαρμογές που παρέχουν λειτουργίες όπως, αναπαραγωγή αρχείων, αυτόματος τηλεφωνητής.

Μεταφραστής κωδικοποίησης

Χρησιμοποιεί τρόπους για την κωδικοποίηση και την αποκωδικοποίηση διαφόρων τύπων συμπίεσης ήχου, που εφαρμόζονται στην τηλεφωνία. Υποστηρίζονται πολλοί κωδικοποιητές για να μπορέσει να επιτευχθεί μία ισορροπία μεταξύ ποιότητας ήχου και χρήσης του εύρους ζώνης.

Χρονοπρογραμματιστής και Ελεγκτής Εισόδου/Εξόδου

Χειρίζεται λειτουργίες χρονοπρογραμματισμού και εποπτείας σε χαμηλό επίπεδο, επιτρέποντας την επίτευξη της καταλληλότερης επίδοσης σε κάθε περίπτωση φόρτου εργασίας. [5][13][23][24]

3.2.1.β APIs Ενότητες φόρτωσης

Υπάρχουν τέσσερα APIs για να φορτώνονται ενότητες, τα οποία παρέχουν τη διαλειτουργικότητα σε θέματα υλικού και πρωτοκόλλων. Με τη χρήση αυτού του αρθρωτού συστήματος, ο πυρήνας του Asterisk δε χρειάζεται να γνωρίζει λεπτομέρειες για το πώς συνδέεται ο χρήστης, τι κωδικοποιήσεις χρησιμοποιεί, κ.λ.π. Τα APIs είναι τα εξής:

Κανάλι API

Το κανάλι API διαχειρίζεται τον τύπο της σύνδεσης, από την οποία προέρχεται ο χρήστης. Η σύνδεση αυτή μπορεί να είναι VoIP, ISDN, POTS, ή οποιαδήποτε άλλη τεχνολογία. Οι τρόποι φορτώνονται δυναμικά για να χειριστούν τις λεπτομέρειες της σύνδεσης.

API Εφαρμογών

Το API εφαρμογών, επιτρέπει στους τρόπους εφαρμογών να εκτελεστούν ώστε να παρέχουν διάφορες λειτουργίες. Δυνατότητες όπως τηλεδιάσκεψη, μεταφορά δεδομένων, φωνητικό ταχυδρομείο και οποιαδήποτε άλλη εργασία μπορεί να εκτελέσει ένα σύγχρονο ή μελλοντικό PBX.

API Μετάφρασης κωδικοποίησης

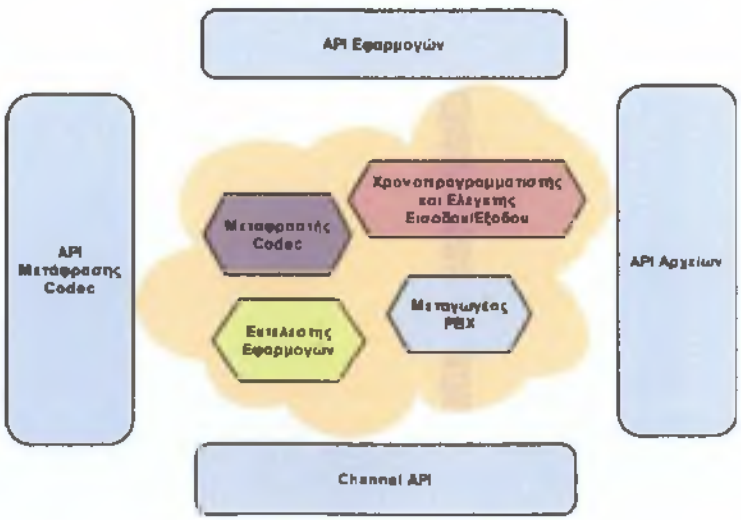
Το API αυτό φορτώνει ξεχωριστά ενότητες προγραμμάτων για την κάθε μορφή κωδικοποίησης, για να υποστηρίξει τους διάφορους τύπους κωδικοποίησης και αποκωδικοποίησης ήχου που υπάρχουν.

API Αρχείων

Το API αρχείων είναι υπεύθυνο για την ανάγνωση και εγγραφή πολλών τύπων αρχείων, και την αποθήκευση δεδομένων στο σύστημα.

Με τη χρήση αυτών των APIs, το Asterisk επιτυγχάνει πλήρη ανεξαρτησία μεταξύ της βασικής λειτουργίας του ως PBX και της πληθώρας των τεχνολογιών που υπάρχουν στο χώρο της τηλεφωνίας. Η αρθρωτή δομή του, του επιτρέπει να συνεργάζεται απόλυτα τόσο με τα παραδοσιακά συστήματα, όσο και με τις νέες τεχνολογίες μετάδοσης πακέτων φωνής. Η δυνατότητα που έχει το Asterisk να φορτώνει ενότητες προγραμμάτων για κάθε κωδικοποίηση, του επιτρέπει να πραγματοποιεί μετάδοση πακέτων φωνής τόσο σε δίκτυα με μικρό εύρος ζώνης (σύνδεση μέσω modem) με χρήση κωδικοποίησης υψηλής συμπίεσης, όσο και σε ευρυζωνικά δίκτυα, παρέχοντας υψηλής ποιότητας ήχο.

Οι εφαρμογές API παρέχουν τη δυνατότητα στις ενότητες εφαρμογών να εκτελούν οποιαδήποτε λειτουργία ευέλικτα και κατά βούληση του χρήστη. Επιτρέπει, επίσης, την εκτέλεση εφαρμογών που έχουν αναπτυχθεί αποκλειστικά για να καλύψουν προσαρμοσμένες ανάγκες και περιπτώσεις χρήσης. Επιπλέον, φορτώνοντας όλες τις εφαρμογές ως ενότητες το Asterisk δίνει τη δυνατότητα στους διαχειριστές να σχεδιάσουν συστήματα με εύκολη προσαρμογή στις τηλεπικοινωνιακές αλλαγές που μπορεί να προκύψουν. [5][13][23][24]



Εικόνα 7: Παρουσίαση του Asterisk

3.2.2 Λειτουργία

Όπως αναφέρθηκε προηγουμένως, είναι πολύ δύσκολο να περιγραφεί το πλήρες φάσμα των δυνατοτήτων του Asterisk λόγω του πλήθους των περίπλοκων θεμάτων που ενσωματώνει: πολλαπλούς τύπους VoIP καναλιών, υλικά διασύνδεσης, γλώσσα δέσμης ενεργειών, Διασύνδεση Προγράμματος Εφαρμογής (API) και πληθώρα λειτουργιών. Παρακάτω, θα αναφερθούμε σε κάποιες από τις λειτουργίες που κάνουν το Asterisk τόσο ισχυρό και στο επόμενο κεφάλαιο θα δούμε πως μπορούμε να υλοποιήσουμε μερικές από αυτές στην πράξη και τις ευπάθειες αυτών.

Λειτουργίες – Δυνατότητες Asterisk

Ενδεικτικά, κάποιες από τις κυρίες λειτουργίες και δυνατότητες του Asterisk είναι οι ακόλουθες :

- *ADSI σύστημα επιλογών επί της οθόνης (ADSI On-Screen Menu System):* Εμφάνιση μενού στην οθόνη κατάλληλου τηλεφώνου (screenphone) μέσω του αναλογικού δικτύου για παροχή προσαρμοσμένων λειτουργιών.
- *Λήπτης ειδοποιήσεων (Alarm Receiver):* Δυνατότητα ειδοποίησης ανάλογα με κάποια προσαρμοσμένα όρια που αφορούν την απόδοση του τηλεφωνικού μας κέντρου (π.χ. μεγάλη αναμονή).
- *Αυτόματος συνοδός (Automated Attendant):* Επιτρέπει σε κάποιον να πληκτρολογήσει έναν κεντρικό αριθμό και στη συνέχεια να πληκτρολογήσει τον κωδικό κάποιας υπηρεσίας ή κάποιας επέκτασης. Μπορεί να χρησιμοποιηθεί σε συνδυασμό με το Dial by Name για να παρέχει π.χ. τη δυνατότητα κλήσης με χρήση ονόματος.
- *Μαύρες λίστες (Blacklists):* Δημιουργία μαύρης λίστας εισερχομένων κλήσεων και ξεχωριστή διαχείριση της ανάλογα με προσαρμοσμένους κανόνες.
- *Εγγραφές λεπτομερειών κλήσεων (Call Detail Records):* Αρχείο καταγραφής κλήσεων με στοιχεία όπως η ώρα έναρξη της κλήσης, η διάρκεια της κλήσης, το νούμερο του καλούντα, την κατάσταση της κλήσης, κ.α.
- *Προώθηση Κλήσεων (Call Forward):* κατά βούληση ή ανάλογα με την κατάσταση (Κατειλημμένο, Δεν απαντά, κ.λ.π.)
- *Παρακολούθηση κλήσεων (Call Monitoring):* σε πραγματικό χρόνο ή καταγραφή τους για διασφάλιση ποιότητας υπηρεσιών.

- *Στάθμευση της κλήσης (Call Parking):* σε ένα εικονικό νούμερο το οποίο χρησιμοποιείται σαν χώρος στάθμευσης των κλήσεων και επανάκτηση της κλήσης κατά βούληση
- *Ουρές αναμονής κλήσεων (Call Queuing):* με δυνατότητα αναπαραγωγής μουσικής ή ανακοινώσεων κατά τη διάρκεια αναμονής.
- *Ηχογράφηση κλήσεων (Call Recording):* σε πραγματικό χρόνο.
- *Μεταφορά κλήσεων (Call Transfer):* από ένα νούμερο σε ένα άλλο.
- *Αναμονή κλήσεων (Call Waiting):* με δυνατότητα αναγνώρισης κλήσης της δεύτερης γραμμής, μουσική κατά τη διάρκεια της αναμονής και προώθηση κλήσης που βρίσκεται στην αναμονή.
- *Αναγνώριση κλήσης (Caller ID):* με στοιχεία το νούμερο και το όνομα του καλούντα (αν είναι διαθέσιμα).
- *Προβλεπόμενος καλών (Predictive Dialler):* Αυτόματη κλήση σε τηλεφωνικά νούμερα. Χρησιμοποιείται σε τηλεφωνικά κέντρα και πραγματοποιεί κλήσεις προς πιθανούς πελάτες με χρήση εξειδικευμένων αλγορίθμων πρόβλεψης.
- *Δρομολόγηση της κλήσης (Call Routing):* ανάλογα με τον αριθμό αυτού που καλεί, την ώρα κλήσης, το κόστος κλήσης, κ.α.
- *Αποστολή γραπτών μηνυμάτων (SMS Messaging)*
- *Δυνατότητα βιντεοκλήσης (Streaming Media Access)*
- *VoIP Gateway:* Δυνατότητα διασύνδεσης VoIP τερματικών ανεξαρτήτως πρωτοκόλλου που χρησιμοποιεί το καθένα και μετατροπή των μη συμβατών πρωτοκόλλων.
- *Τηλεφωνητής (Voicemail):* Φωνητικό ταχυδρομείο με δυνατότητες ειδοποίησης νέων μηνυμάτων μέσω email, αποστολής του μηνύματος ως προσάρτηση σε email, οπτικής απεικόνισης νέων μηνυμάτων στα τερματικά, οργάνωσης σε φακέλους, ομαδικής αποστολής και απομακρυσμένης διαχείρισης.
- *Zapateller:* Χρήση ειδικού ήχου για αποφυγή τηλεφωνημάτων από αυτόματες κλήσεις π.χ. τηλεπωλήσεις.[7][23][24]

3.2.3 Ασφάλεια

Ένα πολύ σημαντικό θέμα στις τηλεδιασκέψεις είναι η ασφάλεια. Μελετώντας την, πρέπει να ληφθεί υπόψιν ότι οι τηλεδιασκέψεις είναι βασισμένες σε πρωτόκολλα δικτύου, οπότε θα πρέπει να αξιολογηθεί η ασφάλεια από την συγκεκριμένη οπτική γωνία. Αυτό δεν σημαίνει ότι δεν θα μελετηθεί η ασφάλεια από πλευράς τηλεπικοινωνιών, αλλά θα δοθεί μεγαλύτερη έμφαση στην κατανόηση από πλευράς δικτύου.

Το σημαντικότερο κομμάτι το οποίο πρέπει να είναι ασφαλές είναι η πρόσβαση στο δίκτυο φωνής. Η χρήση τειχών προστασίας και εικονικών δικτύων είναι ενδεικτικά παραδείγματα τα οποία μπορούν να πραγματοποιηθούν για να επιτύχουμε ασφαλή πρόσβαση. Εξ ορισμού, το δίκτυο φωνής θα πρέπει να είναι προσβάσημο μόνο σε εκείνα τα αντικείμενα που το έχουν ανάγκη. Για παράδειγμα, εάν δεν χρησιμοποιούνται softphones (ειδικές συσκευές που χρησιμοποιούνται στους υπολογιστές για συνομιλίες μέσω asterisk), δεν χρειάζεται να επιτραπεί στους υπολογιστές των χρηστών η πρόσβαση στο δίκτυο φωνής.

Εάν δεν υπάρχει η ανάγκη της χρήσης του ίδιου δικτύου και για την φωνή και για τα δεδομένα, θα ήταν ιδιαίτερα σημαντικό να διατηρούνταν σε ξέχωρα κανάλια δικτύου (αυτό θα έδινε επιπλέον πλεονεκτήματα, όπως στην παραμετροποίηση της Ποιότητας Υπηρεσιών – QoS). Δεν είναι σωστό να κατασκευαστεί το εσωτερικό δίκτυο φωνής σε ένα εξ ολοκλήρου ξεχωριστό δίκτυο LAN, χρησιμοποιώντας την υπάρχουσα CAT3 καλωδίωση (το γνωστό UTP καλώδιο) και τερματισμού σε διακόπτες δικτύου.

Υπάρχει η δυνατότητα να τοποθετήσουμε το σύστημα των τηλεδιασκέψεων κάτω από ένα DMZ (demilitarized zone – αποστρατικοποιημένη ζώνη). Το DMZ είναι ένα φυσικό ή λογικό υποδίκτυο το οποίο περιέχει και εκθέτει τις εξωτερικές υπηρεσίες ενός οργανισμού/επιχείρησης σε ένα μεγαλύτερο μη έμπιστο δίκτυο, συνήθως το διαδίκτυο. Η χρήση το DMZ προσθέτει ένα επιπλέον επίπεδο ασφαλείας στο δίκτυο LAN. Ένας εξωτερικός επιτιθέμενος μπορεί να επιτύχει πρόσβαση μόνο στο DMZ, και όχι σε άλλο μέρος του δικτύου. Υλοποιώντας το DMZ στις τηλεδιασκέψεις, υπάρχει το πλεονέκτημα της επιτρεπτής χρήσης στη συνδεσιμότητα σχετικών εφαρμογών. Όπως γίνεται κατανοητό, είναι αρκετά πιο δύσκολο με επιτεθεί κάποιος στο σύστημα τηλεδιασκέψεων. Βέβαια, ανεξαρτήτως της χρήσης ή μη του DMZ, εάν

υπάρξει κάποια αφύσικη κίνηση πακέτων δεδομένων, τότε αυτή θα πρέπει να θεωρηθεί ύποπτη.

Ένα κρίσιμο σημείο είναι η ενδυνάμωση της ασφάλειας του εξυπηρετητή του Asterisk. Εφαρμόζοντας κάτι τέτοιο, όχι μόνο ευεργετούνται οι λειτουργίες του Asterisk, αλλά και η εξάλειψη κάθε τι μη απαιτούμενου μειώνει την πιθανότητα της ύπαρξης ευπάθειας στο λειτουργικό σύστημα, όπου κάποιος θα μπορούσε να αποκτήσει πρόσβαση και να υλοποίηση μια επίθεση στα άλλα μέρη του δικτύου.

Αν και το Asterisk ακόμα δεν υποστηρίζει πλήρως το SRTP (Secure Real-time Transport Protocol – Πρωτόκολλο Ασφαλούς Μεταφοράς Πραγματικού Χρόνου), είναι δυνατόν να κρυπτογραφηθεί η κίνηση δεδομένων μια τηλεδιάσκεψης. Μια τέτοια υλοποίηση μπορεί να πραγματοποιηθεί με την χρήση ενός εικονικού ιδιωτικού δικτύου (VPN – Virtual Private Network).

Ένας άλλος τομέας, που δεν πρέπει να αγνοηθεί, είναι η φυσική ασφάλεια. Όλος ο τερματικός εξοπλισμός (διακόπτες, δρομολογητές και PBX), θα πρέπει να είναι ασφαλισμένος σε ένα περιβάλλον στο οποίο θα έχουν πρόσβαση μόνο εξουσιοδοτημένα πρόσωπα. Από την πλευρά του χρήστη, είναι πιο δύσκολη η ανάπτυξη φυσικής ασφάλειας, αλλά αν το δίκτυο αντανακλάται μόνο σε συσκευές στις οποίες είναι εξοικειωμένος, τότε η μη εξουσιοδοτημένη εισχώρηση μειώνεται.[35][36]

3.2.4 Αναφορές Προβλημάτων

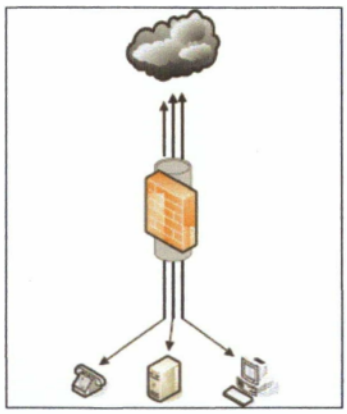
Αν και προτείνεται η χρήση διαφορετικών καναλιών δικτύου για την φωνή και τα δεδομένα, και τα δύο καταλήγουν στο ίδιο καλώδιο. Αυτό έχει ως συνέπεια να μπορούν να πραγματοποιηθούν πολλές επιθέσεις στο σύστημα τηλεδιασκέψεων, καθώς η τηλεπικοινωνιακή υποδομή βρίσκεται σε κίνδυνο. Τέτοιες επιθέσεις θα περιγραφούν στο ακόλουθο κομμάτι.

Άρνηση εξυπηρέτησης υπηρεσιών – διακοπή υπηρεσίας τηλεδιάσκεψης

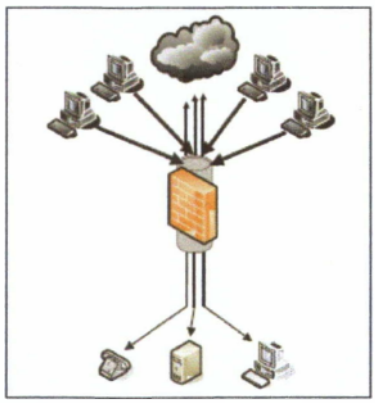
Οι επιθέσεις άρνησης εξυπηρέτησης υπηρεσιών (DoS – Denial of Service) μπορούν να επηρεάσουν κάθε υπηρεσία δικτύου βασισμένη σε IP. Οι επιπτώσεις μια τέτοια

επίθεσης μπορούν να κυμανθούν από μια μέση υποβάθμιση της υπηρεσίας μέχρι την ολοκληρωτική απώλεια της. Υπάρχουν διάφοροι τύποι επιθέσεων DoS.

Ένας τύπος επίθεσης, όπου πακέτα μπορούν να πλημμυρίσουν το στόχο – δίκτυο από πολλαπλές εξωτερικές πηγές, ονομάζεται Κατανεμημένη Άρνηση Εξυπηρέτησης Υπηρεσιών (DDoS). Αναλυτικότερα, στην Εικόνα 8 γίνεται μια απεικόνιση της πρόσβασης του εσωτερικού δικτύου στο διαδίκτυο, ενώ στην Εικόνα 9 παρουσιάζεται το πώς πραγματοποιείται η επίθεση DDoS.

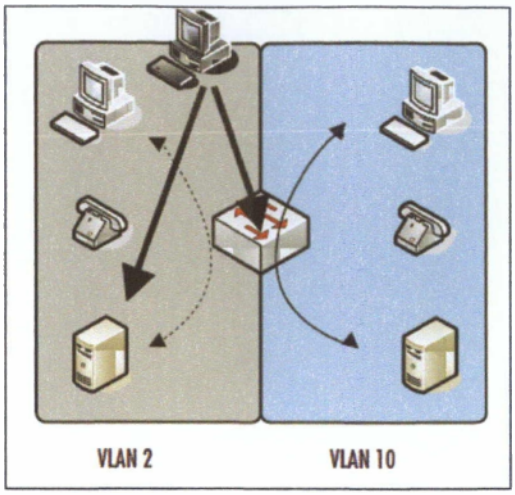


Εικόνα 8: Τυπική πρόσβαση στο διαδίκτυο



Εικόνα 9: Κατανεμημένη Άρνηση Εξυπηρέτησης Υπηρεσιών - DDoS

Ένας δεύτερος μεγάλος τύπος επιθέσεων DoS πραγματοποιείται όταν συσκευές από το εσωτερικό δίκτυο στοχοποιηθούν από μία πλημμύρα πακέτων ώστε να αποτύχουν παρασέρνοντας μαζί και άλλα σχετιζόμενα μέρη της υποδομής. Αυτό αποτυπώνεται ξεκάθαρα στην Εικόνα 10.



Εικόνα 10: Εσωτερική Άρνηση Εξυπηρέτησης Υπηρεσιών

Οι επιθέσεις DoS και DDoS δεν μπορούν να αποφευχθούν είτε με την χρήση κρυπτογράφησης είτε με τον έλεγχο ακεραιότητας. Αυτές οι επιθέσεις χαρακτηρίζονται από το μέγεθος των πακέτων που στέλνονται στο θύμα – υπολογιστή, είτε αυτά τα πακέτα είναι υπογεγραμμένα από έναν εξυπηρετητή, είτε περιέχουν πραγματικές οι ψεύτικες διευθύνσεις, είτε είναι κρυπτογραφημένα με ένα κλειδί.

Οι επιθέσεις DoS είναι δύσκολο να αντιμετωπιστούν, επειδή οι τηλεδιασκέψεις είναι άλλη μια υπηρεσία δικτύου, και είναι επιρρεπής σε μία επίθεση DoS όπως και κάθε άλλη υπηρεσία δικτύου. Επιπροσθέτως οι επιθέσεις DoS είναι ιδιαίτερα ενεργητικές απέναντι σε υπηρεσίες, όπως οι τηλεδιασκέψεις ή κάποια άλλη υπηρεσία πραγματικού χρόνου, επειδή αυτές οι υπηρεσίες είναι πιο ευαίσθητες στο κύρος του δικτύου. Οι ιοί και τα «σκουλήκια» εμπεριέχονται σε αυτή την κατηγορία αφού συνήθως προκαλούν DoS ή DDoS λόγω της αυξημένης κίνησης των πακέτων που δημιουργείται.

Για την αποφυγή αυτών των επιθέσεων και την αντιμετώπιση τους, μπορούν να χρησιμοποιηθούν διάφοροι τρόποι. Μια τέτοια λύση είναι η πολύ δυνατή αυθεντικοποίηση στα περιβάλλοντα τηλεδιάσκεψης, καθώς τα στοιχεία δρομολόγησης μηνύματος πρέπει να εμπιστεύονται και να δρομολογούν μηνύματα και από πιθανούς επιτιθέμενους. Μια άλλη λύση είναι η χρήση συστήματος

ανίχνευσης εισβολών (IPS – intrusion prevention system) το οποίο μπορεί να βοηθήσει σε συγκεκριμένους τύπους επιθέσεων DoS.

Ακόμη, οι διαχειριστές της ασφάλειας μπορούν να ελαχιστοποιήσουν τις πιθανότητες υλοποίησης αυτών των επιθέσεων έχοντας ενήμερα από πλευράς λογισμικού όλα τα IP τηλέφωνα και εξυπηρετητές.

Παρακάτω, παρεντίθεται μερικά είδη επιθέσεων DoS οι οποίες μπορούν να προκαλέσουν μερικώς ή εξ ολοκλήρου μη διαθεσιμότητα του συστήματος απορρίπτοντας την εγκαθίδρυση μιας επιτυχούς κλήσης.

Επανέναρξη σύνδεσης TLS - TLS Connection Reset

Για να πραγματοποιηθεί αυτή η επίθεση, αρκεί κάποιος να στείλει το κατάλληλο πακέτο και η σύνδεση θα διακοπεί και θα γίνει επανεκκίνηση της.

Επίθεση επανεκπομπής πακέτων τηλεδιάσκεψης - VoIP Packet Replay Attack

Σε αυτήν γίνεται καταγραφή και αντιγραφή των πακέτων της τηλεδιάσκεψης και αποστέλλονται ξανά με μια μικρή χρονική καθυστέρηση. Αυτή η επίθεση έχει ως αποτέλεσμα την μείωση της ποιότητας των κλήσεων.

Διείσδυση δεδομένων - Data Tunneling

Δεν είναι ακριβώς μια επίθεση, αλλά μια διείσδυση στα δεδομένα μέσω της φωνής χρησιμοποιώντας τον δρομολογητή. Μεταφέροντας τα σήματα του δρομολογητή μέσου ενός πακέτου δικτύου που χρησιμοποιεί παλμική κωδικοποίηση, η τηλεδιάσκεψη μπορεί να χρησιμοποιήσει μια τέτοια κλήση μέσω IP. Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για τη μη εξουσιοδοτημένη πρόσβαση των δεδομένων.

Επίθεση τροποποίησης της ποιότητας των υπηρεσιών - QoS Modification Attack

Η επίθεση αυτή τροποποιεί τα πεδία του πρωτοκόλλου ελέγχου πληροφοριών στα πακέτα δεδομένων της τηλεδιάσκεψης προκειμένου να μειωθεί η ποιότητα της φωνής ή να απορριφθεί η κλήση.

VoIP Packet Injection

Στην επίθεση αυτή στέλνονται ψεύτικα πακέτα τηλεδιάσκεψης στους τελικούς χρήστες με σκοπό να εκμαιεύσουν κάποιο διάλογο ή θόρυβο σε μια ενεργή κλήση.

Επίθεση άρνησης εξυπηρέτησης υπηρεσιών σε υποστηρικτικές υπηρεσίες - DoS against Supplementary Services

Εδώ πραγματοποιείται μια επίθεση άρνησης εξυπηρέτησης υπηρεσιών σε υπηρεσίες δικτύου από τις οποίες εξαρτάται η τηλεδιάσκεψη, όπως DHCP, DNS.

Πλημμύρα από πακέτα ελέγχου - Control Packet Flood

Σε αυτή την επίθεση γεμίζουν οι διακομιστές με πακέτα. Ο επιτιθέμενος γεμίζει την μνήμη του συστήματος με πακέτα τα οποία δεν έχουν να προσφέρουν τίποτα.

Άρνηση εξυπηρέτησης υπηρεσιών στο ασύρματο δίκτυο - Wireless DoS

Ο επιτιθέμενος δεν επιτρέπει στον τελικό χρήστη να συνδεθεί στο ασύρματο δίκτυο με σκοπό να πραγματοποιήσει κλήση τηλεδιάσκεψης.

Άρνηση εξυπηρέτησης υπηρεσιών με ψεύτικα μηνύματα - Bogus Message DoS

Εδώ στέλνονται στους διακομιστές ή ακόμα και στους τελικούς χρήστες ψεύτικα πακέτα τα οποία όμως μπορούν να προκαλέσουν αποσύνδεση ή καταλάβουν το δίκτυο επικοινωνιών.

Άρνηση εξυπηρέτησης υπηρεσιών με άκυρα πακέτα - Invalid Packet DoS

Σε αυτή την επίθεση στέλνονται στους διακομιστές ή ακόμα και στους τελικούς χρήστες άκυρα πακέτα τα οποία όμως μπορούν να προκαλέσουν αποσύνδεση ή καταλάβουν το δίκτυο επικοινωνιών.

Άρνηση εξυπηρέτησης υπηρεσιών με ψεύτικο λογισμικό - Immature Software DoS

Τα softphones είναι ευπαθή και μπορούν να εγκατασταθούν διάφορα ψεύτικα λογισμικά σε αυτά.

Άρνηση εξυπηρέτησης υπηρεσιών εφαρμογής πρωτοκόλλου τηλεδιάσκεψης - VoIP Protocol Implementation DoS

Σε αυτή την επίθεση δεν δίνεται η δυνατότητα στους τελικούς χρήστες να «τρέξουν» την εφαρμογή της τηλεδιάσκεψης.

Άρνηση εξυπηρέτησης υπηρεσιών με πακέτα θανάτου - Packet of Death DoS

Σε αυτή την επίθεση τερματίζουν οι διακομιστές με πακέτα. Ο επιτιθέμενος τερματίζει την μνήμη του συστήματος με πακέτα τα οποία δεν έχουν να προσφέρουν τίποτα, εξαντλώντας την μνήμη.

Άρνηση εξυπηρέτησης υπηρεσιών πλημμύρας στα τηλέφωνα IP - IP Phone Flood DoS
Εδώ στέλνεται ένας μεγάλος όγκος δεδομένων σε έναν μόνο τελικό χρήστη με αποτέλεσμα να εξαντλούνται από θέμα μνήμης όλες του οι υπηρεσίες με αποτέλεσμα να τερματίζεται η κλήση τηλεδιάσκεψης.

Πειρατεία και υποκλοπή κλήσης

Η υποκλοπή κλήσης και η παρακολούθηση είναι άλλες δύο κύριες θεωρήσεις στα δίκτυα τηλεδιάσκεψης. Η ταξινόμηση απειλών της VOIPSA (www.voipsa.org/Activities/taxonomy-wiki.php) ορίζει ότι η παρακολούθηση είναι μία μέθοδος με την οποία ένας επιτιθέμενος μπορεί να παρακολουθήσει ολόκληρη την σηματοδότηση μεταξύ δύο ή περισσοτέρων τελικών χρηστών, αλλά δεν μπορεί να εναλλάξει τα δεδομένα από μόνη της.

Η οικογένεια αυτών των απειλών βασίζεται στην απουσία της κρυπτογραφικής βεβαίωσης αιτήματος προέλευσης. Οι επιθέσεις σε αυτή την κατηγορία έχουν σκοπό να κλονίσουν την ακεραιότητα της συζήτησης. Η απειλή αυτή δείχνει την ανάγκη ύπαρξης υπηρεσιών ασφαλείας που ενεργοποιούν τις οντότητες οι οποίες αυθεντικοποιούν την προέλευσή τους και βεβαιώνουν το περιεχόμενο των μηνυμάτων τους.

Στα προηγούμενα χρόνια καθώς οι υπολογιστές είχαν αναπτύξει τις δυνατότητες τους και την δύναμή τους χρησιμοποιώντας το διαδίκτυο, οι διαχειριστές του διαδικτύου δημιούργησαν μια δομή ιεραρχικής πρόσβασης, η οποία αποτελείται από ένα μόνο δίαυλο για κάθε υπολογιστή για τον διαμοιρασμό των υπηρεσιών. Κάθε χρήστης του διαδικτύου έχει μια πιο αξιόπιστη και ασφαλή σύνδεση με εγγυημένο εύρος μετάδοσης δεδομένων. Η χρήση αυτής της δομής περιορίζει την ενεργητικότητα των εργαλείων καταγραφής πακέτων ή των αναλυτών των πρωτοκόλλων με σκοπό να μην δημιουργείται καθυστέρηση στην επικοινωνία της τηλεδιάσκεψης.

Πλαστογράφηση του ARP(Address Resolution Protocol- Πρωτόκολλο Ανάλυσης Διεύθυνσης)

Το ARP είναι ένα από τα βασικά πρωτόκολλα δικτύου. Γι' αυτό το λόγο, η δημοσίευση αυτών των πακέτων είναι ο πιο συχνός μηχανισμός επίθεσης στα δίκτυα τηλεδιάσκεψης. Οι περισσότεροι διαχειριστές διαδικτύου υποστηρίζουν ότι, εάν η

σύνδεση στο διαδίκτυο γίνεται ενσύρματα, τότε μειώνεται η πιθανότητα της παρακολούθησης του δικτύου και κατ' επέκταση η παράνομη καταγραφή ευαίσθητων πληροφοριών που ταξιδεύουν στο διαδίκτυο. Δυστυχώς, υπάρχουν πολλές τεχνικές και εργαλεία που επιτρέπουν την παρακολούθηση ακόμη και του ενσύρματου δικτύου, επειδή το ARP δεν απαιτεί αυθεντικοποίηση των ερωτημάτων.

Επί προσθέτως, επειδή το ARP είναι ένα μη στατικό πρωτόκολλο, πολλά λειτουργικά συστήματα το αναβαθμίζουν όταν δέχονται απάντηση από το ARP, ασχέτως αν είχαν στείλει ερώτημα ή όχι.

Ανάμεσα σε αυτές τις τεχνικές, επανεκατεύθυνση του ARP, πλαστογράφηση του ARP, πειρατεία του ARP και «δηλητηρίαση» του ARP, υπάρχουν σχετιζόμενες μέθοδοι για την διακοπή της εύρυθμης λειτουργίας του ARP. Αυτοί οι όροι συχνά διαπλέκονται και μπερδεύονται.[34]

3.3 Σύγκριση NetMeeting και Asterisk

Έχοντας μελετήσει όλες τις ευπάθειες και τα πιθανά προβλήματα που δημιουργούνται στο NetMeeting και στο Asterisk, θα πρέπει να πραγματοποιηθεί μια αντιπαράθεση και σύγκριση αυτών.

Όπως παρουσιάζεται ανωτέρω, και στα δύο εργαλεία μπορεί να υλοποιηθεί η επίθεση της άρνησης εξυπηρέτησης υπηρεσιών. Η διαφορά έγκειται στους λόγους για τους οποίους έχουμε αυτό το αποτέλεσμα. Από την πλευρά του NetMeeting, η άρνηση εξυπηρέτησης υπηρεσιών μπορεί να προκληθεί εξαιτίας άλλων συνεργαζόμενων προγραμμάτων. Στο Asterisk η επίθεση αυτή υλοποιείται μόνο όταν ο επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση στο ίδιο το πρόγραμμα.

Στο NetMeeting βασικό ρόλο συνιστά ο τρόπος σύνδεσης με το διαδίκτυο του υπολογιστή στον οποίο λειτουργεί. Αντιθέτως, το Asterisk δεν επηρεάζεται από τον τρόπο σύνδεσης στο διαδίκτυο.

Ακόμη, στο NetMeeting ο χρήστης όταν αυθεντικοποιηθεί και χαρακτηριστεί ως έμπιστος, τότε θεωρείται για πάντα έμπιστος. Από την άλλη πλευρά, στο Asterisk στον χρήστη ζητείται σε κάθε συνεδρία η αυθεντικοποίηση του και θεωρείται μη έμπιστος, μέχρι αποδείξεως του αντιθέτου.

Τέλος, οι περισσότερες επιθέσεις που πραγματοποιούνται στο NetMeeting έχουν ως στόχο την απόκτηση απομακρυσμένης πρόσβασης στον υπολογιστή που υλοποιείται η εφαρμογή του NetMeeting, ενώ στο Asterisk το μεγαλύτερο κακό αποτέλεσμα που μπορεί να επιτευχθεί είναι η πρόκληση της άρνησης εξυπηρέτησης υπηρεσιών.

3.4 Συμπεράσματα

Έχοντας παρουσιάσει και έχοντας κάνει σύγκριση των δύο βασικότερων εργαλείων που χρησιμοποιούνται στη τηλεδιάσκεψη, θα γίνει εξαγωγή των συμπερασμάτων για την χρήση τους.

Όταν μια επιχείρηση επιθυμεί την χρήση κάποιου εργαλείου εξ' αυτών για την πραγματοποίηση τηλεδιασκέψεων, θα πρέπει να παρακολουθεί και να ελέγχει, όχι μόνο το συγκεκριμένο εργαλείο, αλλά και όλες τις εφαρμογές που εκτελούνται στους υπολογιστές, στους οποίους υλοποιείται το εργαλείο, και σε όλο το δίκτυο της επιχείρησης.

Ακόμη, όταν κάποιος χρησιμοποιεί κάποιο από αυτά τα εργαλεία, θα πρέπει να είναι πολύ προσεκτικός και θα πρέπει να θεωρεί τον / τους συνομιλητή / συνομιλητές του μη έμπιστο μέχρι αποδείξεως του εναντίου. Επιπλέον, η χρήση μηχανισμών ασφαλείας μόνο στα συγκεκριμένα εργαλεία δεν αποτελεί πανάκεια. Θα πρέπει να εγκατασταθούν και επιπλέον υπηρεσίες και εργαλεία, τα οποία θα ενδυναμώσουν το σύστημα, ώστε να επιτευχθεί επικοινωνία μεγαλύτερης ασφάλειας με τον συνομιλητή.

Βάση των ανωτέρω, οι χρήστες των εργαλείων αυτών θα πρέπει να είναι σωστά εκπαιδευμένοι και να τηρούν τους κανόνες ασφαλείας ώστε να μην διατρέχουν τον κίνδυνο της απώλειας δεδομένων ή / και ευαίσθητων πληροφοριών.

Κεφάλαιο 4: Υλοποίηση προβλήματος ασφάλειας σε εργαλείο τηλεδιάσκεψης

Σε αυτό το κεφάλαιο θα περιγραφεί και θα αναλυθεί μια από τις πιο γνωστές επιθέσεις στα συστήματα τηλεδιάσκεψης, και ειδικότερα στο Asterisk, η μη – εξουσιοδοτημένη πρόσβαση σε λογαριασμό αυτού. Πριν προχωρήσουμε στην περιγραφή, θα παραθέσουμε τα χαρακτηριστικά του εξοπλισμού, αλλά και του λογισμικού που χρησιμοποιήσαμε για την υλοποίηση αυτής της επίθεσης στα πλαίσια της συγγραφής αυτής της πτυχιακής εργασίας.

4.1 Απαιτήσεις συστήματος & Απαιτούμενα εργαλεία

Για την υλοποίηση του παραδείγματος της επίθεσης, έγινε χρήση τριών προσωπικών υπολογιστών. Οι δύο από αυτούς χρησιμοποιήθηκαν για την πραγματοποίηση κλήσης τηλεδιάσκεψης, ενώ ο τρίτος χρησιμοποιήθηκε ως ο κακόβουλος χρήστης, δηλαδή ο επιτιθέμενος. Αναλυτικά τα χαρακτηριστικά παρατίθενται ακολούθως.

Ο πρώτος υπολογιστής που συμμετέχει στην τηλεδιάσκεψη έχει τις εξής τεχνικές προδιαγραφές:

- Επεξεργαστής Intel Pentium dual core processor T2310 (1.46 GHz, 1MB L2 Cache, 533MHz FSB)
- 2GB DDR2 μνήμη RAM (2x 1024MB)
- Κάρτα δικτύου Broadcom (R) 802.11b/g WLAN

Επίσης, το εγκατεστημένο λειτουργικό σύστημα είναι λογισμικό ανοιχτού κώδικα (open source) και συγκεκριμένα είναι η έκδοση Linux Ubuntu 12.04.

Ο δεύτερος υπολογιστής που συμμετέχει στην τηλεδιάσκεψη έχει τις εξής τεχνικές προδιαγραφές:

- Επεξεργαστής Intel Celeron mobile processor 575/585 (3 MB L2 cache, 2/2.13 GHz, 667 MHz FSB)
- 2 GB μνήμη RAM DDR2 SDRAM 667 MHz
- Κάρτα δικτύου Gigabit Ethernet supporting ASF (Alert Standard Format) 2.0

Επίσης, το εγκατεστημένο λειτουργικό σύστημα είναι λογισμικό ανοιχτού κώδικα (open source) και συγκεκριμένα είναι η έκδοση Linux Ubuntu 12.04.

Και στους δύο υπολογιστές, χρησιμοποιήθηκε το ίδιο λειτουργικό σύστημα, καθώς επίσης και την ίδια έκδοση λογισμικού του Asterisk, ώστε να αποφευχθεί τυχόν ασυμβατότητα στην επικοινωνία των δύο υπολογιστών που πραγματοποίησαν την κλήση τηλεδιάσκεψης. Ειδικότερα χρησιμοποιήθηκε το λειτουργικό σύστημα Linux, καθώς σε αυτό δίνεται η δυνατότητα στον χρήστη να παραμετροποιήσει το σύστημά του αναλόγως, ώστε να επιτύχει μεγαλύτερο βαθμό ασφάλειας. Επίσης, για το συγκεκριμένο είδος λειτουργικού συστήματος δεν υπάρχει μεγάλο εύρος ιομορφικού λογισμικού. Έτσι κάνοντας χρήση αυτού του λειτουργικού συστήματος και με την αντίστοιχη ρύθμιση του τείχους προστασίας, αλλά και του λογισμικού προστασίας από τους ιούς έγινε η υλοποίηση της επίθεσης.

Στους δύο υπολογιστές μεταξύ των οποίων πραγματοποιήθηκε η κλήση τηλεδιάσκεψης εγκαταστάθηκε το λογισμικό τηλεδιάσκεψης Asterisk, και ειδικότερα η έκδοση 11.2.1, η οποία είναι η τελευταία έκδοση κατά την πραγματοποίηση της επίθεσης στα πλαίσια αυτής της πτυχιακής εργασίας. Αξίζει να σημειωθεί ότι κάνοντας χρήση της τελευταίας έκδοσης του λογισμικού, αυτό σημαίνει ότι έχουν καλυφθεί και επιδιορθωθεί παλαιότερα κενά ασφαλείας και ευπάθειες.

Ο τρίτος υπολογιστής, που χρησιμοποιήθηκε για την υλοποίηση της επίθεσης και είχε τον ρόλο του επιτιθέμενου, έχει τις εξής τεχνικές προδιαγραφές:

- Επεξεργαστής Intel Core i5 – 3470 3.2 GHz
- 4 GB μνήμη RAM DDR3 1066 MHz
- Κάρτα δικτύου Realtek PCIe GBE Family Controller

Επίσης, το εγκατεστημένο λειτουργικό σύστημα είναι λογισμικό ανοιχτού κώδικα (open source) και συγκεκριμένα είναι η έκδοση Linux Ubuntu 12.04.

Ο λόγος που χρησιμοποιήθηκε η συγκεκριμένη έκδοση λειτουργικού συστήματος στον υπολογιστή – επιτιθέμενο είναι ότι αυτή η έκδοση είναι η κατάλληλη για μια επίθεση μη - εξουσιοδοτημένης πρόσβασης. Ακόμη, σε πραγματικές συνθήκες αν κάποιος θέλει να υλοποιήσει μια τέτοια επίθεση για τον οποιοδήποτε λόγο, τότε θα χρησιμοποιήσει παρόμοιο λειτουργικό σύστημα.

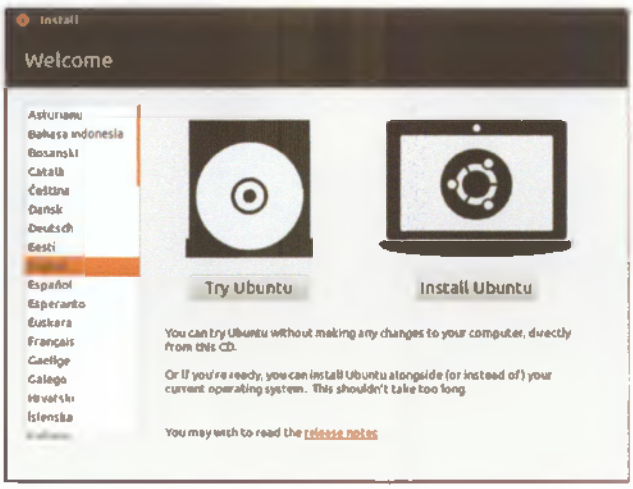
4.2 Εγκατάσταση - Υλοποίηση εργαλείων τηλεδιάσκεψης

Η εγκατάσταση του απαραίτητου λειτουργικού συστήματος (Ubuntu 12.04) και κατάλληλου λογισμικού χωρίζεται σε επιμέρους στάδια. Τα στάδια αυτά πρόκειται να τα αναλύσουμε διεξοδικώς ακολούθως.

Κατά το πρώτο στάδιο της διαδικασίας, θα γίνει περιγραφή της εγκατάστασης του απαιτούμενου λειτουργικού συστήματος που πραγματοποιήθηκε στους δύο υπολογιστές στους οποίους πραγματοποιήθηκε η κλήση τηλεδιάσκεψης.

Βήμα 1:

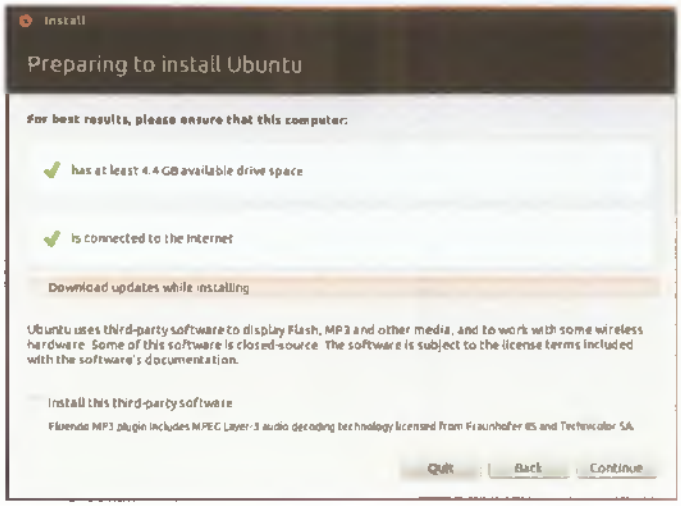
Αφού γίνει εκκίνηση στον υπολογιστή, γίνεται εισαγωγή του οπτικού δίσκου (CD) με το λειτουργικό σύστημα στον αναγνώστη δίσκων (DVD – ROM drive) και ζητείται από τον χρήστη να επιλέξει εάν θα γίνει δοκιμή ή εγκατάσταση του λειτουργικού συστήματος. (εικόνα 11)



Εικόνα 11

Βήμα 2:

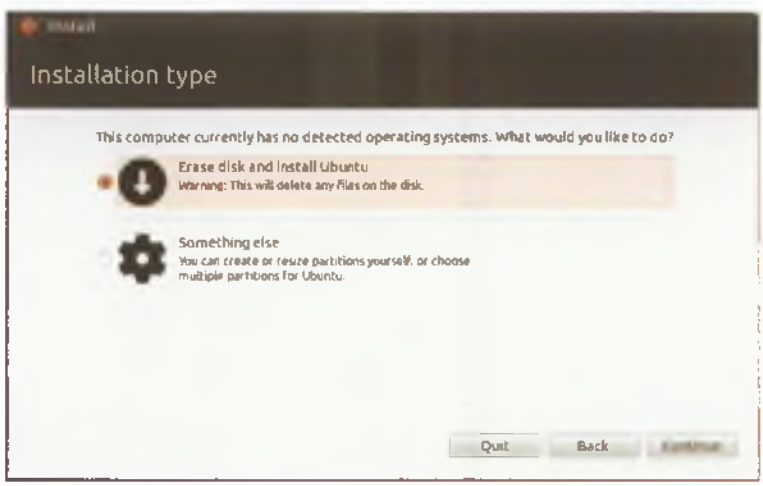
Στην συνέχεια γίνεται έλεγχος των απαιτούμενων προδιαγραφών στον υπολογιστή, με ιδιαίτερη έμφαση στο διαθέσιμο ελεύθερο χώρο του σκληρού δίσκου. (εικόνα 12)



Εικόνα 12

Βήμα 3:

Στο επόμενο παράθυρο διαλόγου ο χρήστης επιλέγει εάν επιθυμεί να διαγράψει το παλιό του λειτουργικό του σύστημα ή να τα διατηρήσει και τα δύο παράλληλα. Στην υλοποίηση της επίθεσης που πραγματοποιήθηκε, επιλέχθηκε και για τους δύο υπολογιστές η παράλληλη λειτουργία των λειτουργικών συστημάτων. (εικόνα 13)



Εικόνα 13

Βήμα 4:

Σε αυτή την φάση, έχοντας δημιουργηθεί το κατάλληλο διαμέρισμα στο σκληρό δίσκο, γίνεται η εγκατάσταση των ubuntu. (εικόνα 14)

Εικόνα 14

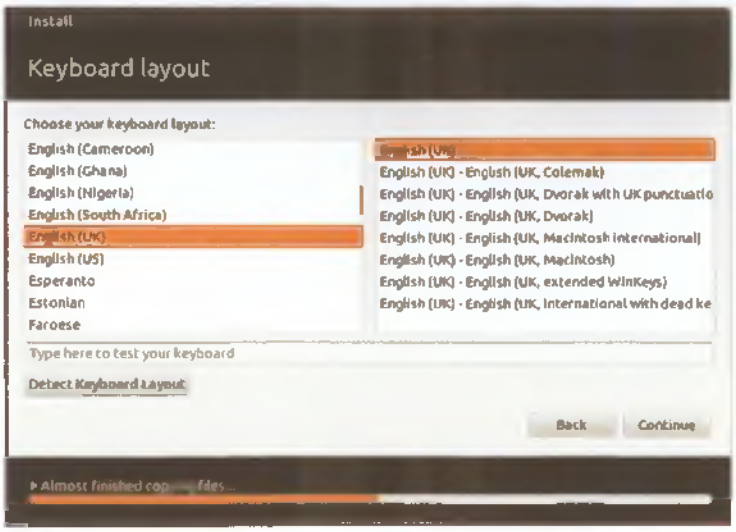
Βήμα 5:

Μετά ζητείται η εισαγωγή της ζώνης ώρας στην οποία βρίσκεται ο υπολογιστής. (εικόνα 15)

Εικόνα 15

Βήμα 6:

Έπειτα ο χρήστης επιλέγει την γλώσσα με την οποία πρόκειται να δουλέψει στον υπολογιστή. (εικόνα 16)



Εικόνα 16

Βήμα 7:

Στην επόμενη φάση ο χρήστης «βαφτίζει» τον υπολογιστή και δημιουργεί τον πρώτο λογαριασμό χρήστη, ο οποίος είναι και ο διαχειριστής του συστήματος. (εικόνα 17)

Εικόνα 17

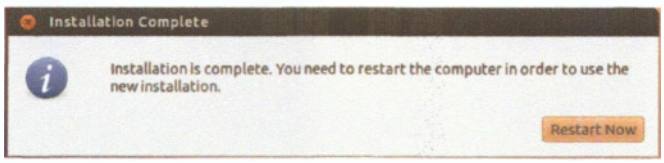
Βήμα 8:

Πλέον, εκκινεί η εγκατάσταση του λειτουργικού συστήματος. Κατά τη διάρκεια αυτής προβάλλονται διάφορες εικόνες οι οποίες πληροφορούν για τις δυνατότητες που παρέχει το λειτουργικό σύστημα. (εικόνα 18)

Εικόνα 18

Βήμα 9:

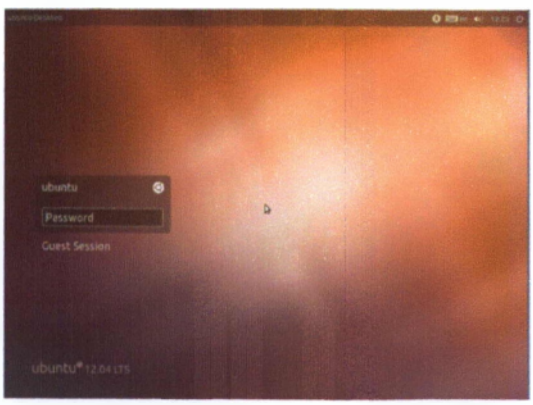
Αφού ολοκληρωθεί η εγκατάσταση, πραγματοποιείται η επανεκκίνηση του συστήματος. (εικόνα 19)



Εικόνα 19

Βήμα 10:

Σε αυτό το σημείο ο χρήστης εισέρχεται στο λειτουργικό σύστημα με τα προσωπικά του συνθηματικά. (εικόνα 20)

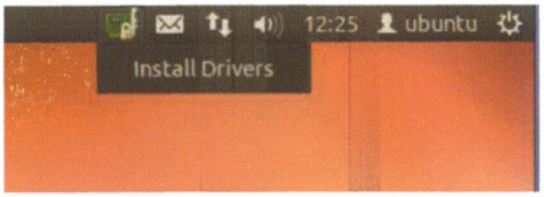


Εικόνα 20

Βήμα 11:

Αφού έχει επιτευχθεί η είσοδος στο λειτουργικό σύστημα, αυτό αναζητά πιθανές νέες ενημερώσεις λογισμικού, καθώς επίσης και ενημερώσεις για το υλικό (hardware). (εικόνα 21 και 22)

Εικόνα 21



Εικόνα 22

Αξίζει να σημειωθεί ότι η διαδικασία της εγκατάστασης που περιγράφηκε ανωτέρω, είναι η τυπική διαδικασία που ακολουθείται σε οποιονδήποτε υπολογιστή και αν γίνει αυτή.

Κατά το δεύτερο στάδιο της διαδικασίας, θα γίνει περιγραφή της εγκατάστασης του απαιτούμενου λογισμικού (Asterisk) για την πραγματοποίηση στους δύο υπολογιστές της κλήσης τηλεδιάσκεψης. Η διαδικασία αυτή αντλήθηκε από δύο ιστοτόπους, όπου γίνεται η περιγραφή αυτής αναλυτικά, καθώς δεν είναι μία απλή τυπική διαδικασία εγκατάστασης, αλλά χρειάζεται συγχρόνως και να πραγματοποιηθούν ενημερώσεις – αναβαθμίσεις κάποιων επιμέρους εφαρμογών – προγραμμάτων.

Βήμα 1:

Σε πρώτη φάση θα πρέπει να επιλυθούν κάποιες εξαρτίσεις που υπάρχουν στο σύστημα. Αυτό επιτυγχάνεται με την ακόλουθη εντολή που δακτυλογραφείται στο τερματικό παράθυρο (terminal):

```
apt-get install build-essential wget libssl-dev libncurses5-dev
libnewt-dev libxml2-dev linux-headers-$(uname -r) libsqlite3-dev
```

Βήμα 2:

Μετά γίνονται ενημερώσεις στις πιο πρόσφατες ενημερώσεις τον εξής εφαρμογών DAHDI, libpri and Asterisk.

Γίνεται είσοδος στον ακόλουθο φάκελο:

```
cd /usr/src/
```

και σε αυτό το σημείο κάνοντας την ακόλουθη πληκτρολόγηση, γίνονται οι αναβαθμίσεις.

```
wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-
complete/dahdi-linux-complete-current.tar.gz
```

```
wget http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-
current.tar.gz
```

```
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-
11-current.tar.gz
```

Βήμα 3:

Έχοντας πραγματοποιηθεί οι λήψεις, γίνεται η αποσυμπίεση αυτών με τις ακόλουθες εντολές:

```
tar zxvf dahdi-linux-complete*
```

```
tar zxvf libpri*
```

```
tar zxvf asterisk*
```

Βήμα 4:

Πλέον, μπορεί να πραγματοποιηθεί η εγκατάσταση του DAHDI

```
cd /usr/src/dahdi-linux-complete*

make && make install && make config
```

και η εγκατάσταση του libpri

```
cd /usr/src/libpri*

make && make install
```

και του Asterisk

```
cd /usr/src/asterisk*

./configure && make menuselect && make && make install && make config
&& make samples
```

Βήμα 5:

Αφού έχει πραγματοποιηθεί η εγκατάσταση, πραγματοποιείται η εκκίνηση του DAHDI

```
/etc/init.d/dahdi start
```

και του Asterisk συνδέοντας το με το CLI

```
/etc/init.d/asterisk start

asterisk -rvvv
```

Βήμα 6:

Μπορεί να γίνει επιβεβαίωση της εγκατάστασης των επιμέρους εκδόσεων λογισμικού με τις ακόλουθες εντολές:

```
*CLI> dahdi show version

*CLI> pri show version
```

4.3 Εγκατάσταση - Υλοποίηση εργαλείων επίθεσης

Για την υλοποίηση της επίθεσης μη – εξουσιοδοτημένης πρόσβασης στον υπολογιστή επιτιθέμενο, πέραν του λειτουργικού συστήματος και της πλατφόρμας τηλεδιάσκεψης, απαραίτητο εργαλείο για την υλοποίησή της είναι το SIPVicious.

Το SIPVicious είναι ένα σύνολο εργαλείων τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση (είτε με την καλή έννοια, για την εύρυθμη λειτουργία, είτε με την κακή έννοια, για υποκλοπή) συστημάτων τηλεδιάσκεψης βασισμένων στο πρωτόκολλο SIP, όπως προδίδει και η ονομασία του εργαλείου. Το εργαλείο αυτό αποτελείται από τα εξής επιμέρους εργαλεία:

- svmap: αυτό είναι ένα εργαλείο σάρωσης για συσκευές συγκεκριμένου εύρους IP που χρησιμοποιούν το πρωτόκολλο SIP
- svwar: αυτό το εργαλείο αναγνωρίζει ενεργές επεκτάσεις σε ένα PBX
- svcrack: με αυτό το εργαλείο υπάρχει η δυνατότητα εύρεσης του συνθηματικού σ' ένα πρωτόκολλο SIP και για να ενεργήσει σωστά θα πρέπει να είναι συνδεδεμένο στο διαδίκτυο
- svreport: αυτό το εργαλείο διαχειρίζεται τις συνεδρίες και εξάγει τεχνικές αναφορές σε διάφορους τύπους
- svcrash: το εργαλείο αυτό δίνει την δυνατότητα να σταματήσει τις μη – εξουσιοδοτημένες σαρώσεις από τα svwar και svcrack.

Το συγκεκριμένο εργαλείο για να μπορέσει να εγκατασταθεί και να λειτουργήσει σωστά, απαιτεί το σύστημα να μπορεί να υποστηρίξει τη γλώσσα Python 2.6 ή νεώτερη έκδοση.

Σε αυτό το σημείο θα περιγραφεί η διαδικασία εγκατάστασης του ανωτέρω εργαλείου. Πρώτα θα πρέπει μέσω του τερματικού να μεταβεί ο χρήστης στον προσωρινό φάκελο.

```
cd /tmp
```

Ακολούθως, ο χρήστης δίνει την παρακάτω εντολή:

```
wget http://sipvicious.googlecode.com/files/sipvicious-0.2.8.tar.gz
```

και γίνεται λήψη του εργαλείου. Τέλος, ο χρήστης αποσυμπιέζει το αρχείο το οποίο έκανε λήψη,

```
tar xvfz sipvicious-0.2.8.tar.gz
```

και μπαίνει στον φάκελο

```
cd sipvicious-0.2.8
```

4.4 Πραγματοποίηση επίθεσης - Αποτελέσματα επίθεσης

Η επίθεση της μη – εξουσιοδοτημένης πρόσβασης υλοποιήθηκε σε υπολογιστές του ίδιου δικτύου και ήταν γνωστές οι διευθύνσεις IP. Ακόμη, τα συνθηματικά στις επεκτάσεις είναι μόνο αριθμοί.

Για την υλοποίηση της επίθεσης θα πρέπει να αναζητηθεί και να βρεθεί ο server του Asterisk. Αυτή η αναζήτηση θα πραγματοποιηθεί από το svmap.py, το οποίο σαρώνει και τις διευθύνσεις IP οι οποίες είναι φραγμένες (μη ορατές στο δίκτυο). Η εντολή με την οποία ενεργοποιείται το svmap είναι:

```
./svmap.py asteriskdemo
```

Μετά την υλοποίηση της παραπάνω εντολής, όπου δίνεται το hostname και η IP διεύθυνση του Asterisk server, εξάγονται τα εξής αποτελέσματα:

```
| SIP Device          | User Agent | Fingerprint                                |
-------------------------------------------------------------------------------
|asteriskdemo:5060|Asterisk PBX|Asterisk/SJphone/1.60.289a (SJ Labs)|
```

Τώρα, θα πρέπει ο επιτιθέμενος να ελέγξει τις επεκτάσεις που χρησιμοποιούνται στο server, και αυτό υλοποιείται με το εργαλείο svwar.py πληκτρολογώντας την εντολή:

```
./svwar.py -e 1000-9999 asteriskdemo
```

Δίνοντας την παράμετρο «`-e 1000-9999`», το svwar σαρώνει όλες τις επεκτάσεις μεταξύ αυτών των αριθμών. Τα αποτελέσματα αυτού του εργαλείου είναι:

```
| Extension | Authentication |

-----------------------------

| 1003      | reqauth        |

| 1002      | reqauth        |

| 1001      | noauth         |
```

Ο πίνακας, που εξάγεται, πληροφορεί τον επιτιθέμενο ποιες επεκτάσεις υπάρχουν και αν είναι παραμετροποιημένες και ζητούν συνθηματικό για την σύνδεση στο Asterisk. Όπως φαίνεται και στα αποτελέσματα, η επέκταση 1001 δεν ζητά συνθηματικό. Έτσι δυναμικά ως κακόβουλος χρήστης, ο επιτιθέμενος μπορεί να συνδεθεί στο Asterisk και να πραγματοποιήσει κλήσεις.

Ο επιτιθέμενος, χρησιμοποιώντας το εργαλείο svcrack.py, προσπαθεί να αναζητήσει αν υπάρχουν άλλες πιθανές επεκτάσεις με ευπάθειες. Έτσι, δίνει την εντολή:

```
./svcrack.py -u1002 -r1-9999 asteriskdemo
```

Χρησιμοποιώντας την παράμετρο «`-u1002`», ο επιτιθέμενος δίνει την εντολή να αναζητηθεί το συνθηματικό της επέκτασης, και με την παράμετρο «`-r1-9999`» λέει να χρησιμοποιηθεί αυτό ως μια σειρά από πιθανούς συνδυασμούς πρόσβασης. Απαιτούνται τρία (3) δευτερόλεπτα ώστε να δοκιμαστούν όλοι οι πιθανοί συνδυασμοί και να αποκαλυφθεί το συνθηματικό.

```
| Extension | Password |

------------------------

| 1002      | 1002     |
```

Υπάρχει η δυνατότητα επίσης, να ληφθούν αρχεία λεξιλογίων και να δοθεί η εντολή στο SIPVicious να τα χρησιμοποιήσει ως συνθηματικά. Βέβαια, ενεργώντας κάποιος επιτιθέμενος με αυτό τον τρόπο, είναι προφανές ότι ο χρόνος αποκάλυψης των συνθηματικών αυξάνεται.

4.5 Αντίμετρα – Αντιμετώπιση επίθεσης

Γενικότερα, θα πρέπει οι χρήστες τον προγραμμάτων τηλεδιάσκεψης να υπακούουν στους γενικότερους κανόνες ασφαλείας, αλλά και οι διαχειριστές των συστημάτων να θέσουν συγκεκριμένους κανόνες καλής λειτουργίας αυτών, όπως συστήματα ανίχνευσης εισβολών, τείχη προστασίας, χρήση εικονικών ιδιωτικών δικτύων (VPN), και άλλα παρόμοια. Όσον αφορά την ενδυνάμωση του Asterisk και την προστασία των χρηστών μπορούν να πραγματοποιηθούν δύο βασικά σημεία.

Πρώτα απ' όλα, συνίσταται οι χρήστες να χρησιμοποιούν συνθηματικά μεγαλύτερου μήκους, ώστε να δυσκολεύει η αποκάλυψη των συνθηματικών και να αυξάνεται εκθετικά ο χρόνος αυτής. Επίσης, θα ήταν προτιμότερο οι χρήστες να εντάξουν στα συνθηματικά τους και γράμματα του λατινικού αλφαβήτου, είτε πεζά είτα μικρά, καθώς και τους επονομαζόμενους «ειδικούς» χαρακτήρες. Έχοντας εντάξει ένας χρήστης τους παραπάνω κανόνες για το συνθηματικό, τότε εάν δεχτεί επίθεση μη – εξουσιοδοτημένης πρόσβασης τότε ο χρόνος που θα απαιτηθεί για την αποκάλυψη του συνθηματικού του από τον επιτιθέμενο, ο οποίος μπορεί να χρησιμοποιεί και λεξικά κωδικών, θα είναι εξαιρετικά μεγάλος λόγω της ποικιλίας των χαρακτήρων του συνθηματικού.

Επίσης, ένα δεύτερο βασικό βήμα που πρέπει να παραμετροποιηθεί στο Asterisk είναι να μην αποκαλύπτει σε έναν σαρωτή SIP ποιες επεκτάσεις είναι έγκυρες. Για να πραγματοποιηθεί αυτό, θα πρέπει ο χρήστης να τροποποιήσει το αρχείο /etc/asterisk/sip_custom.conf και να εισάγει την εξής εντολή:

```
alwaysauthreject=yes
```

Αφού αποθηκεύσουμε τις αλλαγές στο αρχείο, τότε επαναφορτώνουμε το SIP στο Asterisk πληκτρολογώντας τις ακόλουθες εντολές :

```
asterisk -rv
sip reload
exit
```

Τώρα, αν κάποιος κακόβουλος χρήστης επαναλάβει την παραπάνω επίθεση, τότε δίνοντας την εντολή:

```
./svwar.py -e 1000-9999 asteriskdemo
```

θα λάβει ως αποτέλεσμα το εξής σφάλμα:

```
ERROR:TakeASip:SIP server replied with an authentication request for
an unknown extension. Set --force to force a scan.
WARNING:root:found nothing
```

Έτσι, πλέον, οι χρήστες του Asterisk είναι πιο ασφαλείς σε σχέση με την προηγούμενη κατάσταση, πριν την παραμετροποίηση. [41][42][43]

4.6 Συμπεράσματα

Μετά την εμπειρία της υλοποίησης της ανωτέρω επίθεσης και ενδυναμώνοντας το Asterisk, γίνεται αντιληπτό ότι θα πρέπει να πραγματοποιηθεί η κατάλληλη εκπαίδευση των χρηστών, όσον αφορά τα συνθηματικά στις επεκτάσεις, καθώς και των διαχειριστών των συστημάτων που ελέγχουν την εύρυθμη λειτουργία του Asterisk. Αυτό αντλείται από το ότι έγινε αδύνατη η ανάγνωση σωστών αποτελεσμάτων από το svmap, όταν πραγματοποιήθηκε στο Asterisk τροποποίηση όσον αφορά την αυθεντικοποίηση των χρηστών. Ακόμη, όταν οι χρήστες χρησιμοποίησαν συνθηματικά με μεγαλύτερο μήκος και μεγαλύτερο εύρος χαρακτήρων, το svcrack δεν μπορούσε να εξάγει αποτελέσματα.

Η ίδια η επίθεση μπορεί να πραγματοποιηθεί με το εργαλείο Sipautohack, το οποίο είναι ένα εργαλείο που ανακαλύπτει τις «τρύπες» και αποκαλύπτει τα συνθηματικά των επεκτάσεων. Το Sipautohack μπορεί να ενεργήσει πιο αποτελεσματικά σε σύγκριση με το SIPVicious.

Κεφάλαιο 5: Συμπεράσματα

5.1 Η ασφάλεια στα πρωτόκολλα και στα εργαλεία τηλεδιάσκεψης

Έχοντας φτάσει στο τέλος αυτής της εργασίας, θα πρέπει να συνοψίσουμε τα εξαχθέντα αποτελέσματα της σύγκρισης των πρωτοκόλλων και των εργαλείων σε συνδυασμό με την υλοποίηση της επίθεσης.

Τα πρωτόκολλα, που χρησιμοποιούνται στην τηλεδιάσκεψη, είναι ένα από τα βασικότερα συστατικά της. Όπως αναφέραμε και στο δεύτερο κεφάλαιο. υπάρχουν σημαντικά ζητήματα ασφαλείας σε αυτά, τα οποία θα πρέπει να τα διαχωρίσουμε σε ποιο πρωτόκολλο αντιστοιχούν. Τα προβλήματα που αναφέρονται στο SIP μπορούν εν δυνάμει να αντιμετωπιστούν, καθώς είναι ένα πρωτόκολλο το οποίο συνεχώς αναπτύσσεται και μπορεί να θωρακιστεί καλύτερα. Τα προβλήματα που αναφέρονται στο H.323 είναι πιο δύσκολο να αντιμετωπιστούν, καθώς δεν δημοσιεύονται νέες εκδόσεις του πρωτοκόλλου αυτού.

Ένα δεύτερο και πολύ σημαντικό συστατικό των συστημάτων της τηλεδιάσκεψης είναι τα εργαλεία που την υλοποιούν. Στα πλαίσια της εργασίας έγινε μελέτη των πιο γνωστόν εργαλείων που χρησιμοποιούνται στις επιχειρήσεις, το NetMeeting και το Asterisk. Όπως γίνεται αντιληπτό και από την μελέτη του τρίτου κεφαλαίου. τα προβλήματα που αντιμετωπίζουν τα εργαλεία είναι διαφορετικής φύσεως μεν, αλλά ίδιας σημαντικότητας δε. Τα προβλήματα του NetMeeting δημιουργούνται από τις συνεργαζόμενες εφαρμογές, ενώ στο Asterisk τα προβλήματα αφορούν το ίδιο το εργαλείο και κυρίως τους λογαριασμούς των χρηστών. Στο Asterisk τα περισσότερα προβλήματα που δημιουργούνται, οδηγούν στη μη – εξουσιοδοτημένη πρόσβαση σε λογαριασμό, όπως στην επίθεση που υλοποιήθηκε στο τέταρτο κεφάλαιο.

Η επίθεση που πραγματοποιήσαμε υλοποιήθηκε στο πιο γνωστό εργαλείο τηλεδιάσκεψης, το Asterisk, το οποίο για να λειτουργήσει χρησιμοποιεί το πρωτόκολλο SIP, που όπως αναφέραμε και στην παράγραφο 2.4 είναι το αναπτυσσόμενο πρωτόκολλο και κατά την άποψη μου το πιο ασφαλές. Παρ' όλα αυτά, τα αποτελέσματα της επίθεσης έδειξαν ότι η χρήση του πρωτοκόλλου SIP δεν απέτρεψε την υλοποίηση αυτής.

Αυτό, μας οδηγεί στο συμπέρασμα ότι η μεμονωμένη μελέτη του κάθε επιμέρους συστατικού της τηλεδιάσκεψης σε θέματα ασφαλείας, δεν μας βοηθά – καθοδηγεί

στα σωστά συμπεράσματα για την πραγματοποίηση των κατάλληλων ενεργειών για την ενδυνάμωση του συστήματος τηλεδιάσκεψης.

5.2 Μελλοντική εργασία

Μετά την μελέτη των πρωτοκόλλων τηλεδιάσκεψης H.323 και SIP, καθώς και των εργαλείων τηλεδιάσκεψης NetMeeting και Asterisk, και μετά την πραγματοποίηση της επίθεσης της μη – εξουσιοδοτημένης πρόσβασης στο Asterisk, θα μπορούσε κάποιος να μελετήσει περαιτέρω το Asterisk όταν είναι βασισμένο στο πρωτόκολλο H.323.

Επίσης, λόγω των τελευταίων αλλαγών στον παγκόσμιο χάρτη των πλατφορμών τηλεδιάσκεψης, και την αντικατάσταση του NetMeeting από το Skype (Μάρτιος 2013 η οριστική αντικατάσταση), θα ήταν ιδιαίτερα ενδιαφέρον να μελετηθεί η ασφάλεια και γενικότερα τα πιθανά προβλήματα και οι ευπάθειες του Skype.

Βιβλιογραφία

Δημοσιεύσεις

[1] Δασκόπουλος Δημήτρης - Καρακούσης Απόστολος - Φεργάδης Γιώργος, «Υποδομές Τηλεδιάσκεψης για Διαχειριστές», Κέντρο Λειτουργίας Δικτύου Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2010

[2] Dan Moniz, «Alternative Thinking in H.323 Capable Firewall Design», Phrack Magazine Vol.9, 1999

[3] Xinyu Xing - Jianxun Dang - Richard Han - Xue Liu - Shivakant Mishra, «Intrusions into Privacy in Video Chat Environments: Attacks and Countermeasures», University of Colorado at Boulder, 2010

[4] Hong Yan - Hui Zhang - Kunwadee Sripanidkulchai - Zon-Yin Shae - Debanjan Saha, «Information Leak Vulnerabilities in SIP Implementations», IEEE, 2006

[5] The Asterisk Company, «Asterisk Quick Start Guide», Digium, 2012

[6] Π. Κασαπίδης - Κ. Βασιλάκης - Μ. Νικολαΐδου - Π. Γεωργιάδης - Γρ. Βότσης - Ν. Πρόνιος, «Συγκριτική Μελέτη Πρωτοκόλλων Επιπέδου Μεταφοράς Για Εφαρμογές Πολυμέσων»

Τεχνικές Αναφορές

[7] Αγιωτάκης Δημήτριος, «Μελέτη και υλοποίηση συστήματος τηλεφωνίας μέσω διαδικτύου (VOIP)», ΤΕΙ Κρήτης, 2011

[8] Αλμπανάκης Αστέριος, «Ζητήματα και απαιτήσεις ασφάλειας συστημάτων VoIP», Πανεπιστήμιο Μακεδονίας, 2011

[9] Αναγνωστόπουλος Ιωάννης, «VoIP H.323 / SIP», Εθνικό Μετσόβιο Πολυτεχνείο, 2009

[10] Γεροβασίλης Βασίλης, «Μελέτη και ανάπτυξη εφαρμογής VoIP (Voice over IP) ή/και VVoIP (Voice and Video over IP) με τη χρήση του SIP πρωτοκόλλου», Πανεπιστήμιο Πατρών, 2009

[11] Γκουγκούσης Σωτήριος- Κριμνήτσας Ευγένιος- Σαλονικίδης Κων/νος, «Standards for multimedia conferencing & Multimedia network transmission standards», Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, 2001

[12] Δασκόπουλος Δημήτρης - Καρακούσης Απόστολος - Φεργάδης Γιώργος, «Ανάπτυξη υπηρεσιών τηλεδιάσκεψης με open-source λογισμικό», Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Μάιος 2006

[13] Καρακατσάνης Χρήστος - Αργυριάδης Περικλής, «Asterisk», Τ.Ε.Ι. Θεσσαλονίκης, 2008

[14] Κατσανικάκης Χρήστος, «Μελέτη ασφάλειας και υλοποίησης σε IMS/SIP συστήματα», Πανεπιστήμιο Πειραιά, 2011

[15] Κυριαζοπούλου Χριστιάνα, «Φωνή επί Διαδικτυακού Πρωτοκόλλου Voice over Internet Protocol», Εργασία στα πλαίσια του μαθήματος «Δίκτυα Υπολογιστών», Πανεπιστήμιο Μακεδονίας Οικονομικών και Κοινωνικών Επιστημών, Ιανουάριος 2011

[16] Λεοντιάδης Ηρακλής, «Ανωνυμία σε SIP δίκτυα», Οικονομικό Πανεπιστήμιο Αθηνών, 2009

[17] Μπούρας Χρήστος - Τσιάτσος Θρασύβουλος, «Τεχνολογίες και Πρότυπα για την Υλοποίηση Συνεργατικών Συστημάτων», Πανεπιστήμιο Πατρών και ΕΑΙΤΥ

[18] ΟΤΕ Α.Ε., «Προηγμένες Τηλεπικοινωνιακές Υποδομές και Υπηρεσίες» (τόμος Β)

[19] Ροζή Ευαγγελία, «Μελέτη πρωτοκόλλων και εργαλείων τηλεδιάσκεψης», Διπλωματική Εργασία, Τμήμα Μηχανικών ΗΥ & Πληροφορικής Πανεπιστημίου Πατρών, 2007

[20] Σουρέλη Ασπασία, «Τηλεφωνία- εικονοτηλεφωνία- τηλεδιάσκεψη», Εργασία στα πλαίσια του μαθήματος «Σχεδίαση και μελέτη υλοποίηση δικτύων» Τμήμα Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Ιανουάριος 2012

[21] Στυλιάδης Κ. – Ορόβας Χ., «Το Πρόγραμμα Επικοινωνίας NetMeeting», Κέντρο ΠΛΗ.ΝΕ.Τ. Ν. Φλώρινας

[22] Τζιγκουνάκης Παύλος, «Συστήματα Τηλεδιάσκεψης», Τμήμα Πληροφορικής ΕΕΤΤ

[23] Τρουλάκη Ανδρονίκη, «Μελέτη του πρωτοκόλλου SIP σε ασύρματο κανάλι επικοινωνίας», Πανεπιστήμιο Πειραιώς, 2008

[24] Ψιαχούλιας Αργύριος, «Εφαρμογές του πρωτοκόλλου SIP στην πλατφόρμα Asterisk», Πανεπιστήμιο Πειραιώς, 2008

[25] Mark D. Collier, «Session Initiation Protocol (SIP) Vulnerabilities», IPComm, 2006

[26] Frost & Sullivan, «Delivering on the promise of easy to use, secure, and inexpensive video conferencing in an IP environment», 2010

[27] Sandro Gauci, «How to exploit the SIP Digest Leak vulnerability», 2009

[28] James M. Hayes, «Microsoft NetMeeting 3.0 Security Assessment and Configuration Guide», National Security Agency USA, 2001

[29] Microsoft Team, «NetMeeting Guide», Microsoft

[30] Jason Ostrom - Arjun Sambamoorthy, «Advancing Video Attacks», Viper Lab, 2009

[31] Kewin Stoeckight, «Overcoming Firewall & NAT problems in H.323», QUESTnet 2005

[32] Symantec group, «H.323 Mediated Voice over IP: Protocols, Vulnerabilities & amp; Remediation», 2010

[33] Wainhouse Research, «The CIO's Guide to Videoconferencing Security: Keeping Pace with DoF», 2010

Βιβλία

[34] Chaffin Larry – Long Johnny, «Asterisk Hacking», Sun Gress, 2007

[35] Leif Madsen – Jim Van Meggelen – Smith Jared, «Asterisk: The definitive Guide», 2nd edition, O'Reilly, 2007

[36] Leif Madsen – Jim Van Meggelen – Russell Bryant, «Asterisk: The definitive Guide» - Chapter 26, 3rd edition, O'Reilly, 2011

Ιστοσελίδες

[37] http://www.technicalreview.gr/index.php?option=com_content&task=view&id=487

[38] http://www.javvin.com/protocolH235.html

[39] http://vivliothmmy.ee.auth.gr/18/1/VoIP.doc

[40] http://www.essortment.com/security-risks-netmeeting-139381.html

[41] http://blogs.digium.com/2012/11/14/how-to-install-asterisk-11-on-ubuntu-12-4-lts/

[42] http://www.kartook.com/2012/05/ubuntu-how-to-install-asterisk-10-on-ubuntu-12-04-lts/

[43] http://code.google.com/p/sipvicious/