ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΚΑΤΕΥΘΥΝΣΗ : "ΨΗΦΙΑΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ & ΔΙΚΤΥΑ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ VOIP

Ονοματεπώνυμο : Φαφούλα Ιωάννα

Α.Μ: ΜΕ0558

Επιβλέπων: Κάτσικας Σωκράτης, Καθηγητής Πανεπιστημίου Πειραιώς

ΠΕΙΡΑΙΑΣ

ΙΟΥΝΙΟΣ 2008

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία μελετά θέματα ασφαλείας στην VoIP τεχνολογία. Στο πρώτο μέρος γίνεται ανάλυση της τεχνολογίας σε θεωρητικό επίπεδο με στοιχεία από διάφορες πηγές. Περιλαμβάνονται ο ορισμός της VoIP τεχνολογίας, τα δομικά της στοιχεία, καθώς και τα βασικότερα πρωτόκολλα σηματοδοσίας της. Ακολουθεί αναλυτική περιγραφή των επιθέσεων που είναι δυνατόν να πραγματοποιηθούν ενάντια στην σηματοδοσία. Τέλος, μελετώνται οι μηχανισμοί προστασίας ενάντια στις διάφορες επιθέσεις.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: ΑΣΦΑΛΕΙΑ

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: VoIP, SIP, H.323, MGCP, MeGaCo/H.248, TLS, DTLS, S/MIME, IPSec

Περιεχόμενα

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών του τμήματος Διδακτικής της Τεχνολογίας και Ψηφιακών συστημάτων του Πανεπιστημίου Πειραιώς (Κατεύθυνση Ψηφιακές Επικοινωνίες και Δίκτυα), σε συνεργασία με τον Καθηγητή του τμήματος κ. Κάτσικα Σωκράτη. Το αντικείμενο ουσιαστικά εμπίπτει στον ορισμό και στην ανάπτυξη των θεμάτων ασφάλειας της VoIP τεχνολογίας. Επίσης γίνεται μελέτη των μηχανισμών ασφάλειας στην σηματοδοσία.

Πειραιάς, Ιούνιος 2008

Η συγγραφέας,
Φαφούλα Π. Ιωάννα

Εισαγωγή

Η υπηρεσία Voice over IP (VoIP) χρησιμοποιεί το πρωτόκολλο του Διαδικτύου (Internet Protocol) για να μεταφέρει τηλεφωνικές συνομιλίες, μετατρέποντας τη φωνή σε πακέτα δεδομένων. Το υπάρχον μοντέλο τηλεπικοινωνιών επικεντρώνεται στη φωνή και την παροχή σχετικών υπηρεσιών, στην ασύρματη και ενσύρματη τηλεφωνία. Η υπηρεσία Voice over IP αποτελεί μέρος των υπηρεσιών μετάδοσης σε πραγματικό χρόνο, η οποία τείνει να αντικαταστήσει τη συμβατική τεχνολογία του τηλεφώνου ανατρέποντας τα δεδομένα και τις τιμές των τηλεφωνικών υπηρεσιών παγκοσμίως. Η αρχή πάνω στην οποία στηρίζεται η λειτουργία της μετάδοσης φωνής μέσω IP είναι ότι ο πελάτης πληρώνει ένα ορισμένο ποσό για να συνδεθεί στο δίκτυο και στη συνέχεια πληρώνει ανάλογα με το χρόνο χρήσης και τις χρησιμοποιούμενες εγκαταστάσεις (βάσει της απόστασης).

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

Πολλές ευρωπαϊκές -και ελληνικές- εταιρίες τηλεπικοινωνιών έχουν αρχίσει να επενδύουν δυναμικά στο Voice over IP. Μέχρι το 2009 όλες οι υπηρεσίες των εταιρειών αυτών (φωνή, fax, μεταφορά δεδομένων, video conferencing κ.λπ.) θα παρέχονται μόνο μέσω IP.

Η νέα υπηρεσία χρησιμοποιείται ευρέως σε επιχειρήσεις του εξωτερικού. Σύμφωνα με μελέτες, υπολογίζεται ότι μέσα στα επόμενα χρόνια η ανάπτυξη της φωνής μέσω Internet θα είναι ραγδαία και ο όγκος κίνησης θα είναι μεγαλύτερος απ' ότι στην παραδοσιακή τηλεφωνία. Οι προμηθευτές τηλεπικοινωνιακού εξοπλισμού έχουν ξεκινήσει να συμπεριλαμβάνουν στα προϊόντα τους και το πρωτόκολλο IP, ενώ όλοι

οι προμηθευτές εξοπλισμού IP συμπεριλαμβάνουν τη φωνή ως ένα από τα βασικά χαρακτηριστικά των προϊόντων τους.

Παρακάτω αναφέρονται μερικές πρόσθετες υπηρεσίες και εφαρμογές που υποστηρίζονται μέσω της VoIP τεχνολογίας:

- Επικοινωνία μέσω μηνυμάτων. Δυνατότητα επικοινωνίας με πελάτες μέσω ηλεκτρονικών μηνυμάτων, φαξ και ευφυών φωνητικών μηνυμάτων (φωνητικό ταχυδρομείο) μέσα σε ένα και μόνο φάκελο αλληλογραφίας (inbox).
- Πρόσβαση στο ηλεκτρονικό ταχυδρομείο μέσω τηλεφώνου (κινητού και σταθερού), με χρήση της τεχνολογίας μετατροπής "κειμένου σε ομιλία" (text to speech).
- Το κέντρο επικοινωνίας IP προσφέρει υπηρεσίες έξυπνης δρομολόγησης κλήσεων, μεταφορά τηλεφωνικών κλήσεων από το δίκτυο στον προσωπικό υπολογιστή και διαχείριση των επαφών με πολυμέσα για την επικοινωνία με τους αντιπροσώπους του κέντρου μέσω δικτύου IP.
- Αυτόματη διανομή κλήσεων και ενσωμάτωση με βάσεις δεδομένων.
- Ομαδική τηλεφωνική συνδιάσκεψη.
- Διατήρηση των εσωτερικών τηλεφωνικών αριθμών χωρίς να είναι απαραίτητη η ύπαρξη τμήματος υποστήριξης για τη διεκπεραίωση των αλλαγών αυτών (δυνατότητα μεταφοράς εσωτερικού αριθμού).
- Υπηρεσίες καταλόγου για την απευθείας επιλογή εσωτερικού τηλεφώνου, χωρίς η διαδικασία να πραγματοποιείται μέσω του τηλεφωνικού κέντρου.
- Τοποθέτηση της υπηρεσίας υποδοχής σε οποιοδήποτε σημείο. Κάποιος εργαζόμενος σε ένα απομακρυσμένο γραφείο μπορεί να αναλάβει τη διεκπεραίωση των υπηρεσιών υποδοχής, εάν παραστεί ανάγκη.

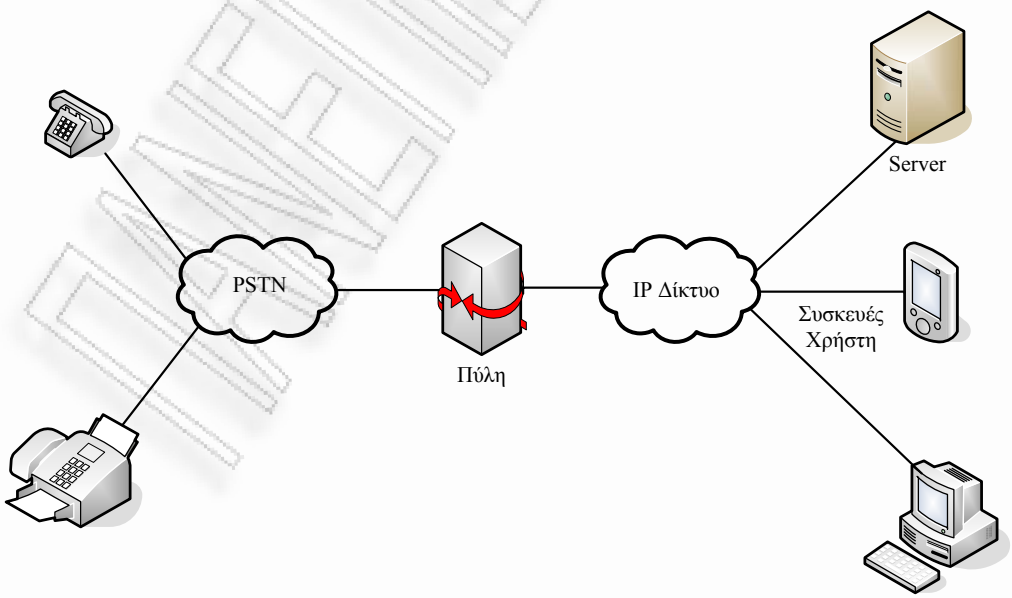
Την VoIP τεχνολογία χρησιμοποιούν και πολλές εφαρμογές τύπου άμεσης αποστολής μηνυμάτων (instant messaging) και συνομιλίας. Οι εφαρμογές αυτές παρέχουν τη δυνατότητα αποστολής και λήψης ψηφιακών πακέτων φωνής, παίζοντας ουσιαστικά ρόλο τηλεφώνου μέσω του Διαδικτύου.

1ο Κεφάλαιο - Δομικά στοιχεία και πρωτόκολλα του VoIP

1.1. VoIP δομικά στοιχεία

Σήμερα, οι εφαρμογές VoIP, γίνονται μέσω ποικίλων συσκευών, πρωτοκόλλων και διαμορφώσεων. Η VoIP τεχνολογία μπορεί να χρησιμοποιηθεί για να εγκαταστήσει κλήσεις μεταξύ: ενός υπολογιστή και ενός παραδοσιακού τηλέφωνου, ενός υπολογιστή και ενός άλλου υπολογιστή, ενός παραδοσιακού τηλέφωνου και ενός άλλου παραδοσιακού τηλέφωνου (η φωνή πακετάρεται και ταξιδεύει μέσω του IP δικτύου), ενός VoIP τηλέφωνου και ενός άλλου υπολογιστή, και ενός παραδοσιακού τηλέφωνου ή VoIP τηλέφωνου.

Τα σημαντικότερα συστατικά ενός VoIP δικτύου διευκρινίζονται στην εικόνα 1. Η πύλη(gateway) μετατρέπει τα σήματα από τις παραδοσιακές διεπαφές τηλεφωνίας σε VoIP. Ο κεντρικός υπολογιστής(server) παρέχει τη διαχείριση και τις διοικητικές λειτουργίες για την υποστήριξη της δρομολόγησης των κλήσεων μέσα στο δίκτυο. Το IP δίκτυο παρέχει τη σύνδεση μεταξύ όλων των τερματικών. Μπορεί να είναι ένα ιδιωτικό δίκτυο, ένα ενδοεταιρικό, ή Διαδίκτυο. Ο εξοπλισμός των τελικών χρηστών αποτελείται από τερματικά που υποστηρίζουν VoIP εφαρμογές και μπορούν να συνδεθούν άμεσα με ένα IP δίκτυο.



Εικόνα 1: Τα κυριότερα συστατικά του VoIP

1.2. VoIP πρωτόκολλα

Κατά μια απλοϊκή άποψη, η Voice over IP τεχνολογία έχει ως στόχο την δημιουργία και τον έλεγχο των συνεδριών επικοινωνίας για την μετάδοση δεδομένων φωνής, ή ήχου γενικότερα, μέσω του IP δικτύου. Η VoIP τεχνολογία μπορεί πρόσθετα να υποστηρίξει τις μεταδόσεις άλλων μορφών δεδομένων όπως βίντεο, κείμενο ή εικόνες. Μια σταθερή και αξιόπιστη μετάδοση πρέπει να διατηρηθεί καθ' όλη τη διάρκεια της συνομιλίας, και η συνεδρία πρέπει να τερματιστεί όταν οποιοδήποτε μέρος με την αναγκαία δικαιοδοσία αποφασίσει περί αυτού.

Η εργασία της παρακίνησης των τελικών κόμβων του καλούμενου για την εγκατάσταση μιας επικοινωνίας ή μιας συνεδρίας κλήσης αφήνεται στα χέρια των πρωτοκόλλων σηματοδοσίας.

Τα δύο δημοφιλή και ανταγωνιστικά πρωτοκόλλα σηματοδοσίας για την παράδοση των πολυμέσων είναι το H.323 και session initiation protocol SIP. Το H.323 πρότυπο καθορίζεται από την ITU ενώ το SIP είναι το πνευματικό δημιούργημα του IETF. Στη βιομηχανία κυρίως προτιμούν το SIP σε σχέση με το H.323 λόγω της απλότητας και της ευελιξίας του. Ο πίνακας 1 παρουσιάζει μερικές σαφείς διαφορές μεταξύ των δύο πρωτοκόλλων στην προσφορά τους για την επίτευξη των εξής στόχων:

- Η παροχή ικανοτήτων που απαιτούνται στην οργάνωση, διαχείριση, και διακοπή κλήσεων και συνδέσεων.
- Υποστήριξη της ικανότητας επέκτασης για έναν πολύ μεγάλο αριθμό καταχωρημένων τελικών σημείων, και ταυτόχρονων κλήσεων (της τάξεως των εκατομμυρίων παγκοσμίως).
- Υποστήριξη των χαρακτηριστικών διαχείρισης δικτύου για την πολιτική ελέγχου, τη λογιστική, την τιμολόγηση, κ.λπ.
- Παροχή μηχανισμών για την επικοινωνία και την οργάνωση της ποιότητας εξυπηρέτησης (Quality of Service) που απαιτείται από τα τελικά σημεία.
- Επεκτασιμότητα στην προώθηση προσθήκης νέων χαρακτηριστικών ευκολότερα

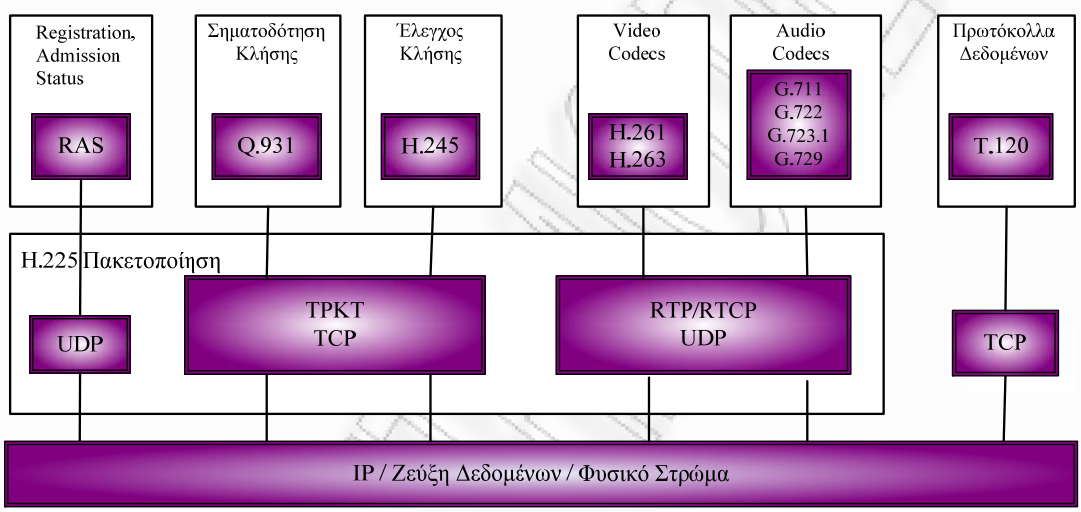
	H.323	**SIP**
Συστατικά	Terminal/Gateway	UA
	Gatekeeper	Servers
Πρωτόκολλα	RAS/Q.931	SIP
	H.245	SDP
Πρωτόκολλο μεταφοράς	Αξιόπιστο ή αναξιόπιστο, π.χ., TCP ή UDP. Οι περισσότερες H.323 οντότητες χρησιμοποιούν μια αξιόπιστη μεταφορά για τη σηματοδότηση.	Αξιόπιστο ή αναξιόπιστο, π.χ., TCP ή UDP. Οι περισσότερες SIP οντότητες χρησιμοποιούν μια αναξιόπιστη μεταφορά για τη σηματοδότηση.
Κωδικοποίηση μηνύματος	Το H.323 κωδικοποιεί τα μηνύματα σε ένα συμπαγές δυαδικό σχήμα, κατάλληλο για τις περιορισμένης ζώνης και ευρυζωνικές συνδέσεις.	Τα SIP μηνύματα κωδικοποιούνται σε ASCII κείμενο, κατάλληλο για να διαβαστεί.
Διευθυνσιοδότηση	Εύκαμπτοι μηχανισμοί διευθυνσιοδότησης, συμπεριλαμβανομένων URLs και E.164 αριθμών.	Το SIP καταλαβαίνει μόνο τις URL-style διευθύνσεις.

Πίνακας 1: Διαφορές μεταξύ του SIP και του H.323

Τα πρωτόκολλα σηματοδοσίας περνούν από τρεις φάσεις, την οργάνωση, την διαπραγμάτευση των παραμέτρων επικοινωνίας και την διακοπή επικοινωνίας. Η πρώτη φάση είναι γνωστή ως το στάδιο έναρξης όπου ο καλών πρώτα έρχεται σε επαφή με τον καλούμενο για να συμφωνήσουν να επικοινωνήσουν. Η δεύτερη φάση χρησιμοποιείται για να διαπραγματευτεί και να ανταλλάξει τις παραμέτρους της κλήσης που και οι δύο άκρες θα χρησιμοποιήσουν στην επικοινωνία. Οι κύριες πληροφορίες που ανταλλάσσονται πρέπει να περιέχουν το σχήμα του κωδικοποιητή/αποκωδικοποιητή που θα χρησιμοποιηθεί, τον αριθμό της UDP πόρτας για τον προσδιορισμό και το πρωτόκολλο που θα χρησιμοποιηθεί για τη συνομιλία. Η τρίτη φάση χρησιμοποιείται για να τερματίσει την επικοινωνία μετά από τη συνομιλία.

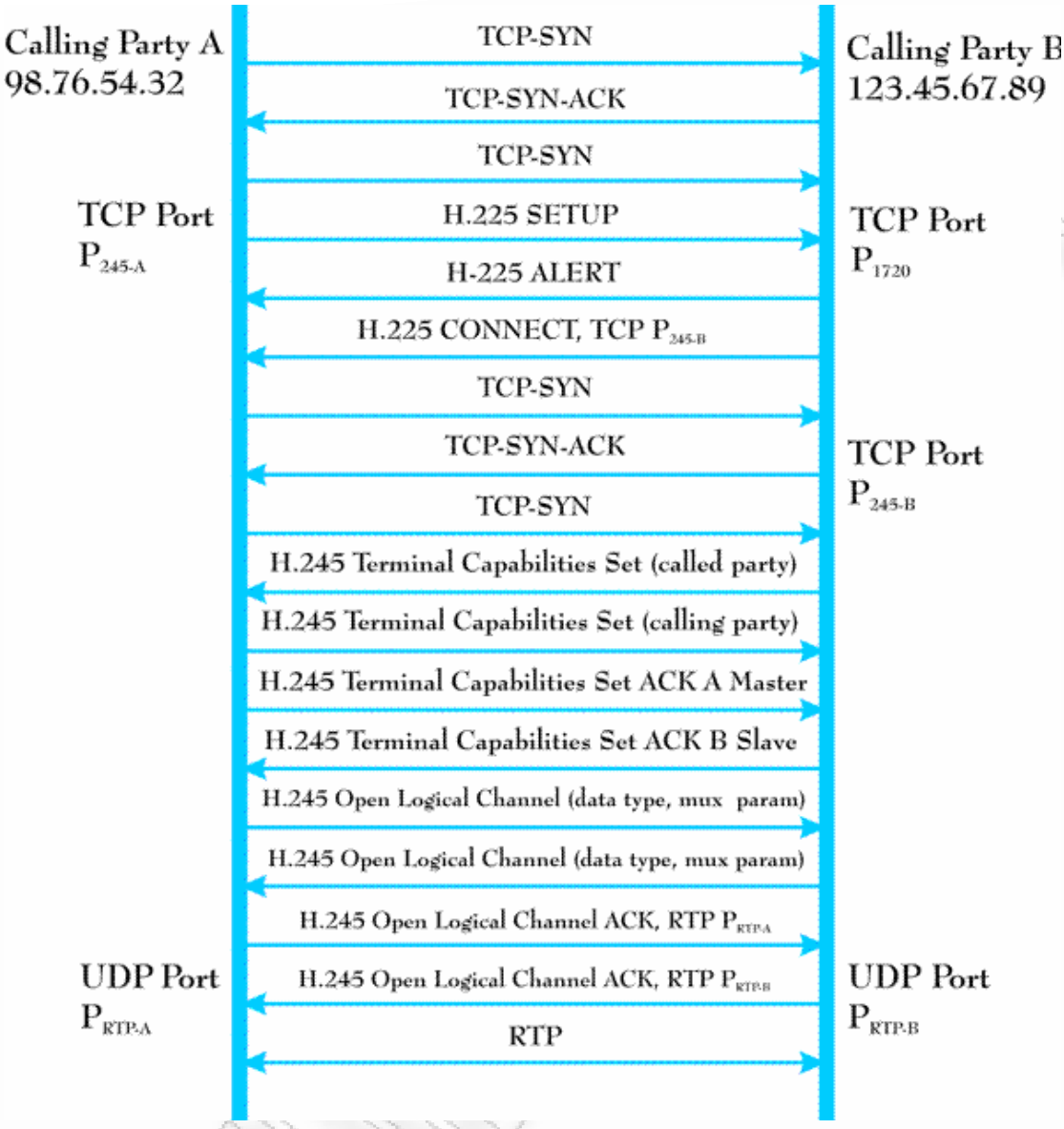
1.2.1. H.323 οικογένεια πρωτοκόλλων

Το H.323 είναι ένα σύνολο συστάσεων από την International Telecommunication Union (ITU) και αποτελείται από μία οικογένεια πρωτοκόλλων που χρησιμοποιούνται για την εγκατάσταση της κλήσης, τη λήξη της κλήσης, την εγγραφή, την αυθεντικοποίηση και άλλες λειτουργίες. Αυτά τα πρωτόκολλα μεταφέρονται μέσω των πρωτοκόλλων TCP ή UDP. Το ακόλουθο διάγραμμα παρουσιάζει τα βασικότερα H.323 πρωτόκολλα με τους μηχανισμούς μεταφορών τους:



Εικόνα 2: H.323 οικογένεια πρωτοκόλλων

Αυτά τα πρωτόκολλα μπορούν να υποδιαιρεθούν περαιτέρω σε δύο κατηγορίες – στα πρωτόκολλα που χρησιμοποιούνται για τη σηματοδοσία της κλήσης (Q.931, H.225, H.245, H.235, RTCP) και το πρωτόκολλο που μεταφέρει τη συμπιεσμένη κυκλοφορία της φωνής (RTP). Η ακόλουθη εικόνα επεξηγεί την τυπική οργάνωση και μεταφορά δεδομένων φωνής χρησιμοποιώντας την οικογένεια H.323 πρωτοκόλλων.



Εικόνα 3: Εγκατάσταση κλήσης και μεταφορά δεδομένων φωνής μέσω του H.323

Το H.323 χρησιμοποιεί το H.225 πρωτόκολλο για την αρχική σηματοδοσία. Μετά από την αρχική σηματοδοσία, το H.245 χρησιμοποιείται για να συνεχίσει τη διαπραγμάτευση των ικανοτήτων και των ιδιοτήτων των media. Και τελικά, τα μέσα μεταφέρονται χρησιμοποιώντας το Real-time Transport Protocol (RTP).

Συστατικά του H.323

Το H.323 καθορίζει τέσσερα λογικά συστατικά δηλαδή, τα τερματικά, τις πύλες (Gateways), τους Gatekeepers και την Multipoint Control Units (MCUs). Τα

τερματικά, οι πύλες και οι MCUs είναι γνωστά ως τελικά σημεία και παρουσιάζονται παρακάτω.

- **Τερματικά**

Αυτά είναι τα τελικά σημεία του LAN client που παρέχουν σε πραγματικό χρόνο επικοινωνίες διπλής κατεύθυνσης. Όλα τα H.323 τερματικά πρέπει να υποστηρίζουν τα H.245, Q.931, Registration Admission Status (RAS) και Real Time Transport Protocol (RTP). Το H.245 χρησιμοποιείται για την άδεια της χρήσης των καναλιών, το Q.931 απαιτείται για την σηματοδοσία και την δημιουργία της κλήσης, το RTP είναι πρωτόκολλο μεταφοράς σε πραγματικό χρόνο που μεταφέρει τα πακέτα φωνής ενώ το RAS χρησιμοποιείται για την αλληλεπίδραση με τον gatekeeper. Τα H.323 τερματικά μπορούν επίσης να περιλαμβάνουν τα T.120 πρωτόκολλα δεδομένων σύσκεψης, τους βίντεο κωδικοποιητές/αποκωδικοποιητές και την υποστήριξη για την MCU. Ένα H.323 τερματικό μπορεί να επικοινωνήσει με είτε ένα άλλο H.323 τερματικό, μια H.323 πύλη είτε μία MCU.

- **Πύλες**

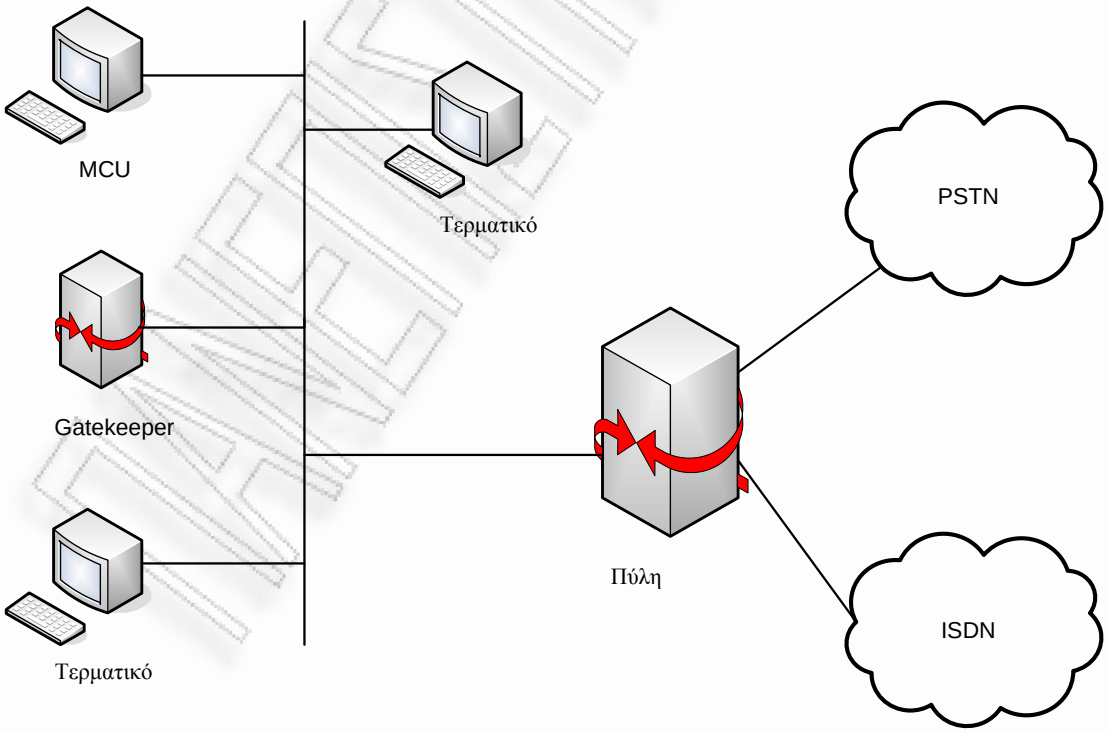
Μια H.323 πύλη είναι ένα τελικό σημείο στο δίκτυο που παρέχει σε πραγματικό χρόνο, επικοινωνίες διπλής κατεύθυνσης μεταξύ των H.323 τερματικών στο IP δίκτυο και άλλων ITU τερματικών σε ένα δίκτυο μεταγωγής, ή σε μια άλλη H.323 πύλη. Εκτελούν το ρόλο του «μεταφραστή» δηλ. εκτελούν τη μετάφραση μεταξύ διαφορετικών μορφών μετάδοσης, π.χ. από H.225 σε H.221. Είναι επίσης σε θέση να μεταφράσουν μεταξύ των κωδικοποιητών/αποκωδικοποιητών ήχου και βίντεο. Η πύλη είναι η διεπαφή μεταξύ του PSTN και του Διαδικτύου. Παίρνει τη φωνή από το κύκλωμα μεταγωγής PSTN και την τοποθετεί στο δημόσιο διαδίκτυο και αντίστροφα. Οι πύλες είναι προαιρετικές δεδομένου ότι τα τερματικά σε ένα ενιαίο τοπικό LAN μπορούν να επικοινωνήσουν το ένα με το άλλο άμεσα. Όταν τα τερματικά σε ένα δίκτυο πρέπει να επικοινωνήσουν με ένα τελικό σημείο σε κάποιο άλλο δίκτυο, τότε επικοινωνούν μέσω των πυλών χρησιμοποιώντας τα πρωτόκολλα H.245 και Q.931.

- **Gatekeepers**

Είναι το πιο ζωτικής σημασίας συστατικό του H.323 συστήματος και εκτελεί τα καθήκοντα ενός «διευθυντή». Ενεργεί ως κεντρικό σημείο για όλες τις κλήσεις μέσα στη ζώνη του (η ζώνη A είναι η συνάθροιση του gatekeeper και των τελικών σημείων που εγγράφονται σε αυτή) και παρέχει υπηρεσίες στα καταχωρημένα τελικά σημεία.

- **Multipoint Control Units (MCU)**

Το MCU είναι ένα τελικό σημείο στο δίκτυο που παρέχει την ικανότητα σε τρία ή και περισσότερα τερματικά και πύλες να συμμετάσχουν σε μια διάσκεψη πολλών σημείων. Το MCU αποτελείται από ένα υποχρεωτικό Multipoint Controller (MC) και προαιρετικούς Multipoint Processors (MP). Το MC καθορίζει τις κοινές ικανότητες των τερματικών με τη χρησιμοποίηση του H.245 αλλά δεν εκτελεί την πολυπλεξία ήχου, βίντεο και δεδομένων. Η πολυπλεξία των media streams υποστηρίζεται από το MP υπό τον έλεγχο του MC. Η ακόλουθη εικόνα παρουσιάζει τις αλληλεπιδράσεις μεταξύ όλων των συστατικών του H.323



Εικόνα 4: Αλληλεπιδράσεις μεταξύ των συστατικών του H.323

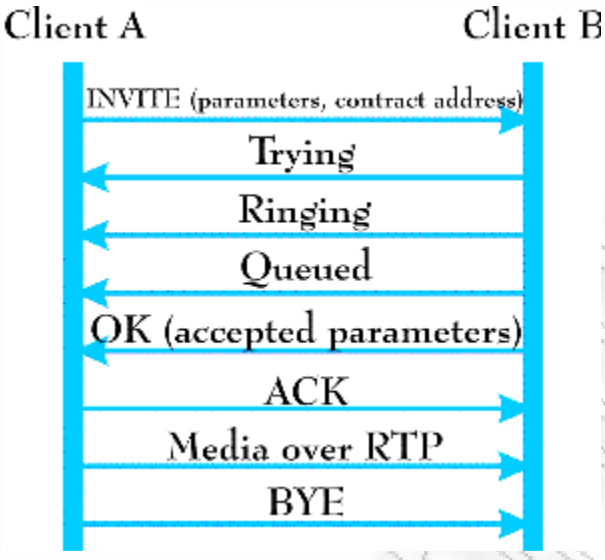
1.2.2. Session Initiation Protocol (SIP)

Το Session Initiation Protocol (SIP) καθορίστηκε από την Internet Engineering Task Force (IETF) για τη δημιουργία, την τροποποίηση και τη λήξη των συνεδριών μεταξύ δύο ή περισσότερων συμμετεχόντων. Αυτές οι συνεδριάσεις δεν περιορίζονται στις VoIP κλήσεις. Το SIP πρωτόκολλο είναι ένα text-based πρωτόκολλο παρόμοιο με το HTTP, και προσφέρει μια εναλλακτική λύση στα σύνθετα πρωτόκολλα της H.323 οικογένειας. Υποστηρίζει και το UDP και το TCP ως πρωτόκολλα μεταφοράς. Εκτός από τη σηματοδοσία, χρησιμοποιείται επίσης για instant messaging. Λόγω της απλούστερης φύσης του, το SIP γίνεται δημοφιλέστερο από την H.323 οικογένεια πρωτοκόλλων και πιθανώς να καταστεί το κυρίαρχο πρότυπο στα ερχόμενα έτη.

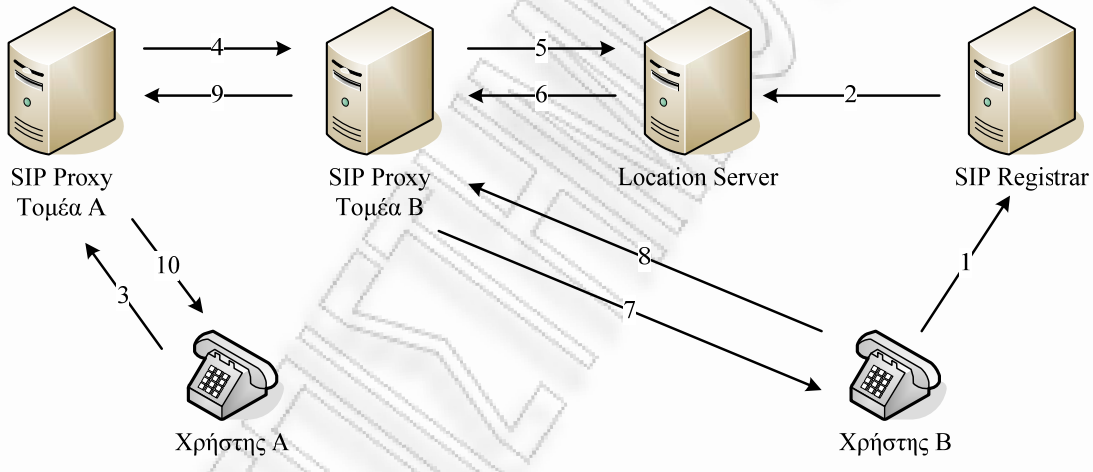
Σε αντίθεση με πολλά παραδοσιακά IP πρωτόκολλα, οι VoIP εφαρμογές απαιτούνται για να εφαρμόσουν τη λειτουργία και του server και του client. Στο SIP, οποιαδήποτε SIP οντότητα μπορεί να αρχίσει και να τερματίσει μια SIP συνεδρία. Αυτό στηρίζεται στο χωρισμό του SIP σε δύο μέρη: στον user-agent-server (UAS) και στον user-agent-client (UAC). Ο UAC αρχίζει μια συνεδρία με την αποστολή των SIP μηνυμάτων σηματοδοσίας στις server-side εφαρμογές του UAS. Ο UAC αφουγκράζεται συνέχεια για εισερχόμενες SIP συνδέσεις.

Η αρχιτεκτονική ενός SIP δικτύου είναι διαφορετική από τη δομή του H.323. Ένα SIP δίκτυο αποτελείται από τα τελικά σημεία (τερματικά, User Agents - UA), έναν proxy server (για τη μετάδοση μηνυμάτων των τελικών σημείων), τον location server (για την εντόπιση των χρηστών), και το registrar (για την καταχώρηση των πληροφοριών θέσης). Ο registrar και ο location server μπορούν να ενσωματωθούν στον proxy server.

Μια εφαρμογή του SIP τυπικά χρησιμοποιεί έναν proxy server για την έναρξη των κλήσεων για λογαριασμό ενός χρήστης ή ενός VoIP τηλεφώνου, και έναν location server για τον εντοπισμό της θέσης ενός τελικού χρήστη. Οι παρακάτω εικόνες επεξηγούν μία τυπική κλήση βασισμένη στο SIP πρωτόκολλο:



Εικόνα 5: Εγκατάσταση κλήσης και μεταφορά δεδομένων φωνής μέσω του SIP



Εικόνα 6: SIP Κλήση υπό εξέλιξη

Συστατικά του SIP

Το SIP σύστημα αποτελείται από δύο συστατικά:

- **User Agents:**

Ένας user agent είναι ένα τελικό σύστημα που ενεργεί για λογαριασμό ενός χρήστη. Υπάρχουν δύο μέρη: ένας client και ένας server. Η μερίδα των client καλείται User

Agent Client (UAC) ενώ η μερίδα των server καλείται User Agent Server (UAS). Το UAC χρησιμοποιείται για να αρχίσει ένα SIP αίτημα ενώ το UAS χρησιμοποιείται για να λάβει τα αιτήματα και να επιστρέψει τις απαντήσεις για λογαριασμό του χρήστη.

- **Network Servers:**

Υπάρχουν τρεις τύποι servers μέσα σε ένα δίκτυο. Ένας server εγγραφής που λαμβάνει τις αναπροσαρμογές σχετικά με τις τρέχουσες θέσεις των χρηστών. Ένας proxy server στη λήψη αιτημάτων και στην συνέχεια στην προώθηση τους στον server του επόμενου hop, ο οποίος έχει περισσότερες πληροφορίες για τη θέση του καλούμενου μέρους. Ένας redirect server στη λήψη αιτημάτων, και καθορίζει τον server του επόμενου hop και επιστρέφει τη διεύθυνση του server του επόμενου hop στον client αντί της προώθησης του αιτήματος.

Μηνύματα SIP

Το SIP χρησιμοποιεί τα μηνύματα για τις προσκλήσεις κλήσης στην οργάνωση και στον τερματισμό μιας σύνδεσης. Αυτά τα μηνύματα είναι κυρίως κείμενο που βασίζονται και διαιρούνται σε δύο μέρη αποτελούμενα από την επιγραφή και το σώμα. Η επιγραφή δίνει πληροφορίες σχετικά με τον τύπο του μηνύματος που συνήθως είναι ο INVITE, τον τύπο του πρωτοκόλλου, π.χ SIP έκδοση 2.0, τις διευθύνσεις των τελικών σημείων, και τον τύπο σώματος του μηνύματος. Το σώμα του μηνύματος μεταβιβάζει μια περιγραφή των multimedia ικανοτήτων της συνεδρίας που ο καλών επιθυμεί να πραγματοποιήσει.

Τα μηνύματα είναι είτε server είτε client αιτήματα ή απαντήσεις. Τα σχήματα των μηνυμάτων έχουν κανονικά μια γραμμή έναρξης και μερικά πεδία επιγραφής που αποτελούν την επιγραφή. Αυτό ακολουθείται από το σώμα του μηνύματος και απεικονίζεται στις εικόνες 7 και 8. Οι γραμμές μιας έναρξης χρησιμοποιούν μια από τις έξι μεθόδους αιτήματος ή τους κώδικες απάντησης για να υποδείξουν τον τύπο μηνύματος.

SIP αιτήματα και απαντήσεις

Το SIP χρησιμοποιεί τα αιτήματα για την επικοινωνία μεταξύ του client και του SIP server. Αυτά τα αιτήματα είναι:

- **INVITE:** Υποδεικνύει έναν χρήστη ή μια υπηρεσία που καλείται για να συμμετάσχει σε μια συνεδρία κλήσης.
- **ACK:** Επιβεβαιώνει ότι ο client έχει λάβει μια τελική απάντηση σε ένα INVITE αίτημα.
- **BYE:** Ολοκληρώνει μια κλήση και μπορεί να σταλεί είτε από τον καλούντα είτε από τον καλούμενο.
- **CANCEL:** Ακυρώνει οποιεσδήποτε εκκρεμείς αναζητήσεις αλλά δεν τερματίζει μια κλήση που έχει ήδη γίνει αποδεκτή.
- **OPTIONS:** Ρωτάει τις ικανότητες των servers.
- **REGISTER:** Καταχωρεί τη διεύθυνση που απαριθμείται στο **TO** πεδίο της επιγραφής σε έναν SIP server.

Οι ακόλουθοι τύποι απαντήσεων χρησιμοποιούνται από το SIP και παράγονται από τον SIP Proxy Server:

- **SIP 1xx:** Πληροφοριακές Αποκρίσεις
- **SIP 2xx**: Αποκρίσεις Επιτυχίας
- **SIP 3xx:** Αποκρίσεις Επανακατεύθυνσης
- **SIP 4xx:** Αποτυχίες Αίτησης
- **SIP 5xx:** Σφάλματα Server
- **SIP 6xx:** Καθολικές Αποτυχίες

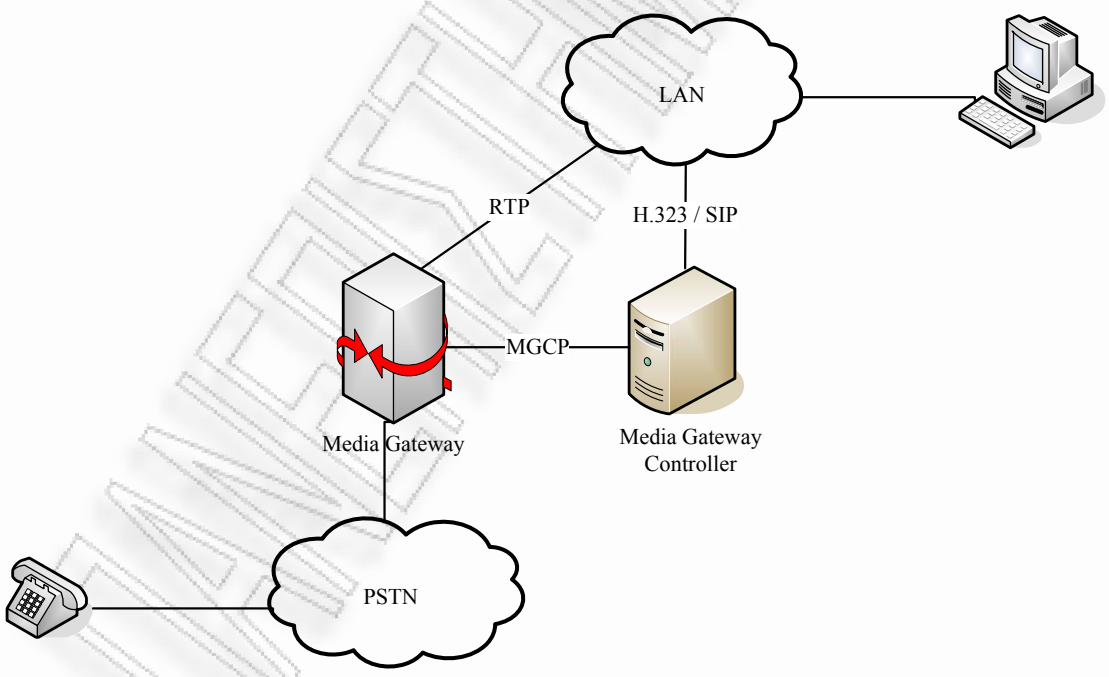
Εικόνα 7: Ένα SIP μήνυμα αιτήματος

Εικόνα 8: Ένα SIP μήνυμα απάντησης

1.2.3. MGCP και MeGaCo/H.248

Τα MGCP και Megaco/H.248 είναι πρωτόκολλα ελέγχου με σκοπό να διαχειριστούν κεντρικά τις Media πύλες που υπάρχουν σε μια VoIP υποδομή. Μια Media πύλη εκτελεί τις εντολές που στέλνονται από τον Media Gateway Controller (MGC) και είναι σχεδιασμένη για την μετατροπή των δεδομένων μεταξύ του PSTN σε IP, PSTN σε ATM, ATM σε IP, και επίσης IP σε IP.

Τα MGCP και Megaco/H.248 παρέχουν μηχανισμούς για την διασύνδεση με άλλα VoIP δίκτυα, και επίσης διευκολύνουν μεγάλης κλίμακας εφαρμογές του VoIP. Τα MGCP και Megaco/H.248 μπορούν να χρησιμοποιηθούν στην οργάνωση, στην διατήρηση και στον τερματισμό των κλήσεων μεταξύ πολλαπλών τερματικών σημείων, καθώς και στον έλεγχο όλων των γεγονότων και των συνδέσεων που συσχετίζονται με αυτά τα τερματικά από το MGC.



Εικόνα 9: Media Gateway και Media Gateway Controller

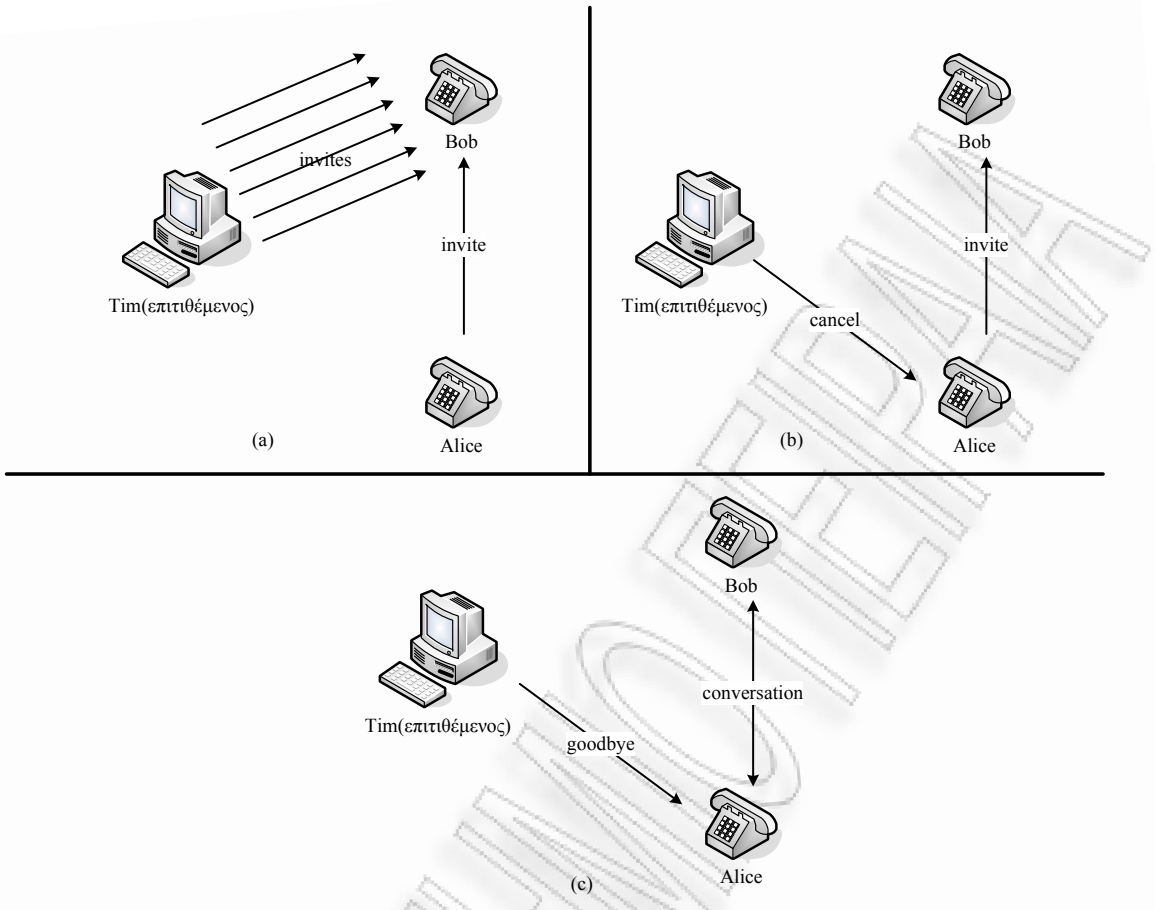
2ο Κεφάλαιο – Επιθέσεις στο Signaling

2.1. Επιθέσεις DoS

Οι επιτιθέμενοι μπορούν να κάνουν κακή χρήση του πρωτοκόλλου σηματοδοσίας για να διεξάγουν denial of service επιθέσεις. Στην πρώτη περίπτωση, οι επιτιθέμενοι μπορούν να δημιουργήσουν ένα μεγάλο αριθμό αιτημάτων εγκατάστασης κλήσης που θα καταναλώνουν τη δύναμη επεξεργασίας του proxy server. Ένα παράδειγμα παρουσιάζεται στο σχήμα 10 (a) όπου ο Tim στέλνει πάρα πολλά «INVITE» αιτήματα στον Bob και ο Bob δεν μπορεί να δεχτεί αίτημα από τη Alice. Αυτός ο τύπος DOS επίθεσης χρειάζεται μόνο μεγάλους όγκους αιτημάτων για να πλημμυριστεί το θύμα.

Στη δεύτερη περίπτωση, οι επιτιθέμενοι χρησιμοποιούν την ακύρωση των εκκρεμών σημάτων εγκατάστασης κλήσης συμπεριλαμβανομένης της αποστολής των CANCEL, GOODBYE ή PORT UNREACHABLE μηνυμάτων. Αυτό προκαλεί στο τηλέφωνο να μην είναι σε θέση να ολοκληρώσει τις κλήσεις ή να κλείσει. Αυτός ο τύπος επίθεσης βοηθιέται από την πολυπλοκότητα των πρωτοκόλλων σηματοδοσίας. Το σχήμα 10 (b) παρουσιάζει ένα παράδειγμα όπου το CANCEL μήνυμα έχει παραπλανηθεί από τον επιτιθέμενο για να αποτρέψει την εγκατάσταση κλήσης.

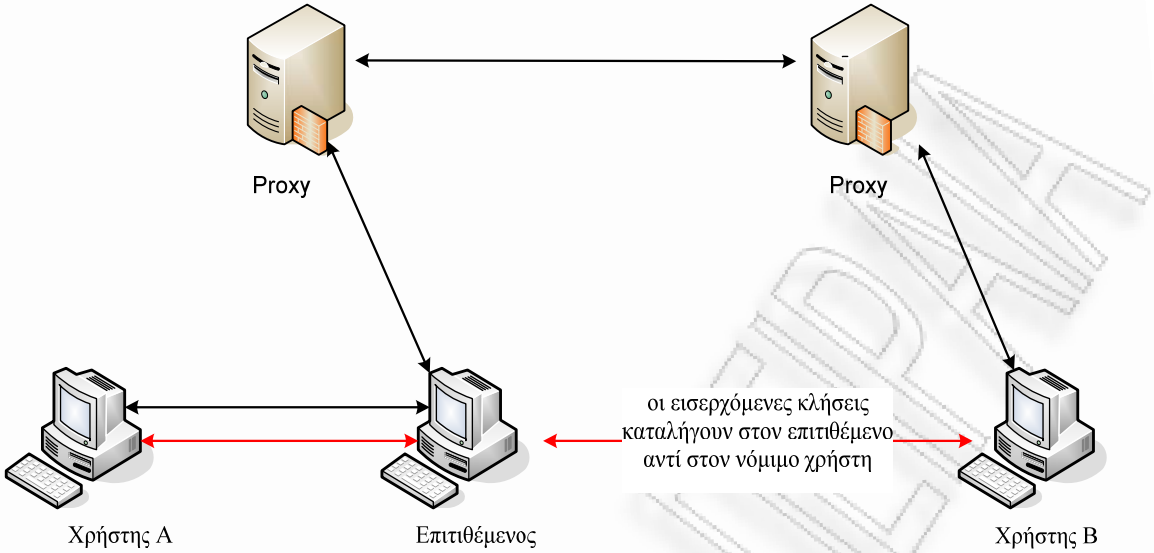
Το σχήμα 10 (c) δίνει ένα παράδειγμα όπου ένα παραπλανητικό GOODBYE μήνυμα καταστρέφει τις εγκατεστημένες συνδέσεις. Ένα σωστά επεξεργασμένο πακέτο μπορεί να καταστρέψει την κλήση. Εντούτοις, αυτή η επίθεση απαιτεί από τον επιτιθέμενο να είναι σε θέση να συμπληρώσει σωστά ορισμένες επιγραφές του μηνύματος. Ο επιτιθέμενος μπορεί να συγκεντρώσει στοιχεία δικτύου για να εξαγάγει αυτές τις πληροφορίες.



Εικόνα 10: Απεικόνιση DOS επιθέσεων

2.2. Registration Hijacking

Με την ανάπτυξη της Voice Over IP (VoIP) τεχνολογίας - και ειδικά του Session Initiation Protocol (SIP) - υπάρχουν διάφορες επιθέσεις που πρέπει να εξεταστούν. Μια τέτοια επίθεση είναι η registration hijacking. Στο πρωτόκολλο SIP (και άλλα πρωτόκολλα VoIP), ένας User Agent(UA) / IP τηλέφωνο πρέπει να εγγραφεί σε ένα SIP proxy/ registrar (ή έναν IP PBX), γεγονός που επιτρέπει στον proxy να κατευθύνει τις εισερχόμενες κλήσεις στον UA. Η Registration hijacking επίθεση συμβαίνει όταν ένας επιτιθέμενος μιμείται έναν έγκυρο UA σε έναν registrar και αντικαθιστά τη νόμιμη εγγραφή με τη δική του διεύθυνση. Αυτή η επίθεση αναγκάζει τις εισερχόμενες κλήσεις προοριζόμενες για τον UA να σταλθούν στον απατεώνα UA. Η παρακάτω εικόνα επεξηγεί την registration hijacking:



Η Registration hijacking επιτρέπει στις εισερχόμενες κλήσεις να υποκλαπούν και να απαντηθούν από έναν επιτιθέμενο, ο οποίος παραδείγματος χάριν, θα μπορούσε να παίξει μια ψεύτικη υπηρεσία υπαγόρευσης προσωπικού τηλεφωνητή. Η Registration hijacking επιτρέπει επίσης σε έναν επιτιθέμενο να "μπει στη μέση" και να καταγράψει τη σηματοδότηση και τον ήχο.

Αιτίες της Registration Hijacking

Με το SIP, η εγγραφή εκτελείται κανονικά χρησιμοποιώντας το Universal Datagram Protocol (UDP), σε αντιδιαστολή με το Transmission Control Protocol (TCP).Το UDP απλοποιεί την παραγωγή των κακόβουλων πακέτων, καθιστώντας τις επιθέσεις όπως την Registration Hijacking ευκολότερες.

Οι SIP registrars δεν χρειάζεται να αυθεντικοποιήσουν τον UA ζητώντας εγγραφή. Επιπλέον, όταν η αυθεντικοποίηση χρησιμοποιείται, δεν είναι ισχυρή, περιλαμβάνοντας μόνο τη χρήση της MD5 digest για το όνομα του χρήστη, τον κωδικό πρόσβασης, και το timestamp-based nonce που στέλνεται στην πρόκληση αυθεντικοποίησης. Οι κωδικοί πρόσβασης είναι συχνά αδύναμοι ή «μηχανικά» παραγμένοι, εννοώντας ότι οι κωδικοί πρόσβασης παράγονται αυτόματα και ακολουθούν ένα προβλέψιμο σχέδιο. Ακόμη και οι ισχυροί κωδικοί πρόσβασης

μπορούν να σπαστούν με τις επιθέσεις λεξικού. Οι επιθέσεις λεξικού είναι εκείνες όπου ένας κατάλογος πιθανών κωδικών πρόσβασης χρησιμοποιείται για «να υποθέσει» έναν κωδικό πρόσβασης που απαιτείται για την εγγραφή. Ένα λεξικό που χτίζεται με τη γνώση μιας οργάνωσης μπορεί να είναι πολύ αποτελεσματικό. Αρκετά συχνά, η γνώση ενός ενιαίου κωδικού πρόσβασης επιτρέπει το σπάσιμο πολλών άλλων κωδικών πρόσβασης.

Το τρέχον SIP RFC 3261 δηλώνει ότι η «βασική» αυθεντικοποίηση που βασίζεται στους κωδικούς πρόσβασης απλών κειμένων, δεν πρέπει να είναι διαθέσιμη. Αυτή η μορφή πολύ αδύναμης αυθεντικοποίησης επιτράπηκε από το προηγούμενο SIP RFC 2543. Το τρέχον SIP RFC συστήνει τη χρήση του Transport Layer Security (TLS), το οποίο ακόμα ευρέως δεν εφαρμόζεται.

Ένας εξωτερικός επιτιθέμενος μπορεί να χτίσει έναν κατάλογο με την ανίχνευση των διαθέσιμων προς εγγραφή διευθύνσεων του UA. Ο ανιχνευτής μπορεί να στείλει διάφορα αιτήματα στον SIP proxy/registrar, και να καθορίσει από τις απαντήσεις, ποιες διευθύνσεις είναι έγκυρες και διαθέσιμες προς εγγραφή. Οι εξωτερικές προσπάθειες εγγραφής στο δίκτυο πρέπει σπάνια να επιτρέπονται, αλλά αυτή η αρχή δεν επιβάλλεται. Τα όρια της Max-Forwards επιγραφής (και άλλες τεχνικές) μπορούν να χρησιμοποιηθούν για να ανιχνεύσουν αυτό το είδος της επίθεσης, αλλά αυτά τα όρια δεν επιβάλλονται συνήθως.

Οι περισσότεροι registrars/proxy servers δεν θα ανιχνεύσουν την επίθεση λεξικού ή τις προσπάθειες της registration hijacking. Επιπλέον, τα προϊόντα ασφάλειας όπως τα τυποποιημένα firewalls αποτυγχάνουν να ανιχνεύσουν αυτούς τους τύπους επιθέσεων.

Αποτελέσματα της Registration Hijacking

Η Registration hijacking μπορεί να οδηγήσει στην απώλεια κλήσεων σε έναν στοχευόμενο UA. Αυτός μπορεί να είναι ένας μεμονωμένος χρήστης, μία ομάδα χρηστών, ή ένας πόρος υψηλής-κυκλοφορίας, όπως media gateway, Automated Attendant (AA), Interactive Voice Response (IVR), ή ένα σύστημα υπηρεσίας

προσωπικού τηλεφωνητή. Με την πειρατεία των κλήσεων σε μια media gateway, όλες οι εξερχόμενες κλήσεις μπορούν να εμποδιστούν ή ειδάλλως να παραποιηθούν.

Αντιθέτως, ένας απατεώνας UA που ενεργεί στη μέση μπορεί να εκτρέψει τις κλήσεις σε μια media gateway για να πραγματοποιήσει μια toll fraud επίθεση. Ένας απατεώνας UA που ενεργεί στη μέση μπορεί επίσης να καταγράψει ήχο, σηματοδότηση, και τους DTMF(Dual-tone multi-frequency) κώδικες (για τις οικονομικές συναλλαγές).

Οι μηχανισμοί της Registration Hijacking

Το πρώτο βήμα στην *Registration Hijacking* είναι να βρεθούν οι διαθέσιμες προς εγγραφή διευθύνσεις. Αυτό είναι ασήμαντο για έναν εσωτερικό επιτιθέμενο που ξέρει τη δομή των διευθύνσεων ή/και έχει έναν κατάλογο. Ένας εξωτερικός επιτιθέμενος, πρέπει να ανιχνεύσει τις διαθέσιμες προς εγγραφή διευθύνσεις. Για το σκοπό αυτό μπορεί να χρησιμοποιηθεί ένας «ανιχνευτής». Ο ανιχνευτής μπορεί να παραγάγει διαφορετικούς τύπους αιτημάτων για να ψάξει τις διευθύνσεις, όπως SIP INVITES ή SIP OPTIONS, κάθε ένα από τα οποία επιστρέφει μια απάντηση που μπορεί να χρησιμοποιηθεί για να καθορίσει εάν μια διεύθυνση ισχύει. Κάθε προσέγγιση έχει οφέλη. Η χρησιμοποίηση του INVITE αιτήματος είναι λιγότερο κρυφή, επειδή θα αναγκάσει τον UA να ηχήσει, αλλά έχει το όφελος της μη απαίτησης αυθεντικοποίησης - δεν είναι εφικτό να απαιτηθεί η αυθεντικοποίηση από κάθε εξωτερικό επισκέπτη. Το OPTIONS αίτημα είναι πιο κρυφό, δεν αναγκάζει έναν UA να ηχήσει, και συγκεντρώνει περισσότερες πληροφορίες για τον UA, αλλά είναι πιθανότερο να απαιτηθεί αυθεντικοποίηση. Ένας ανιχνευτής μπορεί να παράγει ένα μόνο αίτημα, ή να παράγει μια τυχαία ακολουθία αιτημάτων, και να περιμένει έπειτα τις απαντήσεις.

Η αυθεντικοποίηση μπορεί να απαιτηθεί και κατά τη διάρκεια της ανίχνευσης και της registration hijacking διαδικασίας. Όταν η αυθεντικοποίηση χρησιμοποιείται, ο proxy ή registrar στέλνει μια απάντηση πρόκλησης αυθεντικοποίησης. Αυτό απαιτεί ένα έγκυρο όνομα χρήστη/κωδικό πρόσβασης προκειμένου να πραγματοποιηθεί η ανίχνευση. Ένα όνομα χρήστη/κωδικός πρόσβασης μπορεί να ληφθεί μέσω social

engineering, γνώση των επιχειρήσεων, ή να εικαστεί μέσω μιας λεξικού επίθεσης. Μόλις ένας κωδικός πρόσβασης γίνει γνωστός, μπορεί να χρησιμοποιηθεί για να ανιχνεύσει τις διευθύνσεις σε όλο τον οργανισμό.

Μόλις προσδιοριστεί μια στοχευόμενη διεύθυνση (ή διευθύνσεις), η εγγραφή του στόχου μπορεί να πειρατευθεί. Η διαδικασία πειρατείας περιγράφεται παρακάτω:

- Η πειρατεία αρχίζει με τον επιτιθέμενο να στέλνει ένα ειδικά επεξεργασμένο REGISTER αίτημα στον στοχευόμενο registrar, για να αποδεσμεύσει όλες τις υπάρχουσες εγγραφές. Η γραμμή της CONTACT επιγραφής περιέχει την παράμετρο μπαλαντέρ (*) σε συνδυασμό με τη γραμμή της EXPIRES επιγραφής με την αξία 0 (μηδέν). Μαζί, αυτές οι γραμμές ζητούν από τον Registrar να αφαιρέσει όλες τις συνδέσεις για τη διεύθυνση του στοχευόμενου χρήστη που καθορίζονται στη γραμμή της TO επιγραφής.

- Είναι επίσης δυνατό να σταλεί ένα REGISTER αίτημα χωρίς τις γραμμές της CONTACT επιγραφής. Αυτό ειδοποιεί τον Registrar να αποκριθεί με έναν κατάλογο όλων των υπαρχουσών επαφών. Αυτός ο κατάλογος επαφών μπορεί έπειτα να χρησιμοποιηθεί και να σταλούν χωριστά REGISTER αιτήματα ώστε να αφαιρεθεί κάθε επαφή χωριστά.

Καθεμία από αυτές τις προσεγγίσεις δουλεύει. Το πλεονέκτημα της δεύτερης προσέγγισης είναι ότι μπορεί να επαναληφθεί περιοδικά, να εξακριβώσει εάν ο UA έχει επανεγγραφτεί. Οι UAs περιοδικά επανεγγράφονται, έτσι για να συνεχίσει να λειτουργεί η registration hijack, αυτές οι περιοδικές επανεγγραφές πρέπει να αφαιρεθούν.

- Εάν ο registrar απαιτεί την αυθεντικοποίηση, απαντά στα REGISTER αιτήματα με μια πρόκληση. Για την αυθεντικοποίηση του ονόματος χρήστη/κωδικού πρόσβασης, ο registrar περιλαμβάνει μία nonce στην απάντηση, την οποία ο επιτιθέμενος χρησιμοποιεί για να υπολογίσει μια MD5 digest του ονόματος χρήστη/κωδικού πρόσβασης.

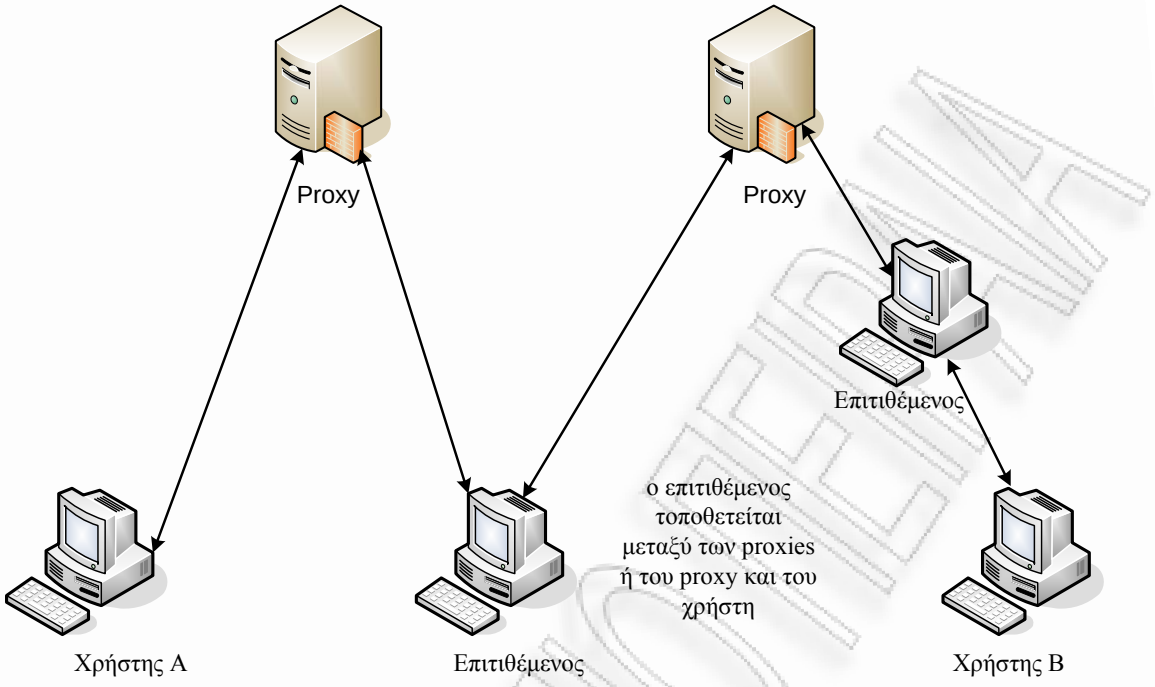
- Μόλις διαγραφούν όλες οι νόμιμες επαφές, ο επιτιθέμενος στέλνει ένα δεύτερο REGISTER αίτημα που περιέχει μια νέα γραμμή της CONTACT επιγραφής με τη διεύθυνση του επιτιθέμενου. Ένα αυθαίρετο EXPIRES διάστημα ζητείται στη γραμμή της EXPIRES επιγραφής του δεύτερου REGISTER αιτήματος (παραδείγματος χάριν, 1 ημέρα).

- Εάν η αυθεντικοποίηση απαιτείται, ο επιτιθέμενος αποκρίνεται μόνο όπως περιγράφεται ανωτέρω.

Η Registration hijacking μπορεί επίσης να εκτελεσθεί με την υποκλοπή και την επεξεργασία των REGISTER αιτημάτων που στέλνονται μεταξύ ενός έγκυρου UA και ενός registrar.

2.3. Proxy Impersonation

Η Proxy impersonation επίθεση εμφανίζεται όταν ένας επιτιθέμενος εξαπατά έναν από τους SIP UAs ή τους proxies ώστε να επικοινωνήσουν με ένα proxy απατεώνων. Εάν ένας επιτιθέμενος επιτυχώς μιμηθεί έναν proxy, έχει πρόσβαση σε όλα τα SIP μηνύματα και έχει τον ολοκληρωτικό έλεγχο της κλήσης. Η ακόλουθη εικόνα εξηγεί την Proxy impersonation:



Οι UAs και οι proxies κανονικά επικοινωνούν χρησιμοποιώντας το UDP και δεν απαιτούν ισχυρή αυθεντικοποίηση για να επικοινωνήσουν με ένα άλλο proxy. Ένας proxy απατεώνων μπορεί επομένως να παρεμβληθεί στο ρεύμα σηματοδοσίας μέσω διάφορων τρόπων, συμπεριλαμβανομένης της Domain Name Service (DNS) spoofing, της Address Resolution Protocol (ARP) cache spoofing, ή αλλάζοντας απλά την διεύθυνση του proxy για ένα SIP τηλέφωνο. Ο proxy απατεώνων έχει τον ολικό έλεγχο πάνω στις κλήσεις και μπορεί να εκτελέσει τους ίδιους τύπους επιθέσεων που περιγράφηκαν στην registration hijacking.

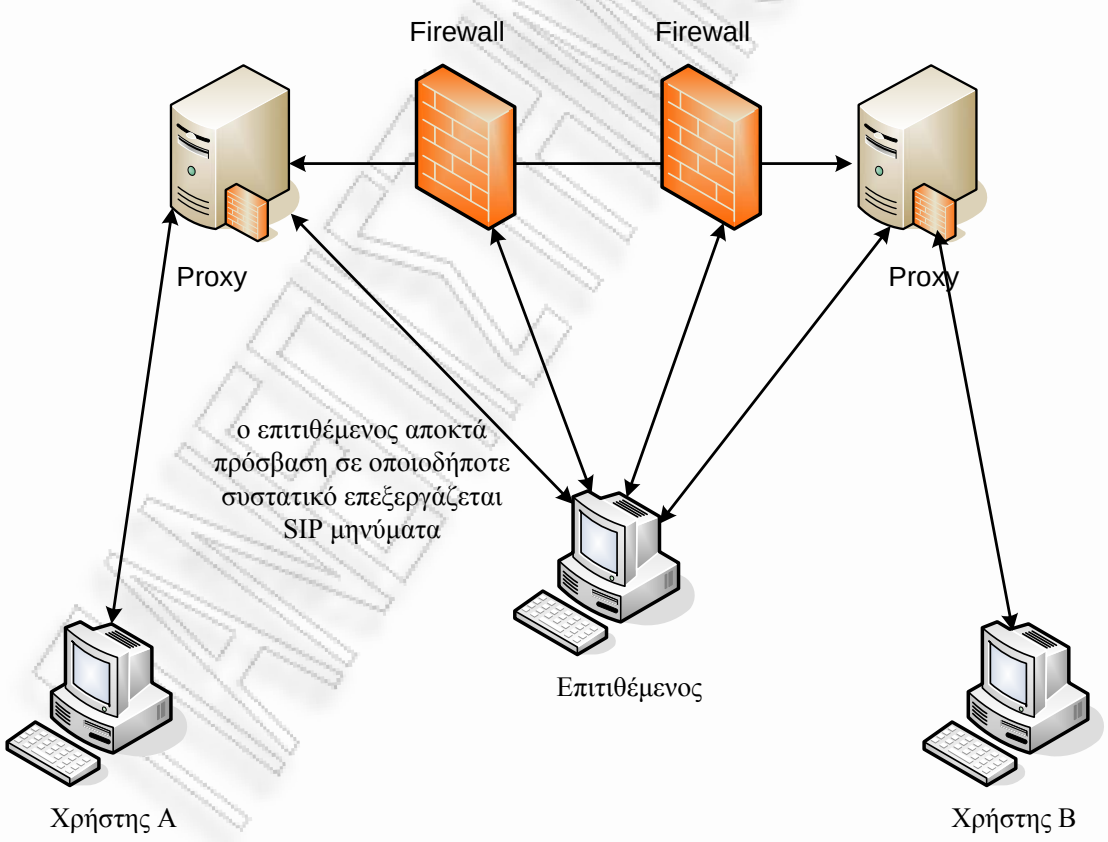
Εάν η DNS spoofing χρησιμοποιείται για να επαναπροσανατολίσει τις εξερχόμενες κλήσεις σε μια συγκεκριμένη περιοχή (π.χ., «company.com»), όλες οι εξερχόμενες κλήσεις σε εκείνη την περιοχή μπορούν να παρεμποδιστούν, παραποιηθούν, εμποδιστούν, ή να καταγραφούν.

Η ARP cache spoofing είναι μια επίθεση ενάντια σε έναν διακόπτη δικτύου που μπορεί να εξαπατήσει ένα UA στο να επικοινωνήσει με ένα proxy απατεώνων στο

εσωτερικό δίκτυο. Εάν είναι επιτυχής, οι κλήσεις που προέρχονται από το UA μπορούν να παρεμποδιστούν, παραποιηθούν, εμποδιστούν, ή να καταγραφούν.

2.4. Message Tampering

Η Message tampering επίθεση πραγματοποιείται όταν ένας επιτιθέμενος παρεμποδίζει και τροποποιεί τα πακέτα που ανταλλάσσονται μεταξύ των SIP τμημάτων. Η Message tampering μπορεί να πραγματοποιηθεί μέσω της registration hijacking, της proxy impersonation, ή μιας επίθεσης σε οποιοδήποτε έμπιστο συστατικό που επεξεργάζεται τα SIP μηνύματα, όπως ο proxy, η media πύλη, ή το firewall. Η ακόλουθη εικόνα εξηγεί την message tampering:

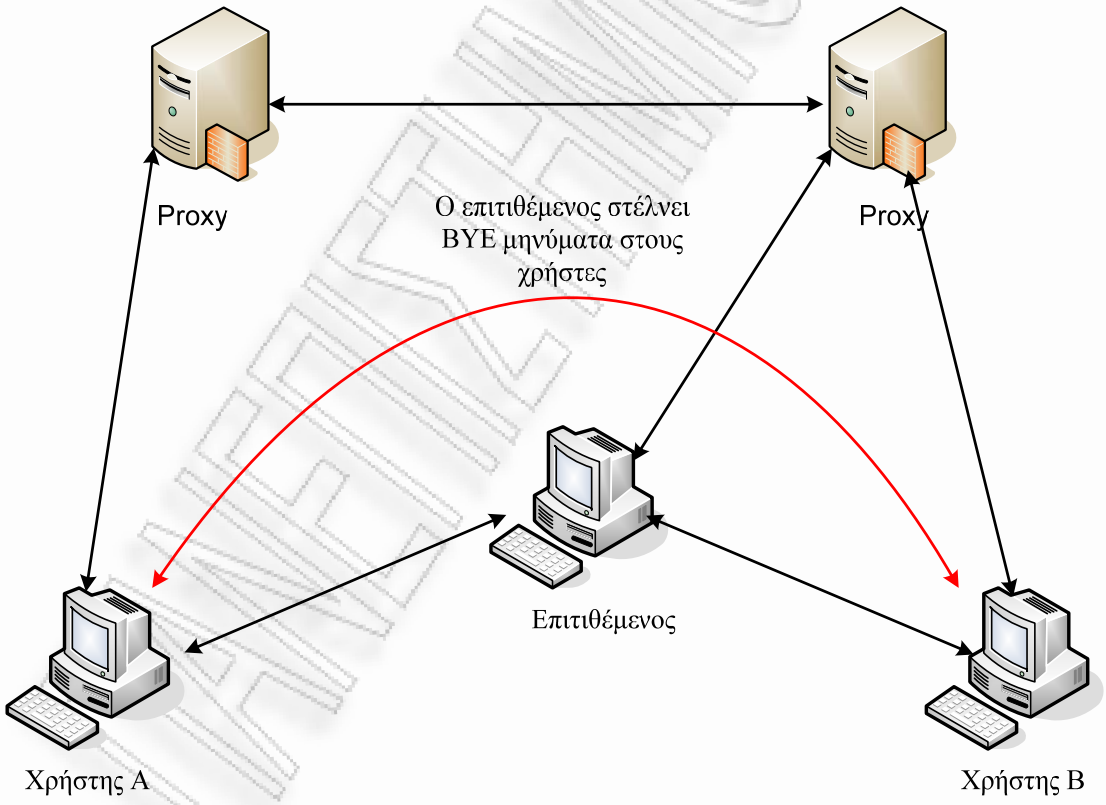


Τα SIP μηνύματα δεν έχουν κανένα ενσωματωμένο τρόπο για να ασφαλίσουν την ακεραιότητα. Με την παραποίηση των SIP μηνυμάτων, ένας επιτιθέμενος μπορεί να

εκτελέσει τους ίδιους τύπους επιθέσεων που περιγράφονται για την registration hijacking και την proxy impersonation.

2.5. Session Tear Down

Η Session tear down επίθεση πραγματοποιείται όταν ένας επιτιθέμενος παρατηρεί τη σηματοδοσία για μια κλήση, και έπειτα στέλνει παραποιημένα SIP BYE αιτήματα στους συμμετέχοντες UAs. Οι περισσότεροι SIP UAs δεν απαιτούν ισχυρή αυθεντικοποίηση, γεγονός που επιτρέπει σε έναν επιτιθέμενο να στείλει κατάλληλα επεξεργασμένα BYE αιτήματα στους δύο UAs, τερματίζοντας βιαίως την κλήση. Η ακόλουθη εικόνα απεικονίζει την Session tear down επίθεση:



Εάν ένας UA δεν ελέγχει τις διαθέσιμες τιμές πακέτων, ο επιτιθέμενος μπορεί μην χρειαστεί ακόμη και να παρατηρήσει τη σηματοδότηση κλήσης. Εάν ο επιτιθέμενος ξέρει τη διεύθυνση ενός συνεχώς ενεργού UA (όπως η media πύλη, το AA, το IVR,

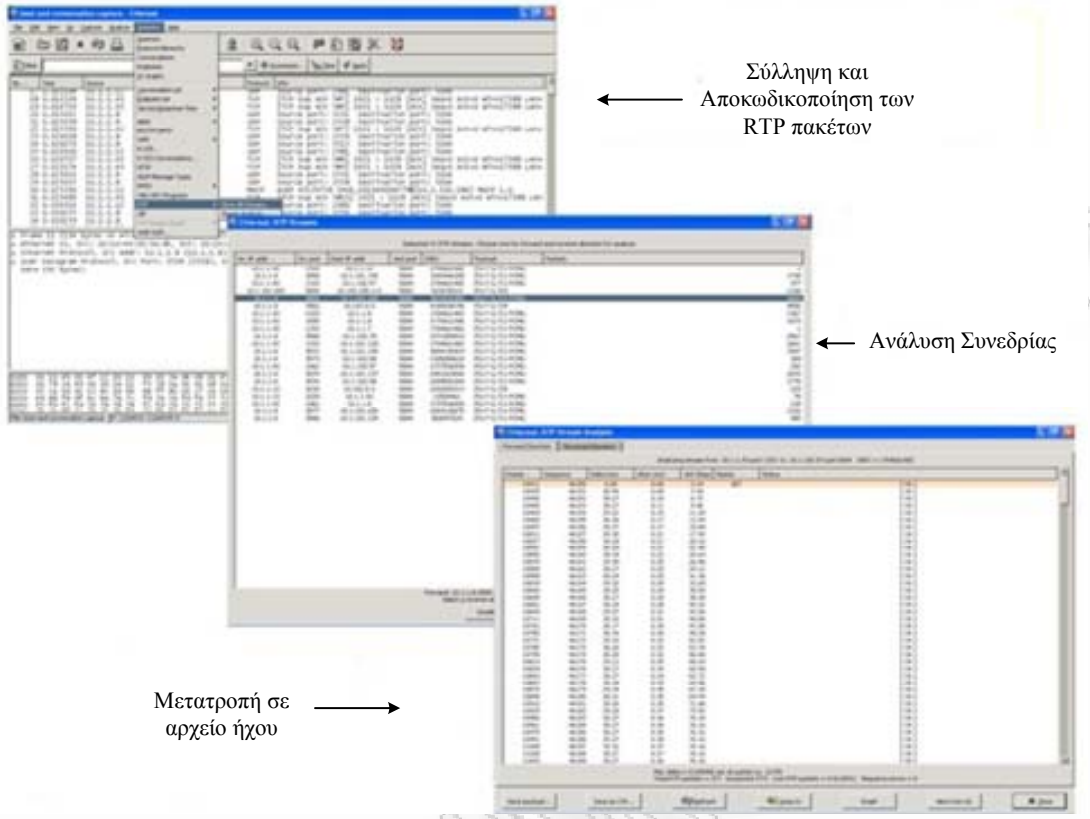
το trading floor phone, κ.λπ.), μπορεί να στείλει BYE αιτήματα, αναγκάζοντας την κλήση να τερματίσει βίαια.

2.6. Eavesdropping

Αυτή η επίθεση χρησιμοποιεί τα εργαλεία σύλληψης και ανάλυσης της κίνησης του δικτύου, όπως το Ethereal, για να κάνει sniffing στα μηνύματα σηματοδοσίας και τα media streams σε μια συνομιλία. Τα συλληφθέντα RTP πακέτα που ανταλλάσσονται από τα UDP ή TCP πρωτόκολλα αποκωδικοποιούνται και μετατρέπονται σε αρχεία ήχου. Τα βήματα που λαμβάνονται για την σύλληψη και την αποκωδικοποίηση των πακέτων φωνής περιλαμβάνουν:

- Πρώτα συλλαμβάνονται και αποκωδικοποιούνται τα RTP πακέτα με την επιλογή **Analyze -> RTP-> Show all streams** στην ethereal διεπαφή.
- Έπειτα, η συνεδρία αναλύεται με την επιλογή ενός ρεύματος προς ανάλυση και επανασυναρμολόγηση.
- Το ρεύμα μπορεί τώρα να μετατραπεί σε αρχείο ήχου μέσω της επιλογής **Publish**.

Η παρακάτω εικόνα απεικονίζει τα βήματα που απαιτούνται για την σύλληψη χρησιμοποιώντας το Ethereal.

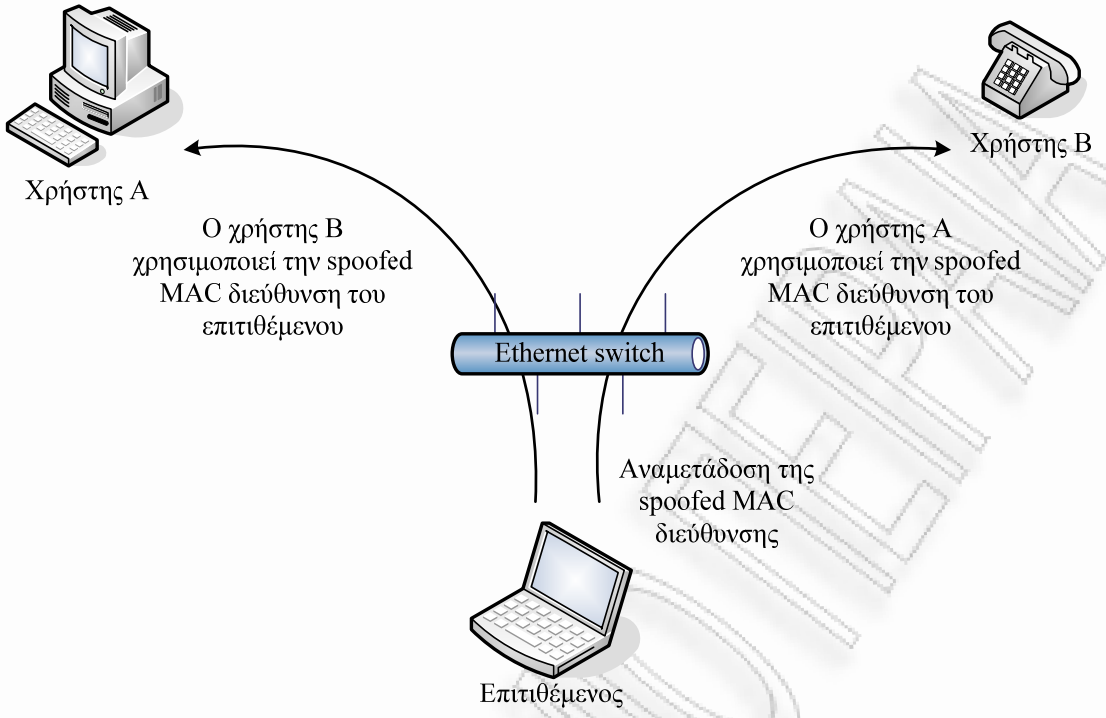


2.7. Man-In-The-middle επίθεση

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

Σε ένα VoIP περιβάλλον, αυτή η επίθεση χρησιμοποιεί έναν μηχανισμό που αποκαλείται ARP spoofing ώστε να κρυφακούσει την επικοινωνία σε ένα δίκτυο μεταγωγής που βασίζεται στην IP. Δεδομένου ότι οι Ethernet διακόπτες περιορίζουν την μετάδοση κυκλοφορίας σε ένα δίκτυο, οι περισσότεροι σχεδιαστές δικτύων τους χρησιμοποιούν για να ενισχύσουν την ασφάλεια μέσω του περιορισμού της πρόσβασης στην κυκλοφορία. Παρόλα αυτά με τη βοήθεια ενός ειδικού ARP spoofing εργαλείου όπως το Cain, μια man-in-the-middle επίθεση μπορεί να είναι επιτυχής στα LANs μεταγωγής. Στην ARP spoofing που απεικονίζεται στη εικόνα 11, η μετάδοση των παραποιημένων ARP μηνυμάτων που περιέχουν πλαστές MAC διευθύνσεις στο Ethernet LAN καθιστούν πιθανή την λήψη πλαισίων ενός άλλου σταθμού από τον επιτιθέμενο.

Στην εικόνα 11 τα πλαίσια που στέλνονται μεταξύ του χρήστη A και B στέλνονται εσφαλμένα στον επιτιθέμενο καθιστώντας πιθανή την σύλληψη τους. Αυτό είναι δυνατό επειδή, όταν θέλει ο χρήστης A να στείλει πλαίσια στη IP διεύθυνση του B, ένας κρυφός πίνακας που περιέχει μια χαρτογράφηση των IP διευθύνσεων στις αντίστοιχες MAC επιδεικνύει ότι, η MAC διεύθυνση του B είναι στην πραγματικότητα η MAC διεύθυνση του επιτιθεμένου – με αποτέλεσμα το πακέτο να στέλνεται στον επιτιθέμενο. Η αντίθετη πορεία είναι επίσης δυνατή όταν στέλνει ο B πλαίσια στον A.



Εικόνα 11: Man-in-the-Middle επίθεση χρησιμοποιώντας το ARP Spoofing

2.8. Replay Attack

Μια επίθεση με τη βοήθεια των sniffing εργαλείων πάνω στα πακέτα ενός δικτύου μπορεί να πραγματοποιήσει replay επιθέσεις με τη σύλληψη πληροφοριών σε μια συνεδρία επικοινωνίας. Οι πληροφορίες που συλλαμβάνονται μπορούν να αναμεταδοθούν άθικτες ή τροποποιημένες για να επιτύχουν έναν σκοπό. Οι οικονομικοί οργανισμοί, όπως οι τράπεζες, που αναπτύσσουν την VoIP εφαρμογή μπορεί να βιώσουν μια κατάσταση όπου ευαίσθητα δεδομένα, όπως αριθμοί λογαριασμών, πληροφορίες πιστωτικών καρτών μπορούν να συλληφθούν από τους απατεώνες Διαδικτύου. Από την άποψη της διοίκησης συστημάτων, η σύνδεση των χρηστών σε αυτό προσφέρει ένα τέλειο περιβάλλον για τις replay επιθέσεις. Σε αυτήν την περίπτωση, ο επιτιθέμενος συλλαμβάνει το όνομα και τον κωδικό πρόσβασης του χρήστη και τα χρησιμοποιεί για να συνδεθεί ως νόμιμος χρήστης αργότερα. Η ακεραιότητα των πακέτων βοηθάει στην εξάλειψη της επίθεσης αυτής . Το Timestamping, ένα χαρακτηριστικό που υποστηρίζεται από το RTP σε ένα

συγχρονισμένο περιβάλλον μετριάζει τις replay επιθέσεις με τη βοήθεια του μηχανισμού προστασίας ακεραιότητας όπως οι hash MD5 συναρτήσεις και SHA -1.

Η Replay επίθεση σε ένα VoIP περιβάλλον είναι δυνατή όταν ένας επιτιθέμενος συνδυάζει τις eavesdropping και man-in-the-middle επιθέσεις για την σύλληψη και την αποστολή εκ νέου ζωτικής σημασίας πληροφορίες όπως πιστοποιητικά σύνδεσης δικτύου, πχ τους κωδικούς πρόσβασης και τα ονόματα χρήστη.

2.9. Επιθέσεις βασισμένες στο SIP Signaling

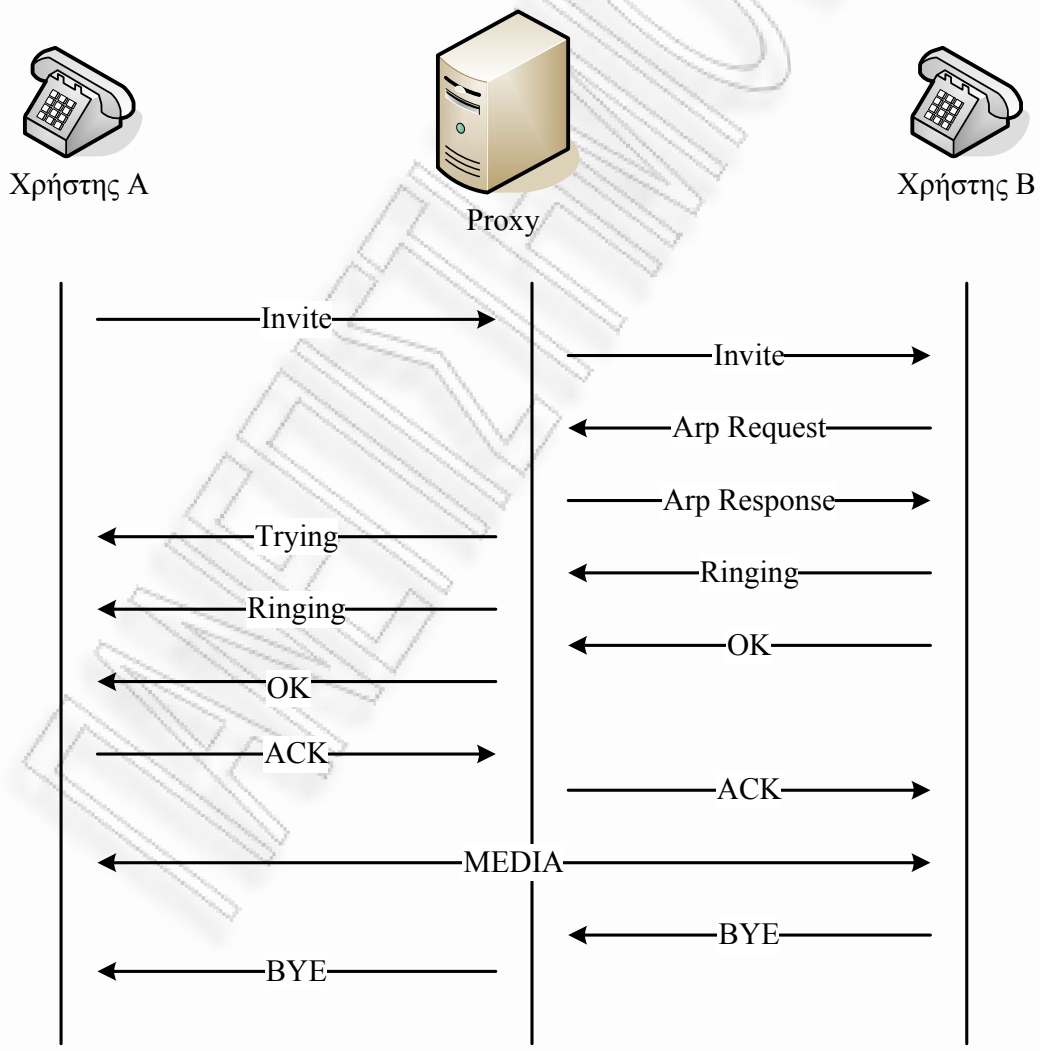
Η προδιαγραφή του SIP πρωτοκόλλου περιγράφει τις μεθόδους για τον τερματισμό/ολοκλήρωση μίας συνεδρίας, την ακύρωση μίας πρόσκλησης, τον επαναπροσανατολισμό μίας κλήσης, και την ενημέρωση των παραμέτρων μίας συνεδρίας. Είναι πολύ πιθανό ότι ο επιτιθέμενος θα προσπαθήσει να εκμεταλλευτεί οποιαδήποτε αδυναμία της ασφάλειας στις προαναφερθείσες μεθόδους και να προκαλέσει την DOS επίθεση στην παρεχόμενη υπηρεσία. Ο κύριος λόγος που ένας επιτιθέμενος μπορεί να πραγματοποιήσει επιθέσεις με τη χρησιμοποίηση αυτών των αιτημάτων είναι η χρησιμοποίηση ενός ακατάλληλου μηχανισμού αυθεντικοποίησης. Στους κινδύνους, οι τρέχουσες SIP προδιαγραφές δεν εξουσιοδοτούν την αυθεντικοποίηση για όλες τις προαναφερθείσες μεθόδους. Πιο συγκεκριμένα, για κάθε μια από τις προηγούμενες διαδικασίες οι ακόλουθες SIP επιθέσεις θα μπορούσαν να πραγματοποιηθούν:

2.9.1. Η "BYE" επίθεση

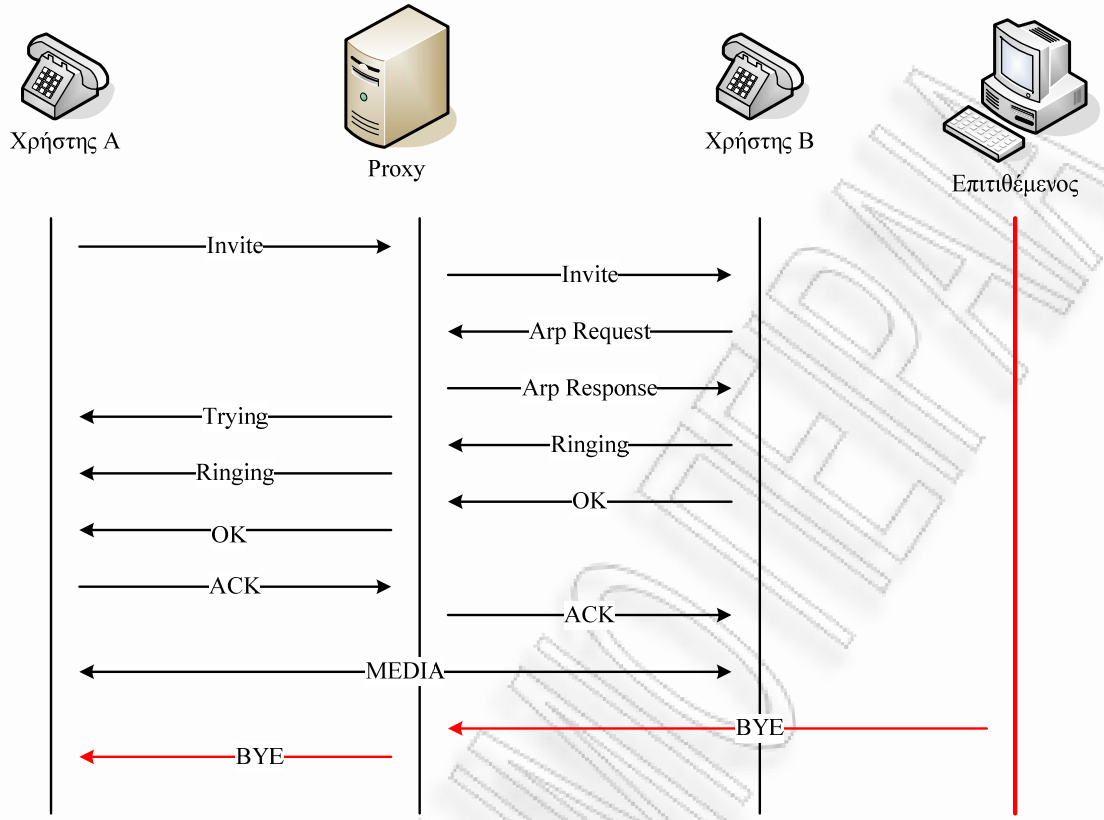
Το BYE αίτημα χρησιμοποιείται για να ολοκληρώσει μια εγκατεστημένη συνεδρία, όπως φαίνεται στην εικόνα 12. Ένας επιτιθέμενος μπορεί ενδεχομένως να χρησιμοποιήσει το BYE αίτημα για να διακόψει μια συνεδρία, όπως απεικονίζεται στην εικόνα 13. Για να πραγματοποιήσει αυτήν την επίθεση, ο επιτιθέμενος πρέπει να μάθει όλες τις απαραίτητες παραμέτρους μιας συνεδρίας (π.χ., το ID της συνεδρίας, την πόρτα του RTP, κ.λπ.). Αυτό μπορεί να επιτευχθεί είτε με sniffing της κυκλοφορίας του δικτύου είτε με την εκτέλεση μιας επίθεσης Man-In-The-Middle για

την παρεμβολή ενός BYE αιτήματος στη συνεδρία. Η BYE μέθοδος όπως αναφέρεται ανωτέρω χρησιμοποιείται για τον τερματισμό μίας εγκατεστημένης συνεδρίας. Εντούτοις, αυτή η επίθεση μπορεί να πραγματοποιηθεί επιτυχώς μόνο στην περίπτωση που κανένας μηχανισμός αυθεντικοποίησης δεν χρησιμοποιείται, λαμβάνοντας υπόψη φυσικά τη δυνατότητα του επιτιθεμένου να ανακαλύψει τις τρέχουσες παραμέτρους συνεδρίας.

Κατά συνέπεια, η προστασία των κρίσιμων παραμέτρων της συνεδρίας σχετικά με την εμπιστευτικότητα πρέπει να θεωρηθεί υποχρεωτική. Όπως θα δούμε στο κεφάλαιο 3, είτε το TLS είτε το IPSec μπορεί να υιοθετηθεί για την παροχή τέτοιου είδους υπηρεσιών ασφάλειας. Επιπλέον, η αυθεντικότητα ενός BYE αιτήματος πρέπει να εξασφαλιστεί με τη χρησιμοποίηση είτε της HTTP Digest είτε του TLS.



Εικόνα 12: κανονικός τερματισμός συνεδρίας



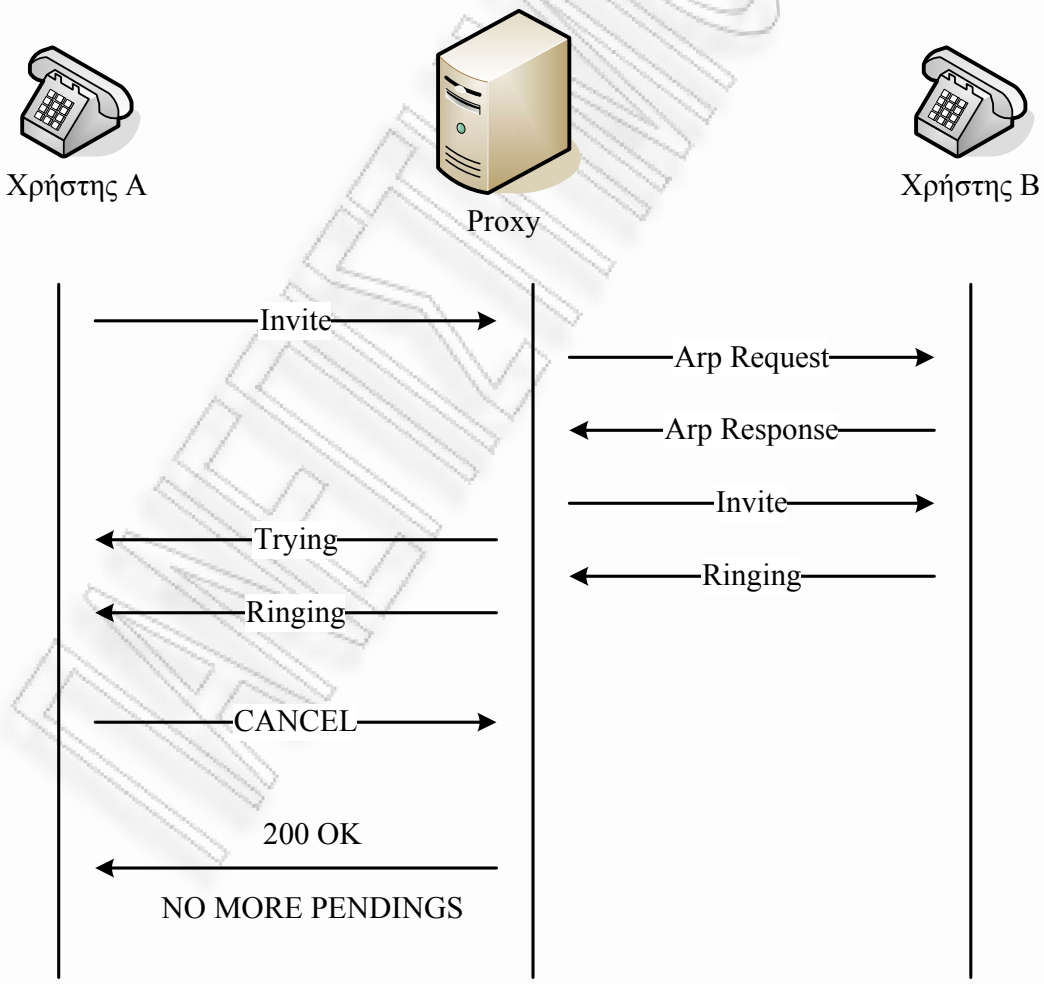
Εικόνα 13: BYE Επίθεση

2.9.2. Η "CANCEL" επίθεση

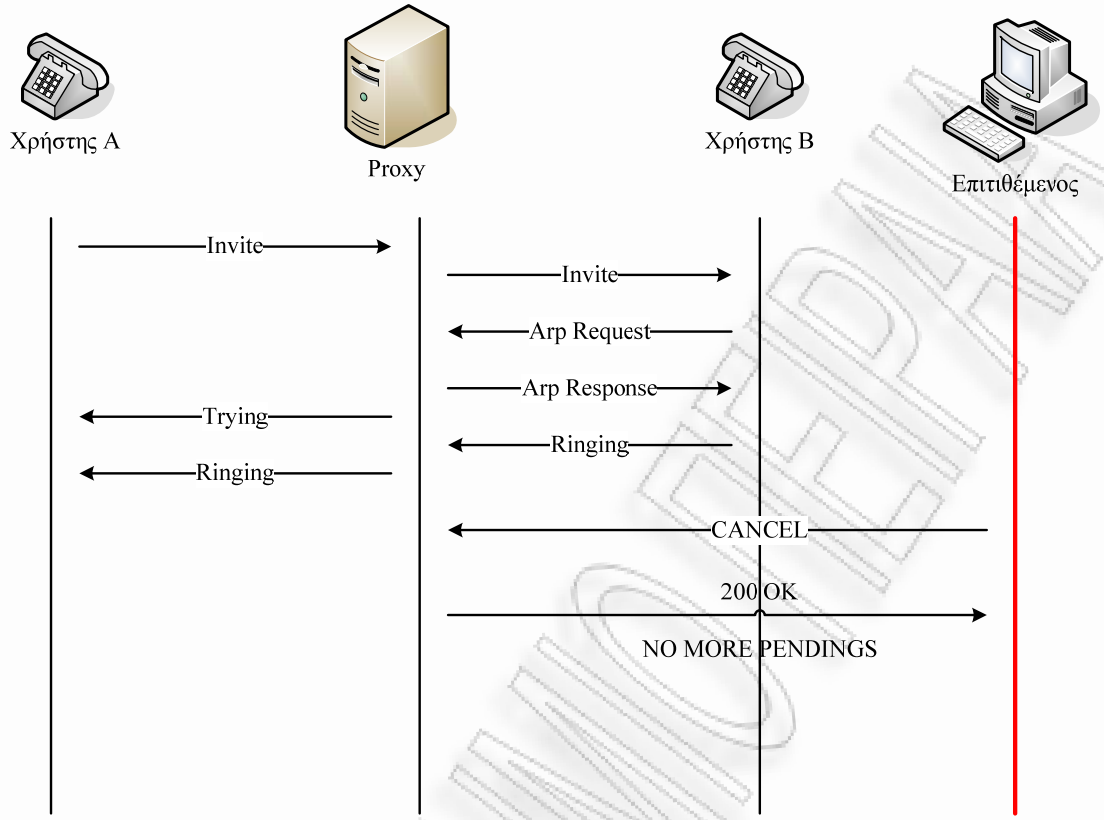
Το CANCEL αίτημα, όπως υπονοεί το όνομα του, χρησιμοποιείται για να ακυρώσει ένα προηγούμενο αίτημα που στέλνεται από έναν πελάτη. Πιο συγκεκριμένα, ζητά από τον αντίστοιχο server να διακόψει την επεξεργασία του αιτήματος και να παράγει μια απάντηση λάθους υποδεικνύοντας το αίτημα αυτό. Αυτή η διαδικασία παρουσιάζεται στην εικόνα 14. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει τη CANCEL μέθοδο για να ακυρώσει ένα INVITE αίτημα που παράγεται από έναν νόμιμο χρήστη, όπως απεικονίζεται στην εικόνα 15. Ένα CANCEL αίτημα πρέπει να σταλθεί μόνο για να ακυρώσει ένα INVITE αίτημα. Κατά συνέπεια, όταν ο SIP-proxy λαμβάνει ένα CANCEL αίτημα για οποιοδήποτε άλλο τύπο μηνυμάτων (από INVITE), δεν πρέπει να επεξεργαστεί αυτό το μήνυμα, αλλά πιθανόν να παράγει μια κατάλληλη απάντηση λάθους. Επιπλέον, εισερχόμενα CANCEL αιτήματα δεν πρέπει να υποβάλλονται σε επεξεργασία εάν για το αρχικό αίτημα έχει ήδη παραχθεί μια

τελική απάντηση. Αυτό είναι επειδή η CANCEL δεν έχει καμία επίδραση στα αιτήματα που έχουν παράγει ήδη μια τελική απάντηση.

Πρέπει να αναφερθεί ότι τα CANCEL αιτήματα παράγονται σε μια hop-by-hop μέθοδο και δεν μπορούν να υποβληθούν εκ νέου. Κατά συνέπεια, δεν μπορούν να προκληθούν από τον server προκειμένου να αποκτήσουν τα κατάλληλα πιστοποιητικά σε ένα Authorization πεδίο επιγραφής. Συνεπώς, η χρησιμοποίηση οποιουδήποτε εφαρμόσιμου, μηχανισμού ασφάλειας υποστρώματος, όπως IPSec ή TLS, θεωρείται υποχρεωτική. Εντούτοις, η επεξεργασία ενός εισερχόμενου CANCEL αιτήματος από μια διαφορετική διοικητική SIP περιοχή είναι ακόμα ένα ανοικτό και εκκρεμές ζήτημα. Επιπλέον, ο έλεγχος των INVITE αιτημάτων που δεν έχουν ήδη παράγει μια τελική απάντηση θα μπορούσε ενδεχομένως να βοηθήσει στον προσδιορισμό οποιουδήποτε παράνομου CANCEL αιτήματος.



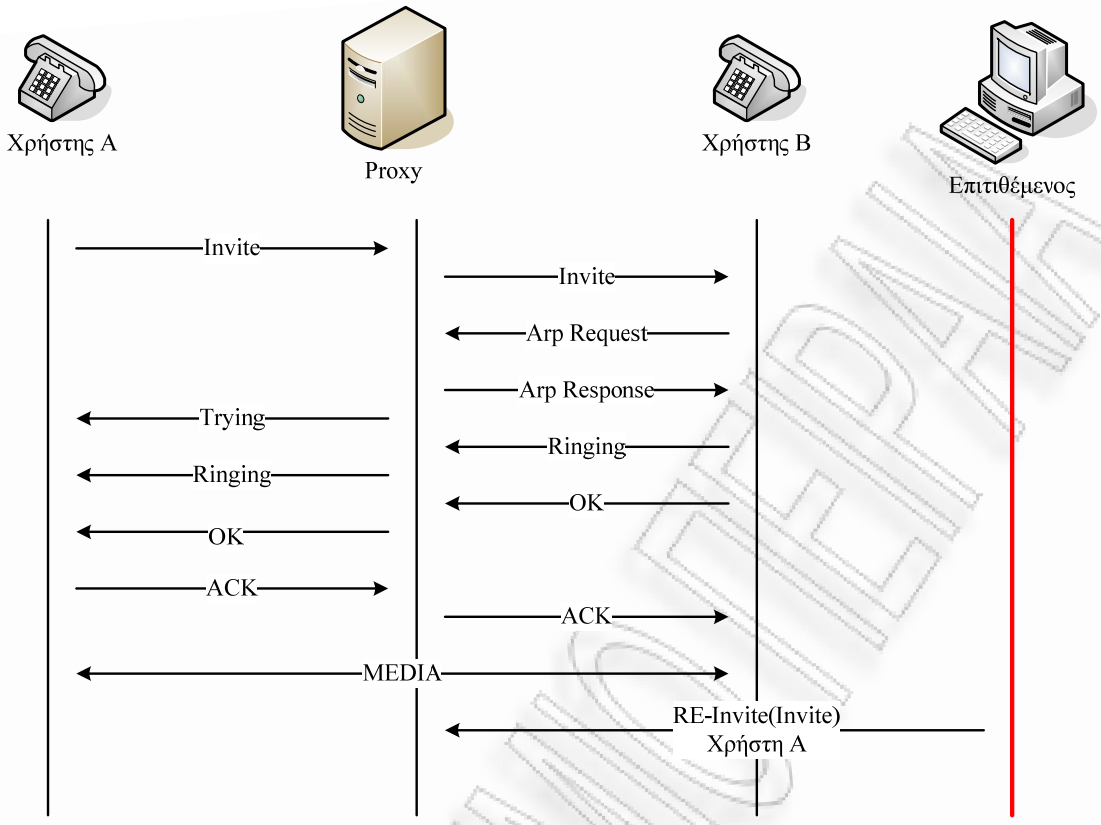
Εικόνα 14: CANCEL αίτημα



Εικόνα 15: CANCEL επίθεση

2.9.3. Η "RE-INVITE" επίθεση

Μόλις εγκατασταθεί μια συνεδρία διαλόγου από το αρχικό μήνυμα, τα επόμενα αιτήματα μπορούν να σταλθούν για να προσπαθήσουν να τροποποιήσουν τις παραμέτρους της συνεδρίας διαλόγου (π.χ., διεύθυνση ή τροποποίηση πορτών). Κατά συνέπεια, οποιαδήποτε μη εξουσιοδοτημένη τροποποίηση της RE-INVITE μεθόδου (εικόνα 16) μιας συνεδρίας διαλόγου από έναν πιθανό επιτιθέμενο μπορεί να προκαλέσει Denial Of Servises .

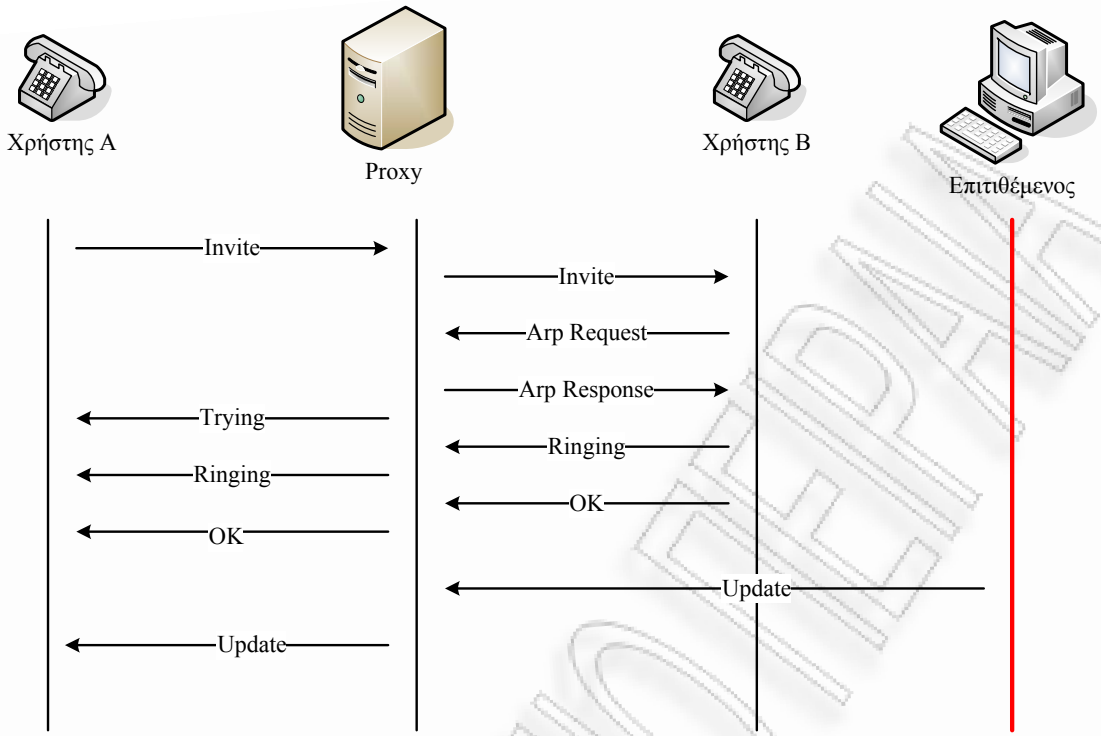


Εικόνα 16: Re-INVITE επίθεση

2.9.4. Η "UPDATE" επίθεση

Η SIP UPDATE μέθοδος δίνει στους τελικούς χρήστες διάφορες δυνατότητες, όπως να χαμηλώσουν ή να βάλουν σε αναμονή τις εισερχόμενες κλήσεις, να προσδιορίσουν την υπηρεσία QoS και να διαπραγματευτούν για άλλες ιδιότητες συνεδριών όπως κάνει και η RE-INVITE. Η μόνη διαφορά είναι ότι η RE-INVITE μπορεί να χρησιμοποιηθεί μόνο αφότου έχει καθιερωθεί μια συνεδρία, ενώ η UPDATE χρησιμοποιείται για να τροποποιήσει τις παραμέτρους της συνεδρίας πριν από την τελική απάντηση στην αρχική πρόσκληση.

Έτσι, παρόμοια με την RE-INVITE επίθεση, ένας επιτιθέμενος μπορεί να στείλει ένα πλαστό UPDATE αίτημα, όπως απεικονίζεται στην εικόνα 17, προκειμένου να τροποποιηθούν οι αρχικές παράμετροι της συνεδρίας ώστε να προκαλέσει μια DOS επίθεση στις παραμέτρους όπως στην QoS ή στις αρχικές διευθύνσεις και τις πόρτες.



Εικόνα 17: UPDATE επίθεση

2.9.5. Η "INFO" επίθεση

Σε πολλές περιπτώσεις, τα SIP δίκτυα μπορούν να χρησιμοποιηθούν ως μεσολαβητές για να διασυνδέσουν τον PSTN μεταφορέα.

Ο λόγος για αυτήν την περίπτωση περιλαμβάνει την χρήση των SIP τηλεφώνων (SIP-T) προκειμένου να μεταβιβαστεί η PSTN σηματοδοσία από έναν PSTN μεταφορέα σε έναν άλλο και αντίστροφα.

Η INFO μέθοδος περιγράφεται ως ένας γενικός μηχανισμός που μεταφέρει τις application-level πληροφορίες κατά μήκος της πορείας της SIP σηματοδοσίας ώστε να επιτρέψει τους tunneling μηχανισμούς. Έχει προταθεί (και, στην πραγματικότητα, χρησιμοποιείται) για μια ποικιλία λειτουργιών, που περιλαμβάνουν:

- Μεταφορά των PSTN μηνυμάτων σηματοδοσίας μεταξύ των PSTN πυλών
- Μεταφορά των DTMF ψηφίων που παράγονται κατά τη διάρκεια μιας SIP συνεδρίας

- Μεταφορά των πληροφοριών του υπόλοιπου λογαριασμού

Το σώμα ενός INFO αιτήματος μπορεί να κρυπτογραφηθεί για λόγους προσωπικού απόρρητου. Εντούτοις, δεν υπάρχει καμία πρόταση για οποιοδήποτε μηχανισμό ασφάλειας για την παροχή της ακεραιότητας και της αυθεντικότητας της INFO μεθόδου. Κατά συνέπεια, η κακόβουλη τροποποίηση της INFO μεθόδου είναι δυνατή και μπορεί να προκαλέσει σοβαρά προβλήματα στα συμβαλλόμενα μέρη επικοινωνίας όπως μη εξουσιοδοτημένη πρόσβαση σε μια κλήση, DOS επίθεση για την αρχική πρόσκληση, λάθη τιμολόγησης, και ούτω καθεξής.

3ο Κεφάλαιο – Μηχανισμοί προστασίας του Signaling

Ένα από τα θεμελιώδη ζητήματα στην ασφάλεια του VoIP είναι η προστασία των μηνυμάτων σηματοδοσίας που ανταλλάσσονται μεταξύ των συμμετεχόντων και των συστατικών. Τα μηνύματα σηματοδοσίας χρησιμοποιούνται στην οργάνωση των επικοινωνιών, στην ανταλλαγή και στην διαχείριση των κρυπτογραφικών κλειδιών για να εξασφαλίσουν τα media streams. Τα μηνύματα σηματοδοσίας μπορεί να διασχίσουν δίκτυα που διατηρούν πολιτικές ασφαλείας αμφισβητήσιμων προτύπων και ποιότητας, και έτσι δημιουργείται ευκαιρία για επίθεση. Η κατάλληλη προστασία των μηνυμάτων σηματοδοσίας παίζει σημαντικό ρόλο στην υπεράσπιση ενάντια στις απειλές και τις επιθέσεις, συμπεριλαμβανομένης της μη εξουσιοδοτημένης πρόσβασης(unauthorized access) στο επίπεδο ελέγχου, της απάτης(fraud), της υποκλοπής(eavesdropping), της εκτροπής κλήσης(call diversion), και άλλων. Επομένως, είναι κρίσιμη η κατανόηση της σπουδαιότητας υπεράσπισης ενός συνόλου θεμελιωδών στόχων ασφάλειας για την προστασία των μηνυμάτων σηματοδοσίας. Αυτοί οι στόχοι ασφάλειας περιλαμβάνουν την αυθεντικότητα, την ακεραιότητα, και την εμπιστευτικότητα των μηνυμάτων. Αυτό το κεφάλαιο προσδιορίζει τους τρόπους για να υποστηριχθούν αυτοί οι στόχοι ασφάλειας.

Μια προκλητική περιοχή για τους μεταφορείς, τους φορείς παροχής υπηρεσιών, και τους ιδιοκτήτες δικτύων επιχειρήσεων είναι η υποστήριξη των προμηθευτών πρωτοκόλλων ασφάλειας για την προστασία του VoIP και των επικοινωνιών του Διαδικτύου. Σε μερικές περιπτώσεις, οι προμηθευτές είναι απρόθυμοι να εξετάσουν τις απειλές και τις επιθέσεις που συνδέονται με τα συγκεκριμένα δίκτυα, γεγονός που οδηγεί στην ανάπτυξη ανασφαλών προϊόντων.

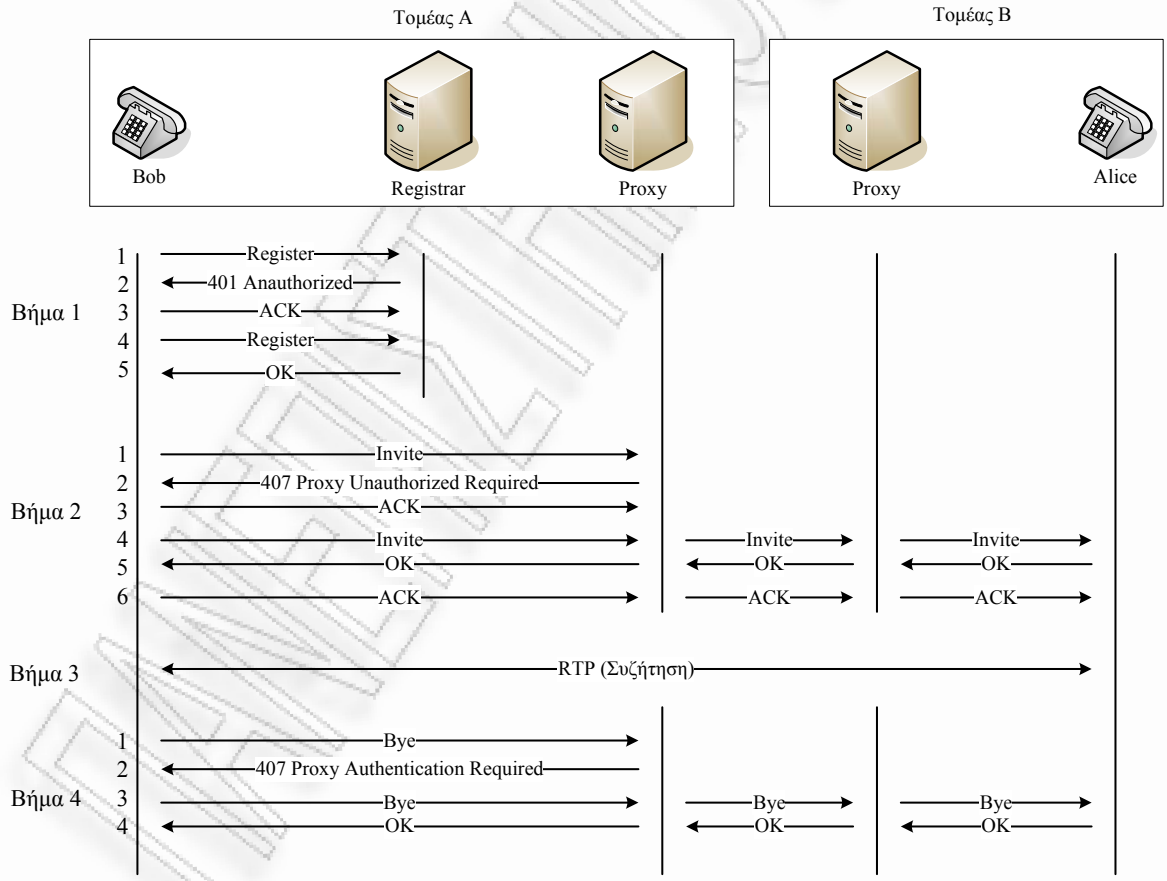
3.1. Μηχανισμοί προστασίας του SIP

Διάφορα πρωτόκολλα μπορούν να χρησιμοποιηθούν για την παροχή της ακεραιότητας και της εμπιστευτικότητας των SIP μηνυμάτων σηματοδοσίας (RFC 3261) ενάντια στις διάφορες επιθέσεις. Αυτές οι συστάσεις περιλαμβάνουν τη χρήση πρωτοκόλλων ασφάλειας όπως IPSec, S/MIME, TLS, και πρόσφατα, DTLS. Αυτές οι συστάσεις είχαν κυμαινόμενη επιτυχία στην υιοθέτηση τους από τη βιομηχανία. Δύο θεμελιώδη μέτρα για την υιοθέτηση των πρωτόκολλων ασφάλειας είναι η ευκολία της εφαρμογής και η δυνατότητα της εξέλιξης. Παραδείγματος χάριν, το TLS προτιμάται από τους προμηθευτές περισσότερο από το S/MIME για την προστασία των SIP μηνυμάτων επειδή το TLS είναι πανταχού παρόν και απαιτεί ελάχιστες αλλαγές στο λογισμικό ή στο firmware για να το υποστηρίξει. Εντούτοις, και οι δύο έχουν τις δυνατότητες και τις αδυναμίες τους. Χαρακτηριστικά, όταν συνδέεται μια SIP συσκευή, όπως ένα SIP hard τηλέφωνο, σε ένα SIP δίκτυο, περνά από τη διαδικασία απόκτησης μίας IP διεύθυνσης χρησιμοποιώντας το DHCP, ένα αρχείο διαμόρφωσης μέσω TFTP (ή ένα άλλο παρόμοιο μηχανισμό) και αναγγέλλει τη διαθεσιμότητά της για την λήψη εισερχόμενων κλήσεων με την καταχώρηση της σε έναν SIP registrar.

Η IP διεύθυνση του SIP registrar μπορεί να ανακαλυφθεί χρησιμοποιώντας τρεις μεθόδους. Ο πρώτος τρόπος είναι με την ανάκτηση ενός αρχείου διαμόρφωσης (παραδείγματος χάριν, ανακτάται κατά τη διάρκεια μιας μεταφοράς TFTP αρχείων), ο δεύτερος χρησιμοποιεί το host μέρος της διεύθυνσης του αρχείου (παραδείγματος χάριν, sip: user@sip-domain.com) και τρίτον χρησιμοποιεί πολλαπλή διανομή (παραδείγματος χάριν, sip.mcat.net ή 224.0.1.75). Η διαδικασία εγγραφής είναι κρίσιμη στην SIP ασφάλεια. Εάν οι επιτιθέμενοι μπορούν να μεταμφιέσουν τα αιτήματα των SIP register, μπορούν να πραγματοποιήσουν διάφορες επιθέσεις όπως παρεκτροπή κλήσης. Επομένως, συνιστάται έντονα οι SIP εγγραφές να επικυρώνονται για την αποφυγή των registration hijacking επιθέσεων. Επιπλέον, τα αιτήματα για την έναρξη κλήσεων (INVITEs) πρέπει επίσης να επικυρώνονται για την παροχή ενός επίπεδου προστασίας ενάντια στην έναρξη των αναρμόδιων κλήσεων και των DOS επιθέσεων ή της ενόχλησης όπως SPIT. Το παρακάτω τμήμα μελετά την επικύρωση της εγγραφής και την δημιουργία της κλήσης.

3.1.1. SIP Αυθεντικοποίηση

Το SIP χρησιμοποιεί την HTTP Digest Authentication για την παροχή προστασίας στην αυθεντικοποίηση και στην επανάληψη των μηνυμάτων αιτήματος για την εγγραφή, την έναρξη και τη λήξη μίας συνεδρίας (παραδείγματος χάριν, REGISTER και INVITE). Χαρακτηριστικά, τα SIP πιστοποιητικά αυθεντικοποίησης είναι σημαντικά μέσα σε μια συγκεκριμένη περιοχή. Μια περιοχή διαχειρίζεται τα πιστοποιητικά των χρηστών της αλλά δεν μπορεί να εξουσιοδοτήσει τα πιστοποιητικά χρηστών της σε άλλες περιοχές εκτός αν υπάρχει μια καθορισμένη ενδοπεριοχική σχέση εμπιστοσύνης. Η εικόνα 18 απεικονίζει μια ροή κλήσης που χρησιμοποιεί τα digest μηνύματα για να επικυρώσει ένα REGISTER αίτημα και ένα επόμενο INVITE αίτημα ώστε να αρχίσει ένα τηλεφώνημα.



Εικόνα 18: Αυθεντικοποίση της SIP εγγραφής και έναρξη της κλήσης.

Η εικόνα 18 απεικονίζει την αυθεντικοποίηση της εγγραφής των συσκευών, την έναρξη και τη λήξη της κλήσης. Να σημειωθεί ότι οι προσωρινές απαντήσεις, όπως 180 Ringing, παραλείπονται για συντομία. Επίσης, η συσκευή πρέπει να επικυρωθεί κατά τη διάρκεια της έναρξης της κλήσης (INVITE) στο βήμα 2.1 και κατά τη διάρκεια της λήξης (BYE) στο βήμα 4.2.

Στο βήμα 1, το SIP τηλέφωνο εγγράφεται στον τοπικό registrar (περιοχή A). Κατά τη διάρκεια της εγγραφής (βήματα 1.1-1.5), ο SIP registrar χρησιμοποιεί μία πρόκληση-επικύρωσης για να επικυρώσει το SIP τηλέφωνο με την αποστολή ενός 401 Unauthorized μηνύματος (που στέλνει ένα nonce) (βήμα 1.2) ως απάντηση στο REGISTER αίτημα του βήματος 1.1. Η συσκευή στέλνει ένα νέο REGISTER αίτημα (στο βήμα 1.4) που περιλαμβάνει τη MD5 digest. Εάν η επικύρωση είναι επιτυχής, ο registrar ενημερώνει τα εσωτερικά αρχεία του για να απεικονίσει τις απαραίτητες πληροφορίες για το χρήστη και τη συσκευή (παραδείγματος χάριν, το URI του χρήστη, την IP διεύθυνση της συσκευής, και ούτω καθεξής) και αποκρίνεται με OK (βήμα 1.5). Ο μηχανισμός της πρόκλησης-επικύρωσης και το σχήμα των μηνυμάτων είναι ίδια για όλες τις SIP μεθόδους. Η μόνη παραλλαγή είναι ότι ένα 401 Unauthorized μήνυμα παράγεται όταν χρησιμοποιείται ένα REGISTER αίτημα, ενώ ένα 407 Proxy Authentication Required μήνυμα παράγεται στις περισσότερες άλλες περιπτώσεις.

Στο βήμα 2, ο χρήστης αρχίζει μια κλήση προς έναν άλλο χρήστη στην περιοχή B. Σε αυτό το βήμα, ο τοπικός SIP proxy (περιοχή A) εκτελεί την πρόκληση-επικύρωση πριν συνεχίζει με την κλήση με την αποστολή ενός 407 Proxy Authentication Required (βήμα 2.2) μηνύματος στο αρχικό INVITE (βήμα 2.1). Τα ακόλουθα επιδεικνύουν τα μηνύματα που ανταλλάσσονται μεταξύ του UA και του proxy.
Το αρχικό INVITE αίτημα στέλνεται χωρίς πληροφορίες αυθεντικοποίησης:

INVITE sip: alice@domain-b.com:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-5ef661a9

From: alice<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0

To: <sip:alice@domain-b.com:5060>

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 101 INVITE

Max-Forwards: 70

Contact: bob<sip:bob@192.168.1.3:5060>

Expires: 240

User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6 (LI)

Content-Length: 313

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER

Content-Type: application/sdp

Ο τοπικός SIP proxy (περιοχή A) προσκαλεί τη συσκευή του χρήστη για να παρέχει τα κατάλληλα πιστοποιητικά:

SIP/2.0 407 Proxy Authentication Required

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-5ef661a9

From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0;

To: <sip:alice@domain-b.com:5060>

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 101 INVITE

Proxy-Authenticate: Digest realm="domain-a.com", domain="sip:domain-a.com", nonce="969467834", algorithm=MD5

Max-Forwards: 15

Content-Length: 0

407 Proxy Authentication Required

Η απάντηση του τοπικού SIP proxy περιέχει μία Proxy-Authenticate επιγραφή που περιλαμβάνει τον τομέα, την περιοχή, το nonce, και τον digest αλγόριθμο ώστε να χρησιμοποιηθούν στην παραγωγή της απάντησης στην πρόκληση (MD5 σε αυτήν την περίπτωση):

Proxy-Authenticate: Digest realm="domain-a.com", domain="sip:domain-a.com", nonce="969467834", algorithm=MD5

Το SIP τηλέφωνο αναγνωρίζει το μήνυμα του SIP proxy με την αποστολή ενός ACK:

ACK sip:alice@domain-b.com:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-5ef661a9
From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0
To: <sip:alice@domain-b.com:5060>
Call-ID: ceab1739-db25a1e9@192.168.1.3
CSeq: 101 ACK
Max-Forwards: 70
Contact: bob<sip:bob@domain-a.com:5060>
User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6 (LI)
Content-Length: 0

Το SIP τηλέφωνο στέλνει έναν νέο INVITE αίτημα που περιλαμβάνει τα πιστοποιητικά του χρήστη στην Proxy-Authorization επιγραφή. Επιπλέον, το CSeq έχει αυξηθεί από το 101 στο 102 για να δείξει ότι αυτό το INVITE αίτημα ανήκει σε έναν νέο διάλογο:

INVITE sip:alice@domain-b.com:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-d04dcaa1
From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0
To: <sip:alice@domain-b.com:5060>
Call-ID: ceab1739-db25a1e9@192.168.1.3
CSeq: 102 INVITE
Max-Forwards: 70

Proxy-Authorization: Digest username="bob", realm="domain-a.com", nonce="969467834", uri="sip:alice@domain-b.com:5060", algorithm=MD5, response="72f370515acd0b878bce1e9e78899ad2"

Contact: bob<sip:bob@domain-a.com:5060>

Expires: 240

User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6 (LI)

Content-Length: 313

Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER

Content-Type: application/sdp

Όταν ο απομακρυσμένος χρήστης σηκώσει το τηλέφωνο, η συσκευή του στέλνει μια OK απάντηση:

SIP/2.0 200 OK

Via: SIP/2.0/UDP domain-a.com:5060; branch=z9hG4bK-f7bb35c3

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-d04dcaa1

From: bob< sip:alice@domain-b.com:5060>; tag=aed516f97e1da529o0;

To: <sip: sip:bob@domain-a.com:5060>; tag=2027561073

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 102 INVITE

Contact: <sip:alice@domain-b.com:5060>

Max-Forwards: 15

Content-Type: application/sdp

Content-Length: 217

Σε αυτό το σημείο, το αρχικό τηλέφωνο ολοκληρώνει την δημιουργία της συνεδρίας με την αποστολή ενός ACK, το οποίο περιλαμβάνει τις πληροφορίες έγκρισης:

ACK sip: alice@domain-b.com:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-6ee04695

From: bob<sip:bob@domain-a.com;5060>; tag=aed516f97e1da529o0

To: <sip:alice@domain-b.com:5060>; tag=2027561073

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 102 ACK

Max-Forwards: 70

Proxy-Authorization: Digest username="bob", realm="domain-a.com", nonce="969467834", uri="sip:alice@domain-b.com:5060", algorithm=MD5, response="28909c2f5b3f682b2d8bc6a36aba572c"

Contact: bob<sip:bob@domain-a.com:5060>

User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6 (LI)

Content-Length: 0

Να σημειωθεί ότι το RFC δεν υποχρεώνει τις SIP εφαρμογές να προκαλέσουν ένα ACK επειδή δεν απαιτεί μια απάντηση. Με άλλα λόγια, όταν ο SIP proxy λαμβάνει το ACK, δεν πρέπει να αποκριθεί με ένα 407 Proxy Authentication Required μήνυμα. Αφήνεται πάνω στη SIP συσκευή που δημιουργεί το αίτημα να επαναχρησιμοποιήσει τις ίδιες πληροφορίες έγκρισης που χρησιμοποιήθηκαν στα προηγούμενα μηνύματα.
Όταν η συνομιλία μεταξύ των δύο χρηστών ολοκληρώνεται και κλείνουν το τηλέφωνο, ένα BYE αίτημα παράγεται. Στο παράδειγμά μας, το BYE αίτημα δημιουργήθηκε από την Alice και επικυρώνεται από τον τοπικό proxy (περιοχή A):

BYE sip:alice@domain-b.com:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-304dbcd

From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0

To: <sip:alice@domain-b.com:5060>; tag=2027561073

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 103 BYE

Max-Forwards: 70

Proxy-Authorization: Digest username="bob", realm="domain-a.com", nonce="969467834", uri="sip:alice@domain-b.com:5060", algorithm=MD5, response="96645bfe26e2a5b64803041948bba38d"

User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6 (LI)

Content-Length: 0

Στο παράδειγμά μας, ο τοπικός SIP proxy για την περιοχή Α απαιτεί από την συσκευή του χρήστη να επικυρώσει το BYE αίτημα, και αποκρίνεται με ένα 407 Proxy Authentication Required μήνυμα:

SIP/2.0 407 Proxy Authentication Required

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-304dbcd

From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0

To: <sip:alice@domain-b.com:5060>; tag=2027561073

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 103 BYE

Proxy-Authenticate: Digest realm="domain-a.com", domain="sip:domain-a.com", nonce="35921938", algorithm=MD5

Max-Forwards: 15

Content-Length: 0

Το SIP τηλέφωνο του χρήστη αναπαράγει το BYE αίτημα και περιλαμβάνει τις σωστές πληροφορίες επικύρωσης:

BYE sip:alice@domain-b.com:5060 SIP/2.0

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-1be1b199

From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0

To: <sip:alice@domain-b.com:5060>; tag=2027561073

Call-ID: ceab1739-db25a1e9@192.168.1.3

CSeq: 104 BYE

Max-Forwards: 70

Proxy-Authorization: Digest username="alice", realm="domain-a.com", nonce="35921938", uri="sip:alice@domain-b.com:5060", algorithm=MD5, response="f17f737430b236c73121ecf6a1031518"
User-Agent: 001217E57E31 Linksys/RT31P2-3.1.6 (LI)
Content-Length: 0

Τέλος, το τηλέφωνο του μακρινού χρήστη αποκρίνεται με ένα OK μήνυμα, και η συνεδρία τερματίζεται:

SIP/2.0 200 OK

Via: SIP/2.0/UDP 192.168.1.3:5060; branch=z9hG4bK-1be1b199
From: bob<sip:bob@domain-a.com:5060>; tag=aed516f97e1da529o0
To: <sip:alice@domain-b.com:5060>; tag=2027561073
Call-ID: ceab1739-db25a1e9@192.168.1.3
CSeq: 104 BYE
Max-Forwards: 15
Content-Length: 0

Οι SIP εφαρμογές μπορούν να επιβάλουν την πρόκληση-επικύρωσης σε διάφορους βαθμούς, οι οποίοι μπορούν να μην παρέχουν τη βέλτιστη ασφάλεια. Παραδείγματος χάριν, μια εφαρμογή μπορεί να επικυρώσει μόνο τα REGISTER αιτήματα, χωρίς να απαιτεί την επικύρωση των INVITE. Μια άλλη εφαρμογή μπορεί να απαιτήσει την επικύρωση για τα REGISTER και INVITE αλλά όχι για τα BYE ή CANCEL αιτήματα. Αυτές οι ασυνέπειες εισάγουν ευκαιρίες για επιθέσεις, όπως η αναρμόδια έναρξη ή λήξη της κλήσης.

Για την προστασία από τις replay ή message-masquerading επιθέσεις, η πρόκληση-επικύρωσης πρέπει να χρησιμοποιηθεί για όλα τα αιτήματα που προορίζονται να δημιουργήσουν, να τροποποιήσουν, ή να ολοκληρώσουν μια συνεδρία. Τέτοια αιτήματα είναι τα INVITE, BYE, ACK, και REFER.

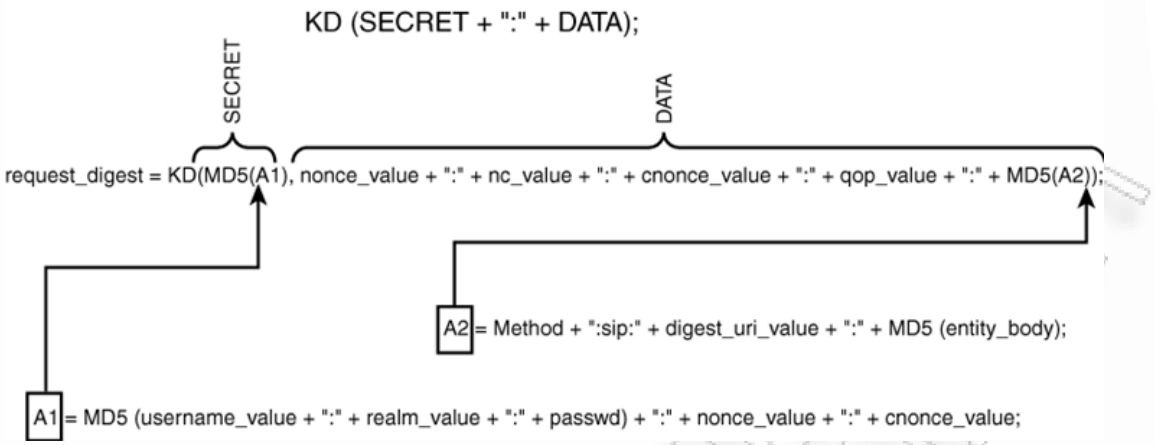
Η SIP RFC 3261 σημειώνει ότι η CANCEL μέθοδος δεν πρέπει να προκληθεί από τους proxy επειδή αυτή η μέθοδος δεν μπορεί να υποβληθεί εκ νέου. Αφήνεται πάνω στον SIP proxy που λαμβάνει το CANCEL αίτημα να ελέγξει ότι το αίτημα δημιουργήθηκε από μια πηγή (παραδείγματος χάριν, έναν SIP proxy) για την οποία υπάρχει μια σχετική SIP συνεδρία. Αυτή η οδηγία υποθέτει ότι υπάρχει ένας σύνδεσμος μεταφοράς ή ασφάλειας στρωμάτων δικτύου σε ισχύ, όπως τα IPSec ή TLS. Αυτή η υπόθεση δημιουργεί μια ευκαιρία για κατάχρηση στις SIP εφαρμογές που χρησιμοποιούν το UDP για την μεταφορά των πρωτοκόλλων και δεν χρησιμοποιούν το IPSec.

Εάν οι επιτιθέμενοι συλλέξουν τις ιδιότητες ενός SIP διαλόγου (παραδείγματος χάριν, χρησιμοποιώντας eavesdropping για να συλλέξει πληροφορίες όπως την ταυτότητα του χρήστη που τηλεφωνεί, το CSeq, κ.τ.λ), μπορούν να μεταμφιέσουν ένα κακόβουλο CANCEL αίτημα για να αποδιοργανώσει την δημιουργία μιας κλήσης. Αυτήν την περίοδο, τα περισσότερα προϊόντα υποστηρίζουν την επικύρωση των SIP INVITE και REGISTER μεθόδων αλλά όχι των BYE ή CANCEL.

Να σημειωθεί ότι γίνονται συζητήσεις στην IETF για να εξετάσουν την ιδέα της προστασίας των τελικών και προσωρινών απαντήσεων (παραδείγματος χάριν, 183, 180) που στέλνονται μέσω του UDP χρησιμοποιώντας κρυπτογραφικούς μηχανισμούς για να διατηρήσουν την ακεραιότητα του μηνύματος. Ο στόχος είναι η προστασία από τις μεταμφιεσμένες προσωρινές απαντήσεις που μπορούν να έχουν επίπτωση στην κατάσταση μιας SIP συνεδρίας.

Ο μηχανισμός που χρησιμοποιείται για να παράγει ένα digest μήνυμα στα SIP αιτήματα εφαρμόζεται σε όλα τα SIP αιτήματα (παραδείγματος χάριν, στα REGISTER, INVITE, και ούτω καθεξής) και φαίνεται στην εικόνα 19.

παραγωγή της απάντησης στην SIP πρόκληση



Εικόνα 19: Διαδικασία για την παραγωγή της απάντησης στην SIP πρόκληση για την SIP αυθεντικοποίηση

Ο σκοπός για κάθε μια από τις μεταβλητές που απεικονίζονται είναι ο ακόλουθος:

- nonce_value ~ Μια server-specified συμβολοσειρά δεδομένων που παράγεται μεμονωμένα κάθε φορά που υποβάλλεται ένα αίτημα.
- nc_value (nonce αρίθμηση) ~ Αυτή είναι μια δεκαεξαδική αρίθμηση του πλήθους των αιτημάτων που ο client έχει στείλει με την nonce τιμή μέσα σε ένα αντίστοιχο αίτημα. Παραδείγματος χάριν, όταν ο client στέλνει το πρώτο αίτημα σε μία απάντηση σε μια δοθείσα nonce τιμή, περιλαμβάνει την «nc=00000001». Η αρίθμηση nonce απαιτείται εάν χρησιμοποιείται η qpop.
- cnonce_value ~ Αυτή είναι μια αδιαφανής παρατιθέμενη συμβολοσειρά που παρέχεται από τον client και χρησιμοποιείται και από τον client και από τον server για την αποφυγή των plaintext επιθέσεων και για την παροχή της αμοιβαίας επικύρωσης και του ενός επιπέδου προστασίας της ακεραιότητας μηνύματος.
- qpop_value ~ Δείχνει την ποιότητα της προστασίας. Δύο τιμές καθορίζονται στην παρούσα φάση. Δείτε RFC 2617. Η τιμή «auth,» που δείχνει την επικύρωση, και η τιμή «auth- int», η οποία δείχνει την επικύρωση με την προστασία της ακεραιότητας.
- A1 ~ Η MD5 digest των τιμών του ονόματος του χρήστη, της realm, του κωδικού πρόσβασης, της nonce, και της cnonce:

- ✓ username_value: Το όνομα του χρήστη στη διευκρινισμένη realm.
- ✓ realm_value: Μια συμβολοσειρά που περιέχει το όνομα του host που εκτελεί την επικύρωση και τη σχετική περιοχή (παραδείγματος χάριν, sipserver.domain.com).
- ✓ passwd: Ο αντίστοιχος κωδικός πρόσβασης χρήστη ή της συσκευής που συνδέεται με το όνομα χρήστη
- ✓ nonce_value: Κοίτα προηγούμενη περιγραφή.
- ✓ cnonce_value: Κοίτα προηγούμενη περιγραφή.

- A2 ~ Η MD5 digest της μεθόδου, digest της URI τιμής, και του σώματος οντοτήτων:
  - ✓ Method: Η SIP μέθοδος που υποδεικνύεται στο αντίστοιχο SIP μήνυμα.
  - ✓ digest_uri_value. Το URI από το Request-URI της Request-Line; αναπαραγμένο εδώ επειδή οι proxy επιτρέπονται να αλλάξουν την Request-Line κατά τη μεταφορά

Το αποτέλεσμα είναι μια συμβολοσειρά 32 δεκαεξαδικών χαρακτήρων που αποθηκεύονται στον Response πεδίο στην Proxy-Authorization επιγραφή, όπως παρουσιάζεται εδώ:

Proxy-Authorization: Digest username="alice", realm="domain-a.com", nonce="35921938", uri="sip:alice@domain-b.com:5060", algorithm=MD5, **response="f17f737430b236c73121ecf6a1031518"**

Αν και η SIP digest του μηνύματος παρέχει ένα επίπεδο προστασίας για τα INVITE και REGISTER αιτήματα που ανταλλάσσονται μεταξύ των SIP οντοτήτων, δεν προστατεύει άλλες SIP μεθόδους, όπως τις CANCEL, BYE, και τις προσωρινές ή τελικές απαντήσεις (παραδείγματος χάριν, 486 Busy Here). Αυτή την αδυναμία μπορεί να εκμεταλλευτεί ένας επιτιθέμενος για να εξαπατήσει τις SIP μεθόδους ή τις προσωρινές ή τελικές απαντήσεις ώστε να εκτελέσει μια επίθεση. Ένας τρόπος για την προστασία από μια επίθεση παραποίησης των μηνυμάτων ή της ροής της κλήσης είναι η κρυπτογράφηση των μηνυμάτων σηματοδοσίας χρησιμοποιώντας ένα

πρωτόκολλο ασφάλειας όπως TLS, S/MIME, και IPSec ή επικυρώνοντας τις SIP απαντήσεις.

Άλλη μία ανησυχητική περιοχή είναι η SIP αυθεντικοποίηση δια μέσου περιοχών που μπορεί να διατηρούν διαφορετικές πολιτικές ή καμία πολιτική.

3.1.2. Κοινές παγίδες που πρέπει να αποφεύγονται κατά την εφαρμογή της SIP αυθεντικοποίησης

Αν και ο μηχανισμός της SIP πρόκλησης-επικύρωσης προσφέρει προστασία ενάντια στις replay επιθέσεις, διάφορες SIP εφαρμογές διατηρούν αδύναμες ιδιότητες και μπορεί να επιτρέψουν σε κάποιον να επαναλάβει τα SIP μηνύματα και να παρακάμψει επιτυχώς τους ελέγχους ασφαλείας. Για την αποφυγή μερικών από αυτές τις παγίδες, θα πρέπει να ακολουθηθούν οι παρακάτω συστάσεις:

- Παραγωγή nonce συμβολοσειρών χρησιμοποιώντας κρυπτογραφικές ψευδοτυχαίες συναρτήσεις.

- Υποστήριξη της SIP πρόκλησης-επικύρωσης για τα SIP μηνύματα που αρχίζουν, τροποποιούν, ή ολοκληρώνουν μια συνεδρία

- Αποφυγή της εναποθήκευσης ή της επαναχρησιμοποίησης των πιστοποιητικών επικύρωσης των χρηστών.

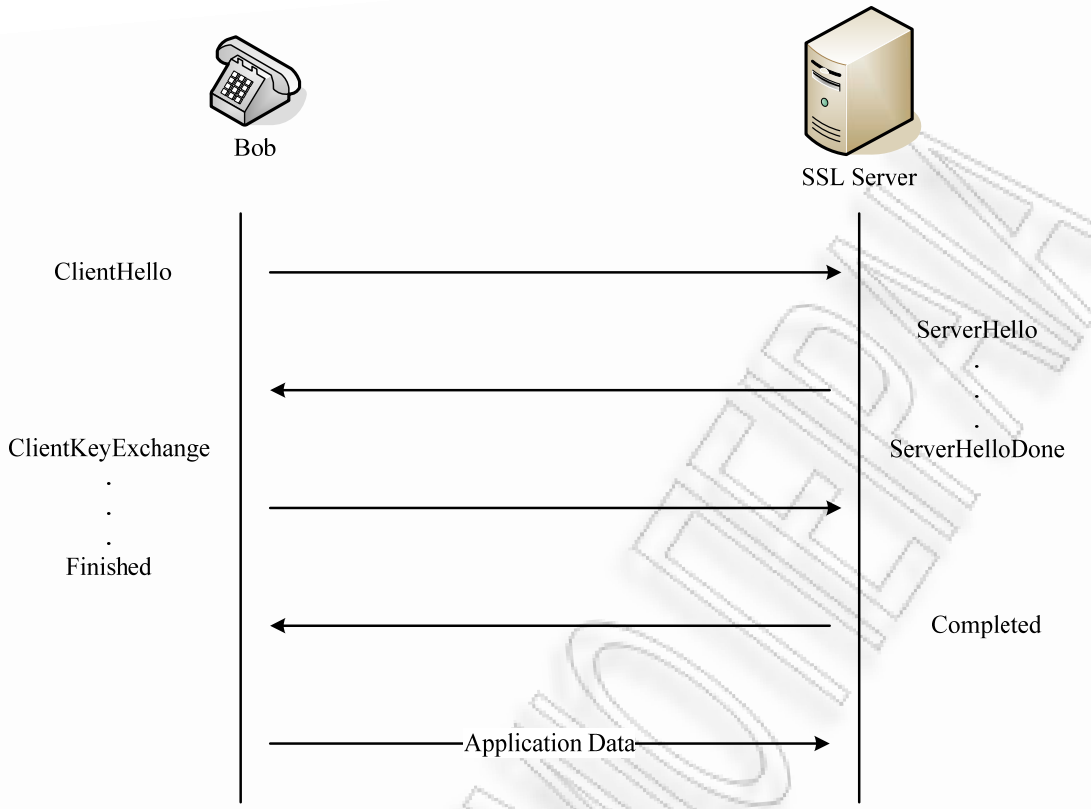
- Χρησιμοποίηση των πρωτοκόλλων δικτύων ή ασφάλειας μεταφορών για την προστασία των μηνυμάτων σηματοδοσίας (παραδείγματος χάριν, IPSec, TLS, DTLS, ή S/MIME).

3.2. Transport Layer Security

Ένα από τα αποδεκτά πρωτόκολλα από την βιομηχανία για την υποστήριξη της εμπιστευτικότητας του στρώματος μεταφοράς είναι το TLS. Το Transport Layer Security έκδοσης 1.1 καθορίζεται στο RFC 4346, και παρέχει τη δυνατότητα να εκτελεσθεί αμοιβαία αυθεντικοποίηση (client και server), εμπιστευτικότητα, και ακεραιότητα. Το πρωτόκολλο αποτελείται από δύο στρώματα: το πρωτόκολλο TLS Record και το πρωτόκολλο TLS Handshake.

Το πρωτόκολλο TLS Record στοχεύει στην διατήρηση μιας ασφαλούς σύνδεσης μεταξύ δύο τελικών σημείων (παραδείγματος χάριν, client και server). Η διαπραγμάτευση των κρυπτογραφικών ιδιοτήτων (παραδείγματος χάριν, κρυπτογραφικές ακολουθίες, κλειδιά κρυπτογράφησης) για την αντίστοιχη σύνδεση εκτελείται από το πρωτόκολλο TLS Handshake, το οποίο είναι ενθυλακωμένο μέσα στο πρωτόκολλο TLS Record.

Το πρωτόκολλο TLS Handshake χρησιμοποιείται για την αμοιβαία αυθεντικοποίηση client/server και για την διαπραγμάτευση των κρυπτογραφικών ιδιοτήτων (παραδείγματος χάριν, αλγόριθμοι κρυπτογράφησης και κλειδιά) της αντίστοιχης συνεδρίας. Το TLS Handshake πρέπει να ολοκληρωθεί επιτυχώς πριν διαβιβαστούν τα δεδομένα. Η εικόνα 20 παρουσιάζει την TLS client/server Handshake.



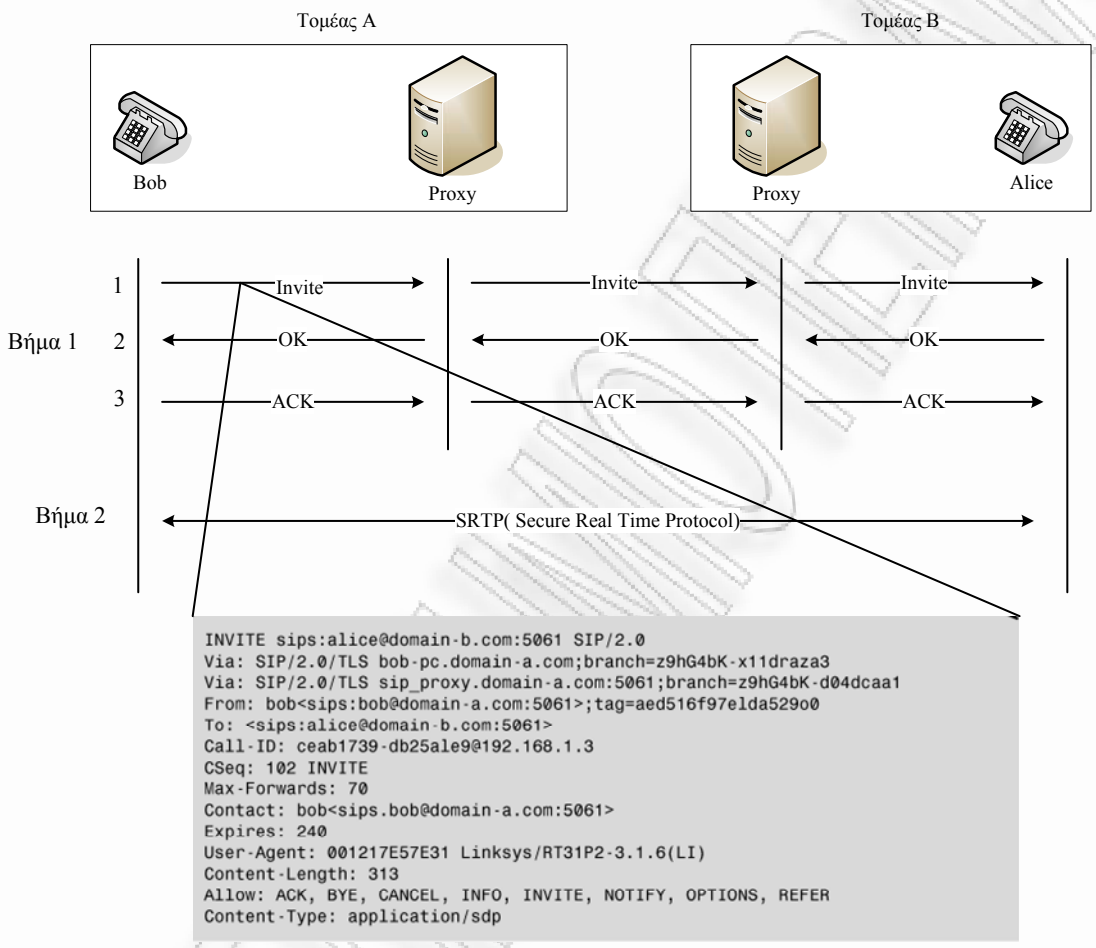
Εικόνα 20: Η TLS handshake όπως καθορίζεται στην RFC 4346.

Το TLS έχει σχεδιαστεί με σκοπό να χρησιμοποιηθεί πάνω σε μια αξιόπιστη μεταφορά όπως το TCP ή SCTP. Αυτό εισάγει έναν περιορισμό για τις εφαρμογές που χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς επειδή το TLS δεν μπορεί να χρησιμοποιηθεί με το UDP για να προστατεύσει τα SIP μηνύματα. Πρόσφατα, το IETF έχει δημοσιεύσει το RFC 4347, «Datagram Transport Layer Security», για να εξετάσει αυτόν τον περιορισμό, και συζητείται αργότερα σε αυτό το κεφάλαιο.

3.2.1. SIP και TLS

Η SIP RFC συστήνει τη χρήση του TLS για την παροχή της απαραίτητης προστασίας ενάντια στις επιθέσεις όπως eavesdropping, message tampering, message replay, και ούτω καθεξής. Όταν οι χρήστες θέλουν να δημιουργήσουν μια κλήση και να διατηρήσουν ένα επίπεδο ιδιοαπορρήτου, μπορούν να χρησιμοποιήσουν τα SIPS URI (secure SIP ή SIP over TLS) για να είναι εγγυημένο ότι μια ασφαλής, κρυπτογραφημένη μεταφορά χρησιμοποιείται για να προστατεύσει τα μηνύματα

σηματοδοσίας μεταξύ δύο χρηστών. Η εικόνα 21 απεικονίζει μια απλή ροή κλήσης που χρησιμοποιεί τα SIPS. Αν και η εικόνα δεν απεικονίζει την αρχική TLS handshake, υποτίθεται ότι τα SIP μηνύματα ανταλλάσσονται χρησιμοποιώντας το TLS.



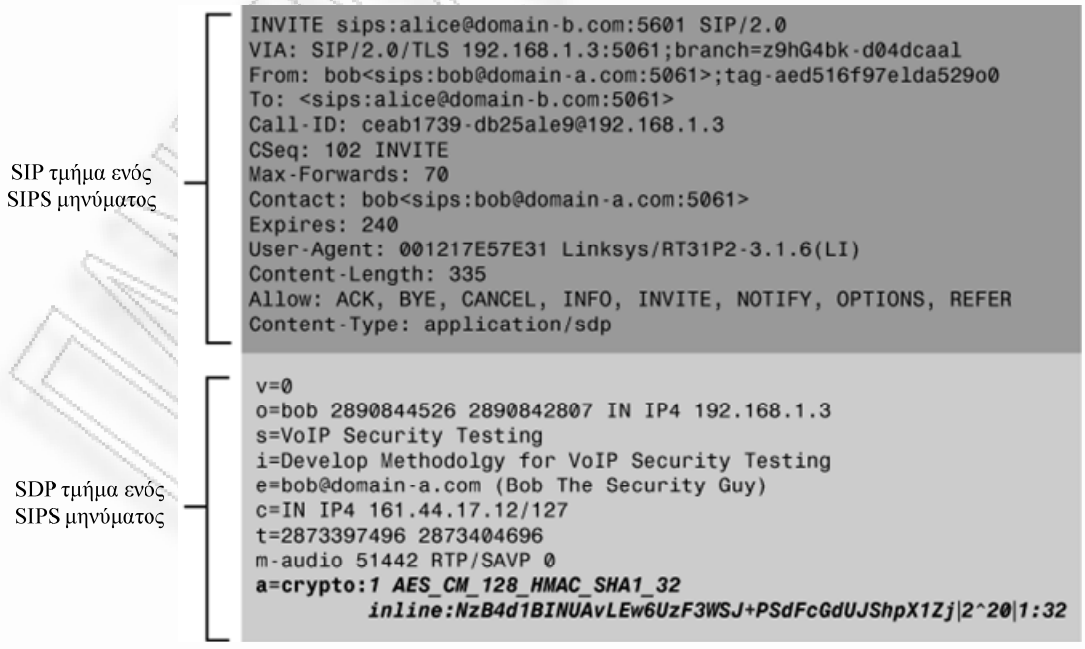
Εικόνα 21: Χρήση του Secure SIP (SIPS).

Το SIPS μήνυμα είναι παρόμοιο με ένα SIP (unencrypted) μήνυμα που μεταφέρεται άνω των UDP, TCP, ή STCP. Οι μεγαλύτερες διαφορές είναι οι ακόλουθες:

- Η σύνταξη του URI ορίζεται ως *sips:* alice@domain-b.com.
- Η μεταφορά γίνεται μέσω του TLS, αντί του UDP ή TCP.
- Η SIPS πόρτα είναι η 5061, αντί της 5060, η οποία είναι δεσμευμένη για τα UDP και TCP.

Όταν χρησιμοποιείται το SIPS, όλα τα SIP μηνύματα μεταφέρονται χρησιμοποιώντας το TLS, που παρέχει ένα επαρκές επίπεδο προστασίας ενάντια στις επιθέσεις όπως eavesdropping, replay, και τροποποίηση μηνυμάτων. Επιπλέον, το TLS παρέχει τα μέσα για αμοιβαία αυθεντικοποίηση χρησιμοποιώντας πιστοποιητικά για την προστασία από τις «man-in-the-middle» επιθέσεις. Η συσκευή μπορεί να επικυρώσει τον εαυτό της στο δίκτυο, αλλά μπορεί επίσης να ελέγξει την αυθεντικότητα του SIP proxy (ή του SIP registrar). Το προτεινόμενο πρότυπο κρυπτογράφησης για να χρησιμοποιηθεί στο SIPS είναι το AES (Advanced Encryption Standard), χρησιμοποιώντας ένα 128-bit κλειδί στην CBC (Cipher Block Chaining) μέθοδο, και ο προτεινόμενος κώδικας επικύρωσης μηνυμάτων είναι ο SHA-1 για την παροχή της ακεραιότητας.

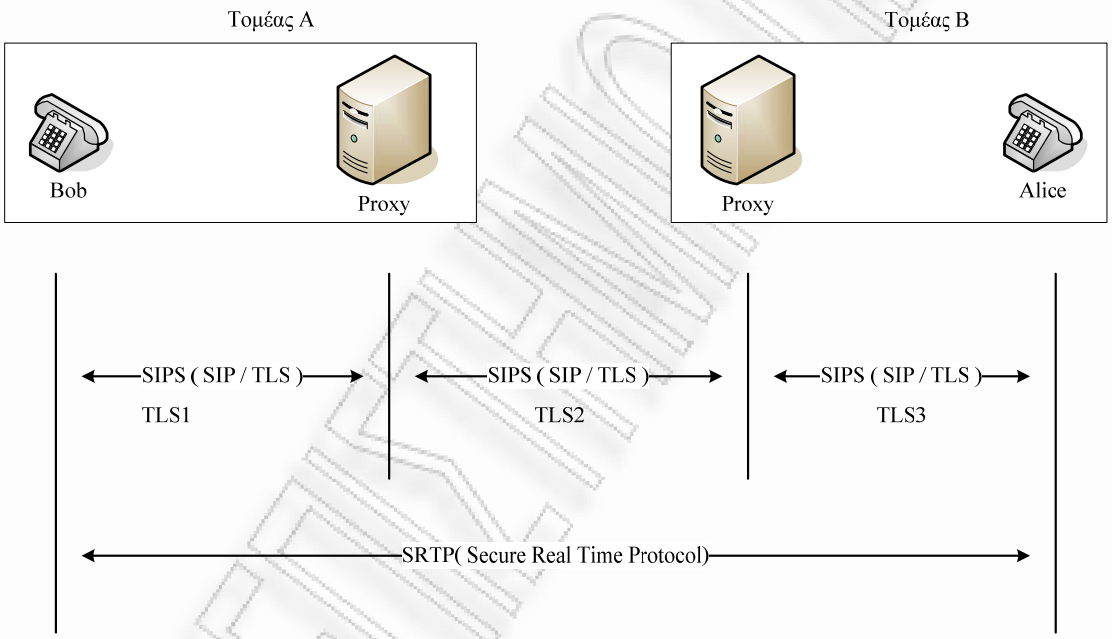
Ένα άλλο επιπρόσθετο όφελος στην χρήση του SIPS είναι η δυνατότητα να ανταλλαχθούν τα κλειδιά κρυπτογράφησης με σκοπό να κρυπτογραφηθεί το ρεύμα δεδομένων χρησιμοποιώντας το SRTP (Secure Real Time Protocol). Παραδείγματος χάριν, το SDescriptions μπορεί να χρησιμοποιηθεί μέσα σε ένα SIPS INVITE αίτημα για να ανταλλάξει το κύριο κλειδί μεταξύ δύο συμμετεχόντων. Το κλειδί κρυπτογράφησης παρέχεται στο SDP τμήμα του SIPS INVITE στην a=crypto ιδιότητα. Η εικόνα 22 παρέχει ένα παράδειγμα.



Εικόνα 22: SIPS μήνυμα με τις SDescriptions crypto ιδιότητες

Το SDescriptions είναι ένας από τους key-exchange μηχανισμούς που συζητούνται αυτήν την περίοδο στο IETF, συμπεριλαμβανομένου των ZRTP και MIKEY(Multimedia Internet KEYing).

Αν και το TLS παρέχει την εμπιστευτικότητα μεταξύ δύο τελικών σημείων (σχέση client/server), δεν υποστηρίζει την άμεση end-to-end εμπιστευτικότητα μεταξύ δύο χρηστών που συνδέονται μέσω ενδιάμεσων SIP proxies. Για κάθε τμήμα, μια ευδιάκριτη TLS σύνδεση πρέπει να εγκατασταθεί. Η εικόνα 23 απεικονίζει αυτή την σχέση.



Εικόνα 23: SIP προστασία μηνύματος που χρησιμοποιεί το TLS σε μια per-hop βάση.

Για αυτήν την συζήτηση, αναφερόμαστε σε μια σύνδεση hop μεταξύ δύο διαδοχικών συστατικών. Αν και η SSL παρέχει επαρκή προστασία για τα SIP μηνύματα, έχει τους περιορισμούς της. Κάθε ενδιάμεσος SIP proxy πρέπει να αναλύσει τις SIP επιγραφές για να οδηγήσει το μήνυμα κατάλληλα, και επομένως η SSL σύνδεση ολοκληρώνεται και επανιδρύεται μεταξύ των hops. Για κάθε hop (παραδείγματος χάριν, μια σύνδεση μεταξύ του Bob και του proxy της A περιοχής του), υπάρχει μια ευδιάκριτη SSL σύνδεση που καθιερώνεται, SSL1. Αυτή η σύνδεση μπορεί να διατηρήσει μια

διαφορετική πολιτική ασφαλείας (παραδείγματος χάριν, ισχυρότερες ή πιο αδύναμες κρυπτογραφικές ακολουθίες) από το επόμενο hop μεταξύ του proxy της περιοχής A και του proxy της περιοχής B, SSL2. Το ίδιο μπορεί να ειπωθεί για τη σύνδεση SSL3.

Σε μερικές περιπτώσεις, δεν είναι γνωστό εάν ένας ενδιάμεσος SIP proxy που βρίσκεται πέρα από την περιοχή του χρήστη μπορεί να υποστηρίξει παρόμοια ή ισχυρότερη πολιτική ασφαλείας ή ακόμα και να υποστηρίζει την SSL. Αυτή η κατάσταση μπορεί να περιπλέξει την εγκατάσταση κλήσης με διάφορες εκβάσεις, συμπεριλαμβανομένων των εξής:

- Η προσπάθεια να εγκατασταθεί η κλήση μπορεί να είναι ανεπιτυχής ανάλογα με το πώς η πολιτική ασφαλείας του χρήστη επιβάλλεται.
- Η σύνδεση μπορεί να εγκατασταθεί με μια πιο αδύναμη ισχύ των κρυπτογραφικών ακολουθιών από αυτή που καθορίζεται στην πολιτική του χρήστη.
- Η σύνδεση μπορεί να εγκατασταθεί χωρίς προστασία μεταξύ των δύο proxy στο συγκεκριμένο τμήμα δικτύου.
- Η σύνδεση μπορεί να εγκατασταθεί χωρίς καθόλου προστασία.

Οποιαδήποτε και αν είναι η έκβαση, ο τελικός χρήστης μπορεί πιθανότατα να μην γνωρίζει τις ασυνέπειες που εμφανίζονται και να διατηρεί μια ψεύτικη αίσθηση ιδιοαπορρήτου. Παραδείγματος χάριν, κατά την δημιουργία μιας διεθνούς κλήσης, δεν υπάρχει εγγύηση ότι όλοι οι ενδιάμεσοι φορείς παροχής υπηρεσιών θα υποστηρίξουν το SIPS είτε λόγω των τεχνολογικών περιορισμών είτε των ρυθμιστικών περιορισμών. Αυτή η έλλειψη της από άκρο σε άκρο εμπιστευτικότητας θα εκθέσει τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται με το SRTP εάν η διαπραγμάτευση των κλειδιών πραγματοποιείται χρησιμοποιώντας το SIP και όχι το SIPS. Από την άλλη μεριά, το ρεύμα δεδομένων δεν χρειάζεται να περάσει μέσω των ενδιάμεσων συστατικών όπως κάνει το SIP, εκτός αν έχει συντονιστεί για να κάνει έτσι. Αντ' αυτού, μια peer-to-peer σύνδεση εγκαθίσταται, όπως απεικονίζεται στην εικόνα 23, για την οποία η εμπιστευτικότητα επιτυγχάνεται χρησιμοποιώντας το SRTP.

3.2.2. Δυνατότητες και περιορισμοί της χρησιμοποίησης του TLS

Το TLS παρέχει διάφορα χαρακτηριστικά γνωρίσματα για την προστασία των SIP μηνυμάτων σηματοδοσίας και μπορεί να χρησιμοποιηθεί ως μηχανισμός για την RTP ανταλλαγή κλειδιών. Παράλληλα, μερικοί περιορισμοί πρέπει να ληφθούν υπόψη για να αξιολογήσουν την αποτελεσματικότητά του σε ένα συγκεκριμένο περιβάλλον.

- **Δυνατότητες**

  - ✓ Υποστηρίζει αμοιβαία αυθεντικοποίηση χρησιμοποιώντας πιστοποιητικά.
  - ✓ Παρέχει την εμπιστευτικότητα και την ακεραιότητα των μηνυμάτων, οι οποίες μπορούν να προστατεύσουν ενάντια στις επιθέσεις όπως eavesdropping, message tampering, και replay.
  - ✓ Η πανταχού παρούσα ύπαρξη της SSL παρέχει ευκολότερη υιοθέτηση και ανάπτυξη.
  - ✓ Μπορεί να προστατεύσει τη διαπραγμάτευση των κρυπτογραφικών κλειδιών.
  - ✓ Επιβεβαιωμένο πρωτόκολλο, χρησιμοποιείται ευρέως στις εφαρμογές Διαδικτύου (εφαρμογές Web, ηλεκτρονικό ταχυδρομείο, VPN).
  - ✓ Χαμηλός αντίκτυπος απόδοσης έναντι άλλων πρωτοκόλλων ασφάλειας όπως IPSec.

- **Περιορισμοί**

  - ✓ Απαιτεί μια PKI υποδομή για να επιβάλει την αμοιβαία αυθεντικοποίηση στο SSL στρώμα.
  - ✓ Δεν παρέχει άμεση από άκρο σε άκρο εμπιστευτικότητα. Απαιτεί τη λήξη και τη δημιουργία μιας νέας συνεδρίας σε κάθε hop (παραδείγματος χάριν, μεταξύ των SIP proxy ή των ελεγκτών συνόρων συνεδρίας).
  - ✓ Μπορεί να χρησιμοποιηθεί με τα TCP και SCTP αλλά όχι με το UDP, το οποίο προσκρούει στις SIP εφαρμογές που χρησιμοποιούν το UDP.

Πολλές SIP εφαρμογές στα δίκτυα επιχειρήσεων και μεταφορέων χρησιμοποιούν αποκλειστικά SIP πάνω σε UDP.

- ✓ Ευάλωτο στις DOS επιθέσεις όπως τις TCP πλημμύρες και τις RSTs (επαναρύθμιση σύνδεσης). Μια επίθεση TCP πλημμυρών στοχεύει να καταναλώσει τους πόρους συστήματος (παραδείγματος χάριν, κύκλοι CPU) εκτελώντας RSA αποκρυπτογράφηση. Επίσης, ένας επιτιθέμενος μπορεί να παράγει μεταμφιεσμένα RST πακέτα ή TLS αρχεία για να τερματίσει μια σύνδεση πρόωρα.

3.3. Datagram Transport Layer Security

Το πρωτόκολλο Datagram Transport Layer Security, που καθορίστηκε στο RFC 4347, αναπτύχθηκε για να καλύψει την ανάγκη για παροχή ισοδύναμης προστασίας με το TLS στα πρωτόκολλα του στρώματος εφαρμογής που χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς, όπως κάνει το SIP. Το DTLS είναι παρόμοιο με το TLS σε πολλά σημεία, συμπεριλαμβανομένου του περιορισμού απαίτησης μιας νέας εγκατάστασης συνεδρίας μεταξύ των hops ώστε να προστατευθούν τα SIP μηνύματα από ένα τελικό σημείο σε άλλο.

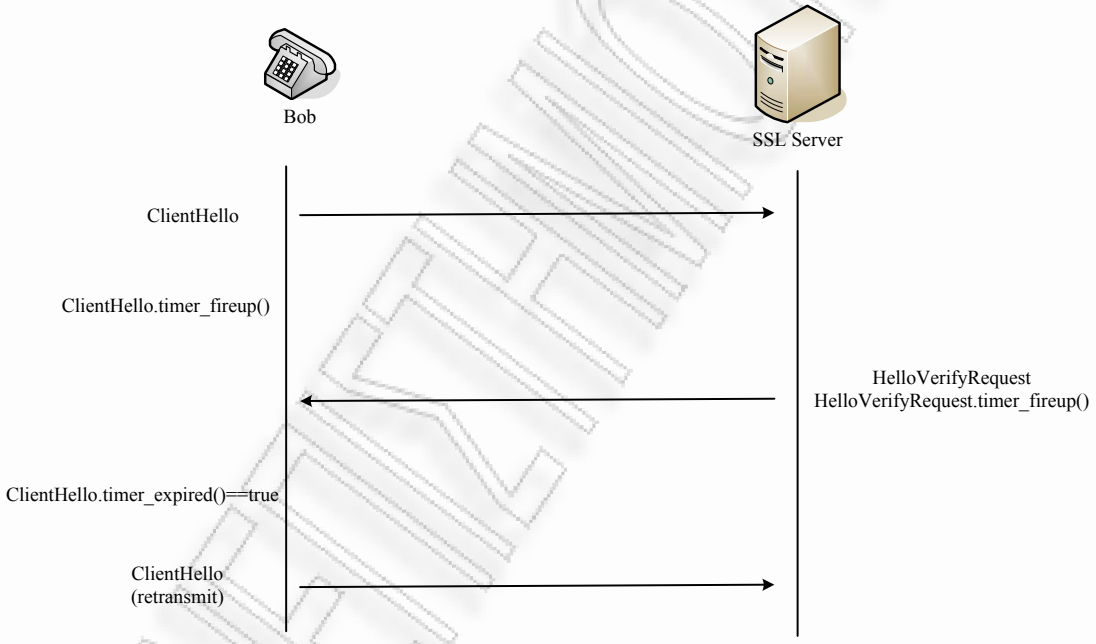
Μια θεμελιώδης διαφορά μεταξύ του TLS και του DTLS είναι ότι το DTLS παρέχει έναν μηχανισμό για να χειριστεί την αναξιοπιστία που συσχετίζεται με το UDP, όπως η πιθανότητα απώλειας πακέτων ή της επαναδιάταξης. Εάν η απώλεια πακέτων συμβεί κατά τη διάρκεια μιας TLS handshake, η σύνδεση αποτυγχάνει. Το TLS Record Layer, όπου πραγματοποιείται η κρυπτογράφηση δεδομένων, απαιτεί τα αρχεία να παραλαμβάνονται και να υποβάλλονται σε επεξεργασία με διαδοχική σειρά. Εάν το αρχείο n δεν παραλαμβάνεται, το αρχείο n + 1 δεν μπορεί να αποκρυπτογραφηθεί επειδή το TLS στρώμα κρυπτογράφησης κυκλοφορίας χρησιμοποιεί το CBC (Cipher Block Chaining), το οποίο απαιτεί τη γνώση του προηγούμενου αρχείου για να αποκρυπτογραφήσει το επόμενο αρχείο στην ακολουθία. Η πιο πρόσφατη έκδοση του TLS, η 1.1, έχει προσθέσει σαφείς CBC οδηγίες στα αρχεία για να αντιμετωπίσει αυτό το ζήτημα.

Ένας άλλος περιορισμός του TLS είναι ότι χρησιμοποιεί μία MAC (Message Authentication Code) για κάθε αρχείο για την προστασία ενάντια στην επανάληψη και στην επαναδιάταξη. Η MAC παράγεται χρησιμοποιώντας τους αριθμούς ακολουθίας των αρχείων που είναι μοναδικοί για κάθε αρχείο. Επομένως, εάν συμβεί απώλεια πακέτων, η ανίχνευση της επανάληψης καθίσταται άχρηστη.

Το DTLS έχει σχεδιαστεί για να υπερνικήσει τους περιορισμούς του TLS με την παροχή των εξής:

- Αξιοπιστία κατά τη διάρκεια της DTLS handshake (απώλεια πακέτων και επαναδιάταξη).
- Ανίχνευση επανάληψης πακέτων.

Για να αντισταθμίσει τις συνθήκες απώλειας πακέτων, το DTLS παρέχει ένα χρονόμετρο αναμετάδοσης. Όταν ένας client διαβιβάζει το ClientHello μήνυμα, αρχίζει το χρονόμετρο και περιμένει ένα HelloVerifyResponse μήνυμα από τον server. Ο server διατηρεί επίσης ένα χρονόμετρο μετάδοσης μηνυμάτων. Εάν το χρονόμετρο του client λήξει, υποθέτει ότι είτε το ClientHello είτε το HelloVerifyResponse χάθηκε και αναμεταδίδει το ClientHello μήνυμα. Η εικόνα 24 απεικονίζει την απώλεια πακέτου και το σενάριο αναμετάδοσης.

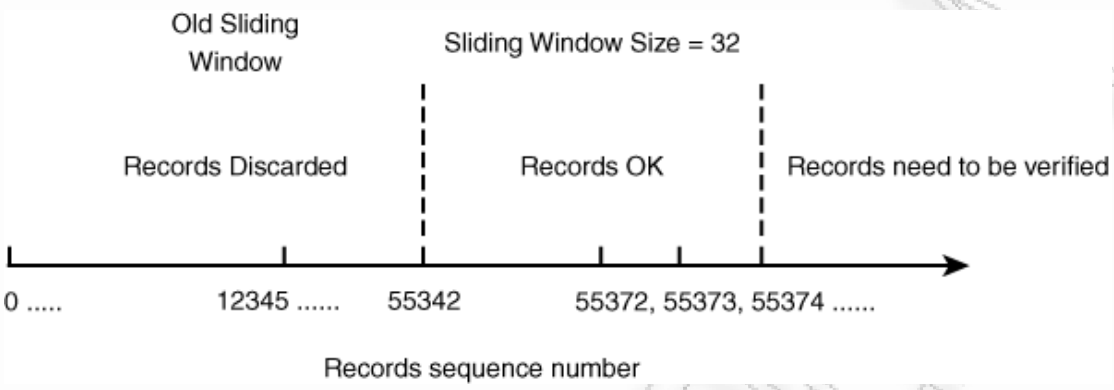


Εικόνα 24: DTLS απώλεια πακέτου και αναμετάδοση.

Από την άλλη μεριά, ο server δεν θα αναμεταδώσει το HelloVerifyResponse μήνυμα πριν από τη λήψη της αναμετάδοσης του ClientHello από τον client.

Για την ανίχνευση της επανάληψης, το πρωτόκολλο DTLS προτείνει την χρησιμοποίηση ενός bitmap παραθύρου από αρχεία τα οποία ο client ή ο server έχει διαβιβάσει, αντίστοιχα. Παραδείγματος χάριν, η χρησιμοποίηση ενός bitmap παραθύρου 32 αρχείων σημαίνει ότι τα τελευταία 32 αρχεία θα υποβληθούν σε

επεξεργασία. Οτιδήποτε πριν από τα 32 αρχεία θα απορριφθεί, και οτιδήποτε μετά θα ελεγχθεί. Η εικόνα 25 βοηθάει στην διευκρίνιση αυτού του μηχανισμού.



Εικόνα 25: Προστασία από τις επιθέσεις επανάληψης αρχείων χρησιμοποιώντας τον μηχανισμό Sliding Window

Ο μετρητής πακέτων του δέκτη αρχικοποιείται στο μηδέν όταν εγκαθίσταται η συνεδρία, και για κάθε λαμβανόμενο αρχείο, ο δέκτης πρέπει να ελέγξει εάν το αρχείο που εξετάζεται αυτήν την στιγμή είναι μέσα στα όρια του παραθύρου. Το δεξί όριο του παραθύρου δείχνει τον υψηλότερο αριθμό ακολουθίας αρχείων που έχει ελεγχθεί μέσα σε μια συνεδρία. Τα αρχεία με αριθμούς ακολουθίας λιγότερους από n + 32 (αριστερό όριο) απορρίπτονται.

Αν και η επιλογή για το μέγεθος του παραθύρου του δέκτη είναι εξαρτώμενη εφαρμογή, το RFC εξουσιοδοτεί την υποστήριξη μιας ελάχιστης τιμής μεγέθους παραθύρου ίσο με 32. Η Sliding Window ιδιότητα είναι προαιρετική για τις εφαρμογές σύμφωνα με το RFC 4347 επειδή ο διπλασιασμός πακέτων δεν είναι πάντα κακόβουλος και μπορεί να εμφανιστεί λόγω λαθών δρομολόγησης.

Μια άλλη ιδιότητα του DTLS είναι η χρήση μιας cookies τεχνικής για την προστασία ενάντια στις DOS επιθέσεις. Κατά τη διάρκεια της αρχικής ανταλλαγής μηνυμάτων (παραδείγματος χάριν, ClientHello και HelloVerifyRequest), ο server περιλαμβάνει ένα cookie στην απάντησή του για να ελέγξει ότι το αίτημα προήλθε από τον μακρινό client και όχι από έναν μιμητή. Ο νόμιμος client θα πρέπει να υπολογίσει ένα άλλο cookie βασισμένο στις πληροφορίες που παραλαμβάνονται από τον server και να

παράγει ένα νέο ClientHello μήνυμα που περιλαμβάνει το cookie του client. Το cookie υπολογίζεται χρησιμοποιώντας την MD5 πάνω σε μία μυστική τιμή, την IP διεύθυνση του πελάτη, και τις παραμέτρους του client που παραλήφθηκαν στο ClientHello μήνυμα. Αυτός ο μηχανισμός βοηθάει στον μετριασμό των επιπτώσεων ενάντια στις DOS επιθέσεις αντανάκλασης όπου ο επιτιθέμενος χρησιμοποιεί τις εξαπατημένες IP διευθύνσεις για να πλημμυρίσει ένα θύμα με απαντήσεις του server.

3.3.1. Δυνατότητες και περιορισμοί του DTLS

Το DTLS πρωτόκολλο βοηθάει στην αντιμετώπιση μερικών ζητημάτων που σχετίζονται με τις εφαρμογές πολυμέσων, την ώρα που παρέχει προστασία στα μηνύματα σηματοδοσίας και media. Η ακόλουθη λίστα δίνει έμφαση στις δυνατότητες και τους περιορισμούς που πρέπει να ληφθούν υπόψη κατά τη διάρκεια μιας εφαρμογής ή μιας αξιολόγησης της αποτελεσματικότητας για την χρήση του DTLS σε ένα συγκεκριμένο περιβάλλον.

- **Δυνατότητες**

  - ✓ Ευκολότερο να εφαρμοστεί σε σύγκριση με τα S/MIME και IPSec.
  - ✓ Κληρονομεί αποδεδειγμένες ιδιότητες ασφάλειας από το TLS.
  - ✓ Παρέχει μηχανισμούς για να αντισταθμίσει τους περιορισμούς του TLS για την αξιοπιστία της handshake και την ανίχνευση επανάληψης.
  - ✓ Η χρήση των cookies προσφέρει προστασία ενάντια στις DOS επιθέσεις.

- **Περιορισμοί**

  - ✓ Απαιτεί την εγκατάσταση μιας νέας crypto συνεδρίας μεταξύ των ενδιάμεσων hops, παρόμοια με το TLS.
  - ✓ Απαιτεί μια PKI υποδομή για να επιβάλει την αμοιβαία αυθεντικοποίηση.

- ✓ Δεν παρέχει άμεση από άκρο σε άκρο εμπιστευτικότητα. Απαιτεί τη λήξη και τη δημιουργία μιας νέας συνεδρίας σε κάθε hop (παραδείγματος χάριν, μεταξύ των SIP proxy ή SBCs).

3.4. S/MIME

Τα Secure/Multipurpose Internet Mail Extensions, που καθορίζονται στο RFC 3851, μπορούν να παρέχουν την από άκρο σε άκρο εμπιστευτικότητα, ακεραιότητα, και επικύρωση για τα πρωτόκολλα εφαρμογής όπως το SMTP και το SIP. Το MIME καθορίζει ένα σύνολο μηχανισμών με σκοπό να κωδικοποιήσει και να αντιπροσωπεύσει τα σύνθετα σχήματα μηνυμάτων όπως τα συνημμένα πολυμέσων (παραδείγματος χάριν, εικόνες ή audio clips) και γλωσσικούς χαρακτήρες (παραδείγματος χάριν, ελληνικά, κινεζικά) μαζί με άλλα πρωτόκολλα όπως το SMTP ή το SIP. Ένα S/MIME μήνυμα είναι βασισμένο πάνω στο MIME, αλλά ενσωματώνει τα PKCS πρότυπα για να επιτύχει τους στόχους ασφάλειάς του (παραδείγματος χάριν, το πρότυπο PKCS#7 Cryptographic Message Syntax, που περιλαμβάνεται στο RFC 3852). Αυτός ο συνδυασμός (MIME και S/MIME) παρέχει ένα μεγάλο επίπεδο ευελιξίας στην υποστήριξη της ανταλλαγής σύνθετων μηνυμάτων μαζί με τη συντήρηση ενός συνόλου στόχων ασφάλειας, συμπεριλαμβανομένης της εμπιστευτικότητας, της ακεραιότητας, και της αυθεντικότητας. Συγχρόνως, η δυνατότητα να παρασχεθεί τέτοια λεπτομερή προστασία προσθέτει στην εφαρμογή ένα μεγάλο επίπεδο πολυπλοκότητας.

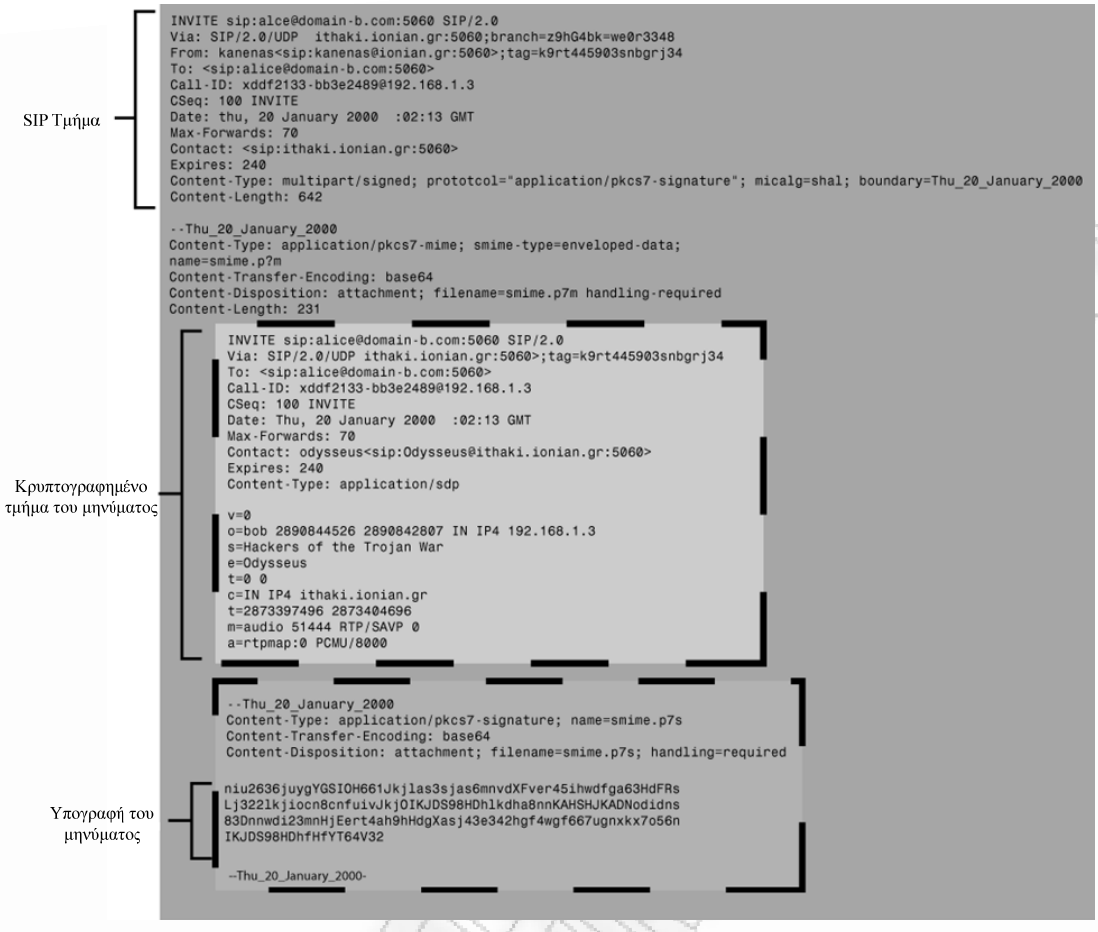
3.4.1. S/MIME και SIP

Το S/MIME μπορεί να χρησιμοποιηθεί για να προστατεύσει τις επιγραφές ενός SIP μηνύματος, εκτός από την VIA επιγραφή, και για να παρέχει την από άκρο σε άκρο εμπιστευτικότητα, ακεραιότητα, και επικύρωση μεταξύ των συμμετεχόντων. Αντίθετα από το TLS και το DTLS, το S/MIME παρέχει ευελιξία για πιο λεπτομερή προστασία των επιγραφών πληροφορίας στα SIP μηνύματα. Όπως αναφέρθηκε στα προηγούμενα τμήματα, το TLS και το DTLS παρέχουν επαρκή προστασία στα SIP μηνύματα, αλλά καλύπτουν ολόκληρο το μήνυμα μέσα στη δομή τους. Το S/MIME επιτρέπει στους χρήστες την επιλεκτική προστασία τμημάτων του SIP μηνύματος. Επιπλέον, μπορεί να χρησιμοποιηθεί με το UDP ή το TCP, το οποίο ξεπερνάει τους περιορισμούς που υφίστανται στα IPSec, TLS, και DTLS, και παρέχει από άκρο σε άκρο προστασία. Η εικόνα 26 απεικονίζει ένα SIP μήνυμα με ένα κρυπτογραφημένο SDP τμήμα χρησιμοποιώντας το S/MIME.

Εικόνα 26: Προστασία του SIP περιεχομένου χρησιμοποιώντας το S/MIME.

Σε αυτό το παράδειγμα, το SIP μήνυμα παραμένει το ίδιο εκτός από το SDP τμήμα, το οποίο κρυπτογραφείται. Αυτό επιτρέπει στους τελικούς χρήστες να προστατεύσουν τις πληροφορίες σχετικά με τη συνεδρία τους, όπως τις UDP πόρτες που χρησιμοποιούνται για την αποστολή και τη λήψη των δεδομένων, τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται για τα media streams (παραδείγματος χάριν, χρησιμοποιώντας SRTP), και τις ιδιότητες σχετικά με το περιεχόμενο της συνεδρίας (παραδείγματος χάριν, θέμα, συμμετέχοντες, URLs σε άλλους πόρους, και ούτω καθεξής).

Μια άλλη προσέγγιση είναι να ενθυλακωθούν τα SIP μηνύματα χρησιμοποιώντας το S/MIME. Αυτό παρέχει ένα πρόσθετο επίπεδο ιδιοαπόρρητου για τον τελικό χρήστη επειδή επιτρέπει το καμουφλάρισμα της ταυτότητας του δημιουργού της συνεδρίας και παρέχει ένα επίπεδο ανωνυμίας. Η εικόνα 27 απεικονίζει αυτήν την προσέγγιση.



Εικόνα 27: Παροχή ακεραιότητας, ανωνυμίας, και εμπιστευτικότητας στα SIP μηνύματα χρησιμοποιώντας το S/MIME.

Το εξωτερικό τμήμα του SIP μηνύματος περιέχει πληροφορίες (παραδείγματος χάριν, From, To, Contact, Via) που μπορούν να χρησιμοποιηθούν από τους μεσάζοντες για να καθοδηγήσουν το μήνυμα στον προορισμό του. Σημειώστε ότι η εξωτερική From επιγραφή περιέχει πληροφορίες που παρέχουν την ανωνυμία του αληθινού αποστολέα του μηνύματος (παραδείγματος χάριν, kanenas@ionian.gr). Αλλά το ενθυλακωμένο SIP μήνυμα περιέχει την αληθινή ταυτότητα του δημιουργού της συνεδρίας (παραδείγματος χάριν, Odysseus@ithaki.ionian.gr). Επιπλέον, η Contact επιγραφή του εξωτερικού τμήματος του SIP μηνύματος περιέχει μόνο την περιοχή του δημιουργού αλλά όχι της ακριβούς θέσης. Η θέση του δημιουργού περιλαμβάνεται στο εσωτερικό SIP μήνυμα, το οποίο κρυπτογραφείται.

Ο παραλήπτης αποκρυπτογραφεί το S/MIME μήνυμα και χρησιμοποιεί την τιμή του εσωτερικού From πεδίου ως δείκτη για να εντοπίσει και να ελέγξει την ταυτότητα του

αποστολέα με την υποβολή ερώτησης σε μία αρχή πιστοποιητικών που διατηρεί το πιστοποιητικό του μακρινού χρήστη μαζί με το δημόσιο κλειδί του αποστολέα.

Και η ακεραιότητα του μηνύματος μπορεί να επικυρωθεί με την επιθεώρηση της συνημμένης υπογραφής. Προφανώς, οι ακριανές συσκευές (παραδείγματος χάριν, τηλέφωνα) για να επεξεργαστούν επιτυχώς τα SIP μηνύματα με S/MIME αντικείμενα, πρέπει να υποστηρίξουν το S/MIME. Δυστυχώς, πολλά VoIP τηλέφωνα δεν υποστηρίζουν το S/MIME, εκτός από μερικές ακαδημαϊκές εφαρμογές που υποστηρίζουν το S/MIME στα soft τηλέφωνα. Επιπλέον, μια PKI υποδομή απαιτείται για την υποστήριξη των S/MIME λειτουργιών που απαιτούν τη χρήση πιστοποιητικών (παραδείγματος χάριν, υπογραφή, επαλήθευση, επικύρωση, και ούτω καθεξής).

Η δυνατότητα της επιλεκτικής προστασίας ενός SIP μηνύματος ξεπερνά το πρόβλημα όπου οι SIP proxy πρέπει να επιθεωρήσουν, ή σε ορισμένες περιπτώσεις να τροποποιήσουν, τις επιγραφές του SIP μηνύματος για να το δρομολογήσουν, δεδομένου ότι χρησιμοποιώντας τα TLS, DTLS, ή IPSec απαιτείται ο τερματισμός της κρυπτογραφημένης συνεδρίας μεταξύ των ενδιάμεσων hop έτσι ώστε οι proxy να εξαγάγουν το περιεχόμενο του κρυπτογραφημένου μηνύματος και να λάβουν αποφάσεις δρομολόγησης. Αυτό επιτρέπει στους τελικούς χρήστες να επιτύχουν την από άκρο σε άκρο εμπιστευτικότητα των μηνυμάτων σηματοδοσίας που ανταλλάσσουν.

Οι SIP εφαρμογές που χρησιμοποιούν το S/MIME πρέπει να υποστηρίζουν τον 3DES για αλγόριθμο κρυπτογράφησης και τον SHA1 ως ψηφιακό αλγόριθμο υπογραφών, στο ελάχιστο. Μια πρόσφατη IETF δημοσίευση, η RFC 3853, αχρηστεύει την χρήση του AES με S/MIME για τις SIP εφαρμογές. Ο AES αλγόριθμος είναι αποδοτικότερος στους κρυπτογραφικούς υπολογισμούς, και έχει σχεδιαστεί για να ελαχιστοποιεί την κατανάλωση των πόρων, κατάσταση ιδανική για τις κινητές συσκευές. Επομένως, προτιμάται η εφαρμογή του AES με ελάχιστη υποστήριξη των 128-bit κλειδιών. Η RFC 3261, στην παράγραφο 23, παρέχει λεπτομέρειες για το πώς να εφαρμοστούν διάφοροι μηχανισμοί προστασίας για το S/MIME στο SIP.

Τα πιστοποιητικά είναι ένας θεμελιώδης φραγμός για το S/MIME για την κατάλληλη υποστήριξη των στόχων ασφάλειας όπως η εμπιστευτικότητα, η ακεραιότητα, και η επικύρωση. Παρόλα αυτά, η επένδυση και οι απαιτήσεις των πόρων που απαιτούνται για την ανάπτυξη μιας PKI υποδομής για την υποστήριξη του S/MIME στην προστασία του VoIP εισάγουν μια προκλητική πρόταση για τους.

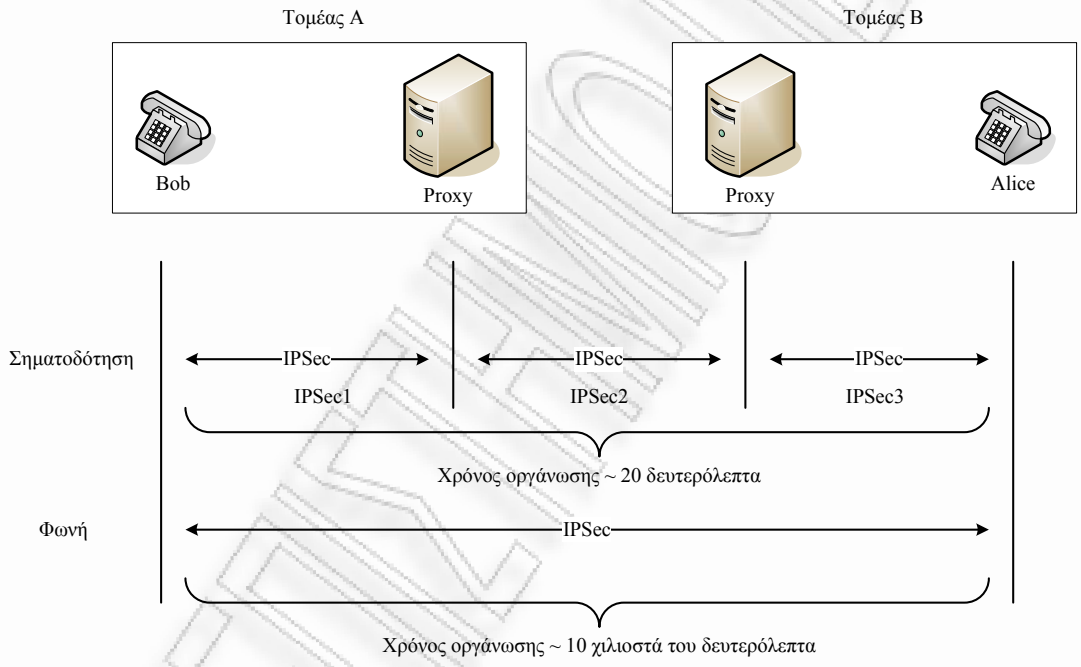
3.4.2. Δυνατότητες και περιορισμοί του S/MIME

Το πρωτόκολλο S/MIME παρέχει προστασία στα μηνύματα σηματοδοσίας σε πιο λεπτομερές επίπεδο από άλλα πρωτόκολλα. Την ίδια στιγμή, η πολυπλοκότητα που απαιτείται για να εφαρμοστεί το S/MIME στην προστασία των μηνυμάτων σηματοδοσίας μπορεί να είναι ένας σημαντικός παράγοντας στον περιορισμό των εφαρμογών του στα περισσότερα περιβάλλοντα. Η ακόλουθη λίστα συνοψίζει τις δυνατότητες και τους περιορισμούς του S/MIME.

- **Δυνατότητες**
  - ✓ Δεν εξαρτάται από το πρωτόκολλο μεταφοράς και μπορεί να χρησιμοποιηθεί είτε με το UDP είτε με το TCP.
  - ✓ Παρέχει μεγάλη ευελιξία λόγω της δυνατότητα προστασίας τμημάτων των SIP μηνυμάτων.
  - ✓ Παρέχει από άκρο σε άκρο εμπιστευτικότητα, ακεραιότητα, και επικύρωση.
- **Περιορισμοί**
  - ✓ Απαιτεί περισσότερη προσπάθεια για να εφαρμοστεί λόγω της πολυπλοκότητας και τις απαιτήσεις υποδομής του (παραδείγματος χάριν, PKI), έναντι άλλων πρωτοκόλλων όπως TLS ή DTLS.
  - ✓ Δεν είναι ευρέως αναπτυσσόμενο.
  - ✓ Η εξέλιξη του είναι αμφισβητήσιμη επειδή απαιτεί μια PKI υποδομή.

3.5. IPSec

Το IPSec είναι ένα αποδεδειγμένο και ευρέως αναπτυγμένο πρωτόκολλο ασφάλειας και παρέχει προστασία στις εφαρμογές που χρησιμοποιούν το UDP ή το TCP ως πρωτόκολλο μεταφοράς. Το IPSec μπορεί να χρησιμοποιηθεί σε tunnel ή στον τρόπο μεταφοράς για να προστατεύσει το ωφέλιμο φορτίο του. Το IPSec μπορεί να παρέχει εμπιστευτικότητα, ακεραιότητα, και επικύρωση για τα μηνύματα της σηματοδοσίας και των media με τη δημιουργία ασφαλών tunnels μεταξύ των τελικών σημείων. Η εικόνα 28 απεικονίζει τη χρήση του IPSec σε ένα SIP περιβάλλον.



Εικόνα 28: Προστασία του SIP χρησιμοποιώντας το IPSec.

Σε αυτό το παράδειγμα, ο Bob προσπαθεί να πραγματοποιήσει μια κλήση στη Alice. Για να προστατεύσει τη SIP σηματοδοσία χρησιμοποιώντας το IPSec, το τηλέφωνο του Bob πρέπει να δημιουργήσει ένα εικονικό IPSec tunnel με τον αντίστοιχο SIP proxy του (περιοχή Α). Όταν το tunnel δημιουργηθεί, ο SIP proxy αναλύει το μήνυμα και το προωθεί στον κατάλληλο προορισμό. Προτού να στείλει το μήνυμα, πρέπει να δημιουργήσει ένα άλλο IPSec tunnel με τον SIP proxy του της Alice (περιοχή Β). Όταν το tunnel δημιουργηθεί, ο SIP proxy της Alice αναλύει το μήνυμα και το προωθεί στο τηλέφωνο της Alice.

Η δημιουργία των τριών ευδιάκριτων IPSec tunnels μπορεί να πάρει κατά μέσο όρο 2.7 δευτερόλεπτα για κάθε IPSec που δημιουργείται (περίπου 5 έως 6 δευτερόλεπτα για ολόκληρο το IPSec tunnel). Μια ερευνητική μελέτη που διεξήχθη από την Telcordia Technologies για λογαριασμό του NIST έδειξε ότι διαρκεί περίπου 20 δευτερόλεπτα μια εγκατάσταση κλήσης (από τον Bob στην Alice και πίσω) όταν χρησιμοποιείται από άκρο σε άκρο το IPSec. Αυτό δεν είναι επιθυμητό επειδή η αποδεκτή από την βιομηχανία παρερχόμενη περίοδος για την εγκατάσταση μίας κλήσης πρέπει να μην ξεπερνά τα 250ms.

Από τη άλλη, το media μονοπάτι (RTP) δημιουργείται άμεσα μεταξύ δύο τελικών σημείων, και διαρκεί κατά μέσο όρο 10 χιλιοστά του δευτερολέπτου, το οποίο είναι αμελητέο. Αυτό δείχνει ότι δεν είναι εφικτό να χρησιμοποιηθεί το IPSec για δυναμικά προσδιορισμένες συνεδρίες επειδή ο χρόνος που παίρνει για τα μηνύματα σηματοδοσίας να διανύσουν τα ενδιάμεσα hop είναι πολύ μεγαλύτερος από το μέσο χρόνο που ένας χρήστης θα ανεχτεί την αναμονή για την εγκατάσταση της κλήσης. Εάν τα IPSec tunnels έχουν ήδη δημιουργηθεί, δεν υπάρχει σχεδόν καθόλου καθυστέρηση για τη δρομολόγηση των μηνυμάτων σηματοδοσίας, το οποίο δείχνει ότι το VoIP χρησιμοποιώντας το IPSec VPNs είναι εφικτό.

Σε μερικές περιπτώσεις, τα IPSec tunnels πρέπει να ξαναδημιουργηθούν εξαιτίας λαθών του δικτύου, αποτυχιών του λογισμικού ή του υλικού, αδράνειας, ή επαναδιαπραγμάτευσης κλειδιών που μπορεί να έχει επίπτωση στις κλήσεις. Γενικά, ωστόσο, το IPSec μπορεί επαρκώς να προστατεύσει την VoIP κυκλοφορία μεταξύ των δικτύων στα οποία τα IPSec tunnels δημιουργούνται εκ των προτέρων. Τυπικά, τα IPSec tunnels μεταξύ των μακρινών περιοχών παραμένουν σταθερά επειδή υπάρχει πάντα κυκλοφορία και τα tunnels δεν λήγουν λόγω αδράνειας. Αυτό δεν ισχύει για τα VoIP τηλέφωνα που μπορεί να χρησιμοποιούν το IPSec για να προστατεύσουν τα μηνύματα σηματοδοσίας και media. Για να λύσουν αυτό, οι εφαρμογές στέλνουν συχνά μηνύματα εγγραφής στον τοπικό τους registrar για να διατηρήσουν το IPSec tunnel.

3.5.1. Δυνατότητες και περιορισμοί του IPSec

Το IPSec είναι αποτελεσματικό στην παροχή της αυθεντικοποίησης και της εμπιστευτικότητας των μηνυμάτων που μεταφέρουν τη σηματοδοσία και τα media. Συγχρόνως, υπάρχουν περιορισμοί που μπορούν να έχουν επίπτωση στην απόδοση της επικοινωνίας των πολυμέσων. Η ακόλουθη λίστα συνοψίζει τις δυνατότητες και τους περιορισμούς του IPSec που πρέπει να ληφθούν υπόψη κατά τη διάρκεια της σχεδίασης ή της υλοποίησης μιας εφαρμογής πολυμέσων:

- **Δυνατότητες**

  - ✓ Αποδεδειγμένο πρωτόκολλο ασφάλειας και ευρέως αναπτυσσόμενο.
  - ✓ Λειτουργεί στο στρώμα δικτύου, έτσι μπορεί να υποστηρίξει τα UDP, TCP, SIP, και RTP.
  - ✓ Παρέχει προστασία συμβολοσειράς ενάντια στις διάφορες επιθέσεις όπως eavesdropping, masquerading, DOS, και άλλες.
  - ✓ Παρέχει εμπιστευτικότητα, ακεραιότητα και επικύρωση.

- **Περιορισμοί**

  - ✓ Απαιτεί περισσότερη προσπάθεια για να εφαρμοστεί λόγω της πολυπλοκότητας και τις απαιτήσεις υποδομής του (παραδείγματος χάριν, PKI), έναντι άλλων πρωτοκόλλων όπως TLS ή DTLS.
  - ✓ Απαιτεί μια PKI υποδομή για να υποστηρίξει την επικύρωση, την ακεραιότητα, και την εμπιστευτικότητα της ακριανής συσκευής.
  - ✓ Τα ενδιάμεσα συστατικά πρέπει να είναι έμπιστα.
  - ✓ Δεν διαβαθμίζεται καλά στα μεγάλα κατανεμημένα δίκτυα και στις κατανεμημένες εφαρμογές (παραδείγματος χάριν, σύσκεψη).

3.6. Μηχανισμοί προστασίας της H.323 οικογένειας

Το H.323 είναι μια σειρά συστάσεων της ITU, από την οποία τα H.225.0, H.245, και H.235.x μας ενδιαφέρουν περισσότερο. Η H.225 σύσταση έχει δύο υποσύνολα, ένα από τα οποία συζητά το RAS (εγγραφή, αποδοχή, και κατάσταση) και άλλες σηματοδοσίες κλήσης. Η σηματοδοσία κλήσης χρησιμοποιείται μεταξύ των H.323 τελικών σημείων για την εγκατάσταση και τον τερματισμό συνδέσεων, και είναι παρόμοια με τη Q.931 σύσταση της ITU. Η RAS σύσταση σηματοδοσίας χρησιμοποιείται από τους gatekeepers για την διαχείριση των τελικών σημείων που βρίσκονται μέσα στη ζώνη τους. Τα τελικά σημεία πρέπει να χρησιμοποιούν το RAS για να εγγραφτούν στον αντίστοιχο τους gatekeeper και να αποκτήσουν πρόσβαση στους πόρους και τις υπηρεσίες δικτύου.

Μια αρχιτεκτονική διαφορά μεταξύ του RAS και της σηματοδοσίας κλήσης είναι ότι το RAS μεταφέρεται μέσω του UDP, ενώ η σηματοδοσία κλήσης μπορεί να υποστηριχθεί μέσω του UDP και του TCP. Επομένως, διαφορετικές επιθέσεις ισχύουν σε κάθε μια με μεταβλητούς βαθμούς επιτυχίας.

Η H.245 προδιαγραφή είναι ένα πρωτόκολλο ελέγχου που χρησιμοποιείται μεταξύ δύο ή περισσότερων τελικών σημείων για να διαχειριστεί τα ρεύματα δεδομένων μεταξύ των συμμετεχόντων στη συνεδρία. Ο κύριος στόχος της είναι να διαπραγματευτεί τις παραμέτρους των δεδομένων μεταξύ των τελικών σημείων, όπως η RTP IP διεύθυνση, πόρτες, codecs (παραδείγματος χάριν, G729, G.711), και ούτω καθεξής. Και τα τρία πρωτόκολλα, το H.225 για τον έλεγχο της κλήσης, το RAS, και το H.245, χρησιμοποιούνται για την δημιουργία, την τροποποίηση, και τον τερματισμό των συνεδριών.

Η H.235 σύσταση συζητά τις υπηρεσίες ασφάλειας όπως η αυθεντικοποίηση και το ιδιοαπόρρητο (κρυπτογράφηση δεδομένων) για τα H.323 συστήματα που χρησιμοποιούν τα H.245 και H.225.0 για την δημιουργία δισημειακής ή πολυσημειακής σύσκεψης. Η πιο πρόσφατη H.235 έκδοση (v4) χωρίζει τις συστάσεις ασφάλειας από το H.235.1 μέχρι το H.235.9 τμήμα. Οι προηγούμενες εκδόσεις

περιέγραφαν τους ελέγχους ασφαλείας ως παραρτήματα από το A μέχρι το F. Ο πίνακας 2 παρέχει μια λίστα με κάθε μια από τις συστάσεις και τον αντίστοιχο στόχο της.

Σύσταση	**Περιγραφή**
H.235.0	Πλαίσιο ασφάλειας για τα συστήματα πολυμέσων της Η σειράς (H.323 και άλλα βασισμένα στο H.245)
H.235.1	Προφίλ βασικής ασφάλειας
H.235.2	Προφίλ ασφάλειας υπογραφής
H.235.3	Υβριδικό προφίλ ασφάλειας
H.235.4	Άμεση και επιλεκτική δρομολογημένη ασφάλεια κλήσης
H.235.5	Προφίλ ασφάλειας για την RAS αυθεντικοποίηση χρησιμοποιώντας αδύναμα κοινά μυστικά
H.235.6	Προφίλ κρυπτογράφησης φωνής με την «εγγενή» H.235/H.245 διαχείριση κλειδιών
H.235.7	Προφίλ ασφάλειας MIKEY + SRTP
H.235.8	Ανταλλαγή κλειδιών για το SRTP σε ασφαλή κανάλια σηματοδοσίας
H.235.9	Πύλη ασφαλείας υποστηρίζοντας το H.323

Πίνακας 2: H.235 Συστάσεις ασφάλειας

Ένα από τα πλεονεκτήματα του H.235 είναι η δυνατότητα ενσωμάτωσης του υλικού κλειδιών για να προστατεύσει τα ρεύματα της σηματοδοσίας και των media κατά την διάρκεια των μηνυμάτων για την εγκατάσταση της κλήσης. Η αμοιβαία αυθεντικοποίηση και η ανταλλαγή κλειδιών συμβαίνουν πριν από την ολοκλήρωση της εγκατάστασης της κλήσης. Μια τυπική H.323 εγκατάσταση χρησιμοποιώντας το H.235 διαρκεί μεταξύ 300 και 400ms ανάλογα με την εφαρμογή (H.323 hard phone ή soft phone). Τα ακόλουθα τμήματα συζητούν κάθε μια από τις απαριθμημένες συστάσεις περαιτέρω.

3.6.1. Η.235.0 Πλαίσιο Ασφάλειας

Το Η.235.0 έγγραφο καθορίζει το αντικείμενο του μέσα στο Η.323 και συζητά τη γενική προσέγγιση για περιοχές όπως οι RAS διαδικασίες σηματοδοσίας για την αυθεντικοποίηση, την ασφάλεια κινητικότητας, την αποκατάσταση λάθους ασφάλειας, και ούτω καθεξής. Κάθε υπο-σύσταση (1 μέχρι 9) θεωρείται ένα Προφίλ του Η.235.0.

Η προστασία της σηματοδοσίας ολοκληρώνεται με τη χρησιμοποίηση του TLS (RFC 2246/3546) ή του IPSec (RFC 2401 χρησιμοποιώντας την ESP μέθοδο). Η χρήση των πρωτοκόλλων ασφάλειας στο στρώμα δικτύου ή μεταφοράς παρέχει τη δυνατότητα να πιστοποιηθούν και να εγκριθούν οι κλήσεις. Η δυνατότητα υλοποίησης του IPSec με το Η.323 ποικίλλει και εξαρτάται από το περιβάλλον και τις απαιτήσεις ασφάλειας. Παραδείγματος χάριν, το IPSec μπορεί να μην είναι η κατάλληλη μέθοδος για να αυθεντικοποιήσει τους συνδρομητές σε ένα περιβάλλον φορέων παροχής VoIP υπηρεσιών όπου εκατομμύρια πιστοποιητικά μπορεί να απαιτηθούν, όπου το TLS μπορεί να ανταποκριθεί καλύτερα. Παράλληλα, ανάλογα με το περιβάλλον, τα Η.235 προφίλ (1 μέχρι 9) μπορούν να εφαρμοστούν όπως απαιτείται. Τα προφίλ διαπραγματεύονται κατά τη διάρκεια της ανταλλαγής των Η.323 μηνυμάτων σηματοδοσίας (παραδείγματος χάριν, το RRQ μήνυμα σε έναν gatekeeper) και συλλαμβάνονται στα προσδιοριστικά αντικειμένου.

Η κατάλληλη αυθεντικοποίηση των χρηστών είναι ένα κρίσιμο συστατικό για την ισχυρή ασφάλεια σε οποιοδήποτε περιβάλλον, και αυτό περιλαμβάνει το VoIP χρησιμοποιώντας το Η.323. Η αυθεντικοποίηση στο Η.235 εκτελείται σε τρεις περιπτώσεις:

- Κατά τη διάρκεια της αρχικής σύνδεσης κλήσης
- Κατά τη διεξαγωγή της ασφάλειας του Η.245 καναλιού ή/και
- Με την ανταλλαγή πιστοποιητικών στο Η.245 κανάλι

Όπως αναφέρεται νωρίτερα, η αυθεντικοποίηση μπορεί να εφαρμοστεί ως τμήμα ενός πρωτοκόλλου ασφάλειας δικτύου ή μεταφοράς, αλλά μπορεί να εφαρμοστεί, επίσης,

από την H.323 εφαρμογή ή υπηρεσία για ένα προστιθέμενο στρώμα προστασίας. Η σύσταση συζητά τις ακόλουθες επιλογές για την αμοιβαία αυθεντικοποίηση της λήψης ή της εγκατάστασης κλήσεων:

- Η αυθεντικοποίηση που στηρίζεται στα πιστοποιητικά είναι βασισμένη στη χρησιμοποίηση ενός μηχανισμού για την ανταλλαγή των πιστοποιητικών προκειμένου να ταυτοποιηθεί ο χρήστης στο δίκτυο (όχι μόνο η συσκευή). Αλλά δεν διευκρινίζει κάποιον μηχανισμό επαλήθευσης, και μάλλον αφήνεται πάνω στον υλοποιητή.

- Κοινή μυστική αυθεντικοποίηση, που μπορεί να πραγματοποιηθεί χρησιμοποιώντας τα H225.0 μηνύματα σηματοδοσίας, όπως διευκρινίζεται στη σύσταση. Η κοινή μυστική αυθεντικοποίηση μπορεί να πραγματοποιηθεί χρησιμοποιώντας την Diffie-Hellman ανταλλαγή κλειδιών για να κρυπτογραφήσει και να ανταλλάξει το κοινό μυστικό.

- Αυθεντικοποίηση πρωτοκόλλου ασφάλειας, χρησιμοποιώντας τις ιδιότητες ενός ξεχωριστού πρωτοκόλλου ασφάλειας όπως το TLS ή το IKE.

Η αυθεντικοποίηση θεωρείται το αρχικό κύριο σημείο στην δημιουργία εμπιστοσύνης μεταξύ των οντοτήτων στα H.323 περιβάλλοντα. Επιπλέον, οποιαδήποτε οντότητα που τερματίζει ένα κρυπτογραφημένο κανάλι ελέγχου ή ένα κρυπτογραφημένο κανάλι δεδομένων θεωρείται στοιχείο αξιόπιστο της αντίστοιχης σύνδεσης.

Ο έλεγχος κλήσης, το H.245, πρέπει επίσης να προστατευθεί χρησιμοποιώντας έναν από τους συζητημένους αλγορίθμους κρυπτογράφησης για την προστασία των πληροφοριών της συνεδρίας. Οι πληροφορίες της συνεδρίας που συλλαμβάνονται στο H.245 κανάλι ελέγχου μπορεί να περιλαμβάνουν αλγορίθμους κρυπτογράφησης και κλειδιά που χρησιμοποιούνται για την προστασία των media streams. Η αρχική διαπραγμάτευση των κρυπτογραφικών αλγορίθμων και της διανομής του υλικού των κλειδιών εκτελείται μέσω του H.245 χρησιμοποιώντας τα OpenLogicalChannel ή OpenLogicalChannelAck μηνύματα. Επιπλέον, η επανάληψη των κλειδιών μπορεί να ολοκληρωθεί από τις ακόλουθες H.245 εντολές:

- Η EncryptionUpdateCommand που χρησιμοποιείται από τον master για να διανείμει το υλικό κλειδιών της συνεδρίας.
- Η EncryptionUpdateRequest που χρησιμοποιείται από το slave για να ζητήσει ένα νέο κλειδί συνεδρίας από τον master.
- Η EncryptionUpdate που χρησιμοποιείται από τον master για να διανείμει ένα νέο κλειδί συνεδρίας.
- Η EncryptionUpdateAck που είναι η απάντηση του slave για την βεβαίωση λήξης ενός νέου κλειδιού.

Η διανομή του υλικού κλειδιών προστατεύεται με τον χειρισμό του H.245 καναλιού ως ιδιωτικό κανάλι (στη ζώνη ή έξω από τη ζώνη) ή με την προστασία του υλικού κλειδιών χρησιμοποιώντας πιστοποιητικά.

3.6.2. Η.235.1 Προφίλ βασικής ασφάλειας

Η σύσταση του προφίλ της βασικής ασφάλειας παρέχει υποστήριξη για την αυθεντικοποίηση των μηνυμάτων και την ακεραιότητα των H.245, H.225.0 RAS, και μηνυμάτων σηματοδοσίας κλήσης. Η ακεραιότητα για την H.225 σηματοδοσία κλήσης και τα RAS μηνύματα ρυθμίζεται με τον κατατεμαχισμό όλων των πεδίων του μηνύματος. Η σύσταση παρέχει επίσης την επιλογή να εφαρμοστεί η αυθεντικοποίηση χωρίς την ακεραιότητα. Αυτό είναι χρήσιμο σε περιπτώσεις όπου μηνύματα σηματοδοσίας διαβαίνουν μια NAT (Network Address Translation) συσκευή που προκαλεί το χάσιμο της ισχύος του αρχικού μηνύματος (επειδή η NAT συσκευή αλλάζει τις ιδιότητές του). Η πρόκληση-αυθεντικοποίησης εφαρμόζεται χρησιμοποιώντας ένα HMAC-SHA1-96 για να παράγει έναν 20-byte τεμαχισμένο κωδικό πρόσβασης. Η αυθεντικοποίηση μεταξύ του τελικού σημείου και του gatekeeper του είναι βασισμένη σε ένα ευδιάκριτο κλειδί, το οποίο μπορεί να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για να προστατεύσει τη σηματοδοσία κλήσης. Σε μερικές περιπτώσεις, απαιτείται να υπάρχουν δύο ευδιάκριτα κλειδιά που να χρησιμοποιούνται για να προστατεύσουν τα RAS μηνύματα και τα μηνύματα σηματοδοσίας κλήσης. Υπάρχουν τρεις τρόποι που συζητούνται στη σύσταση στα

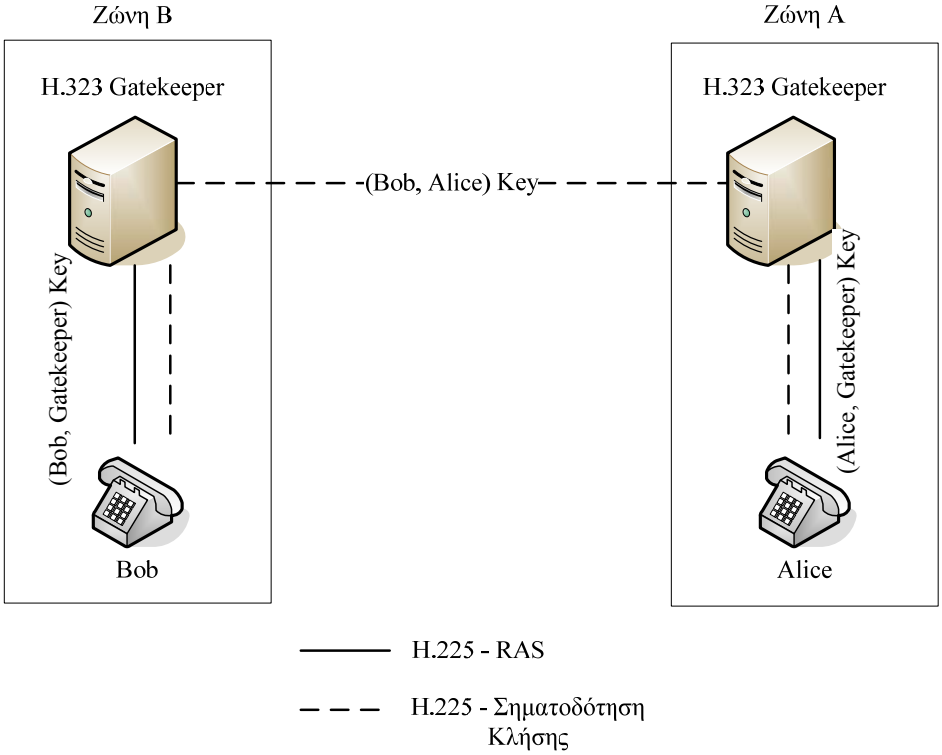
οποία η αυθεντικοποίηση των H.225 μηνυμάτων σηματοδοσίας κλήσης μπορεί να πραγματοποιηθεί:

- Gatekeeper routed – το κλειδί της αυθεντικοποίησης που θα χρησιμοποιηθεί από τα τελικά σημεία για να πιστοποιήσουν τα μηνύματα διασχίζει τους αντίστοιχους gatekeepers τους.

- Direct – το κλειδί της αυθεντικοποίησης που θα χρησιμοποιηθεί από τα τελικά σημεία για να πιστοποιήσουν τα μηνύματα μεταβιβάζεται άμεσα μεταξύ των τελικών σημείων.

- Mixed – και τα δύο τελικά σημεία δρομολογούν το κλειδί μέσω ενός αντίστοιχου gatekeeper.

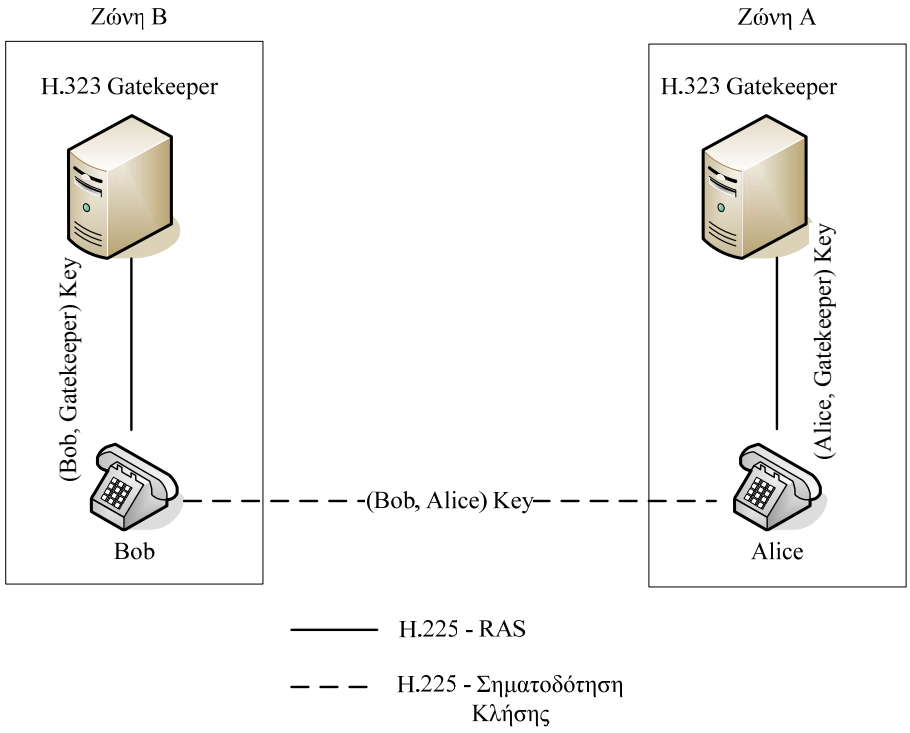
Η εικόνα 29 παρέχει ένα παράδειγμα στο οποίο το κλειδί αυθεντικοποίησης ανταλλάσσεται μέσω των αντίστοιχων gatekeepers.



Εικόνα 29: Κλειδί αυθεντικοποίησης δρομολογημένο από τους Gatekeeper

Η αρχική σχέση εμπιστοσύνης μεταξύ του τελικού σημείου (το τηλέφωνο του Bob) και του gatekeeper εδραιώνεται χρησιμοποιώντας την αυθεντικοποίηση μέσω του H.225 RAS. Όταν αυτή η εμπιστοσύνη εδραιωθεί, το τελικό σημείο μεταβιβάζει το κλειδί αυθεντικοποίησης στην Alice μέσω των ενδιάμεσων gatekeepers (για τη ζώνες A και B). Αυτό το σενάριο εισάγει ευκαιρίες για επίθεση, ειδικά εάν τα μηνύματα σηματοδοσίας διασχίζουν άλλους gatekeepers ή δίκτυα για τα οποία η ασφάλεια είναι αμφισβητήσιμη. Για την αντιμετώπιση αυτής της αδυναμίας, συστήνεται η χρήση ενός πρωτοκόλλου ασφάλειας όπως το TLS ή το IPSec μεταξύ των ενδιάμεσων hop.

Η εικόνα 30 παρέχει ένα παράδειγμα στο οποίο το κλειδί αυθεντικοποίησης ανταλλάσσεται άμεσα μεταξύ των τελικών σημείων.

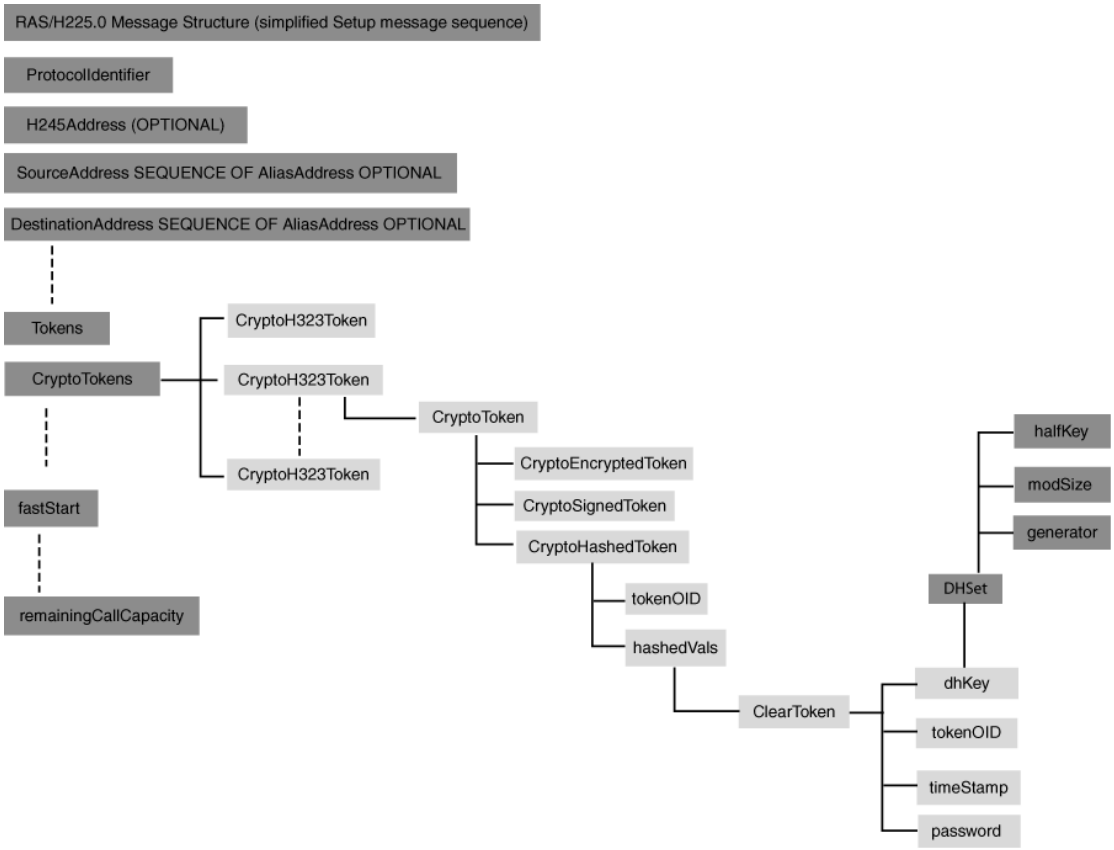


Εικόνα 30: Άμεσα δρομολογημένο κλειδί αυθεντικοποίησης.

Αρχικά, ο Bob και η Alice εγγράφονται στους αντίστοιχους gatekeepers τους χρησιμοποιώντας το RAS και ένα ευδιάκριτο κλειδί για να πιστοποιήσουν τα RAS μηνύματα. Όταν ο Bob αποφασίζει να πραγματοποιήσει μια κλήση στην Alice, η H.323 συσκευή του Bob θα χρησιμοποιήσει τη H.225 σηματοδοσία κλήσης (Setup μήνυμα), στην οποία θα περιλάβει μια halfkey τιμή που παράγεται χρησιμοποιώντας τον Diffie-Hellman. Το halfkey είναι μέρος του dhkey πεδίου της ClearToken

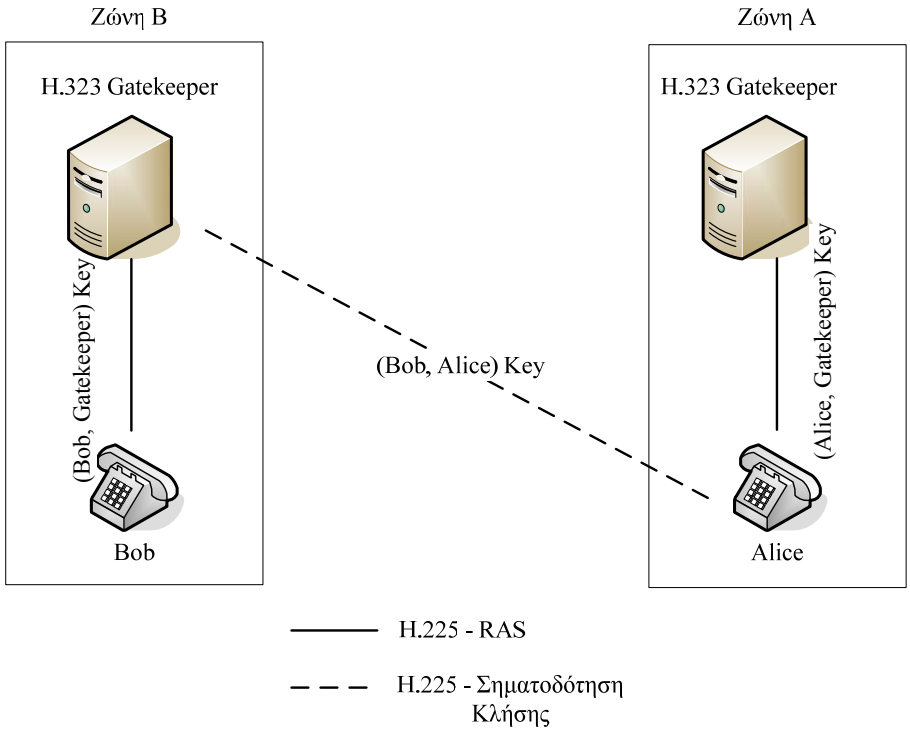
επιγραφής. Τα H.225 (RAS και σηματοδοσία κλήσης) μηνύματα συλλαμβάνουν τα πιστοποιητικά αυθεντικοποίησης και κρυπτογράφησης μέσα σε μια γενικότερη δομή που ονομάζεται cryptoTokens.

Η εικόνα 31 απεικονίζει το σχήμα ενός H.225 Setup μηνύματος που χρησιμοποιεί την αυθεντικοποίηση.



Εικόνα 31: Απλουστευμένο H.225.0 Setup μήνυμα με αυθεντικοποίηση

Η εικόνα 32 παρέχει ένα παράδειγμα στο οποίο το κλειδί αυθεντικοποίησης ανταλλάσσεται μέσω ενός από τους δύο gatekeepers (μικτό σενάριο).



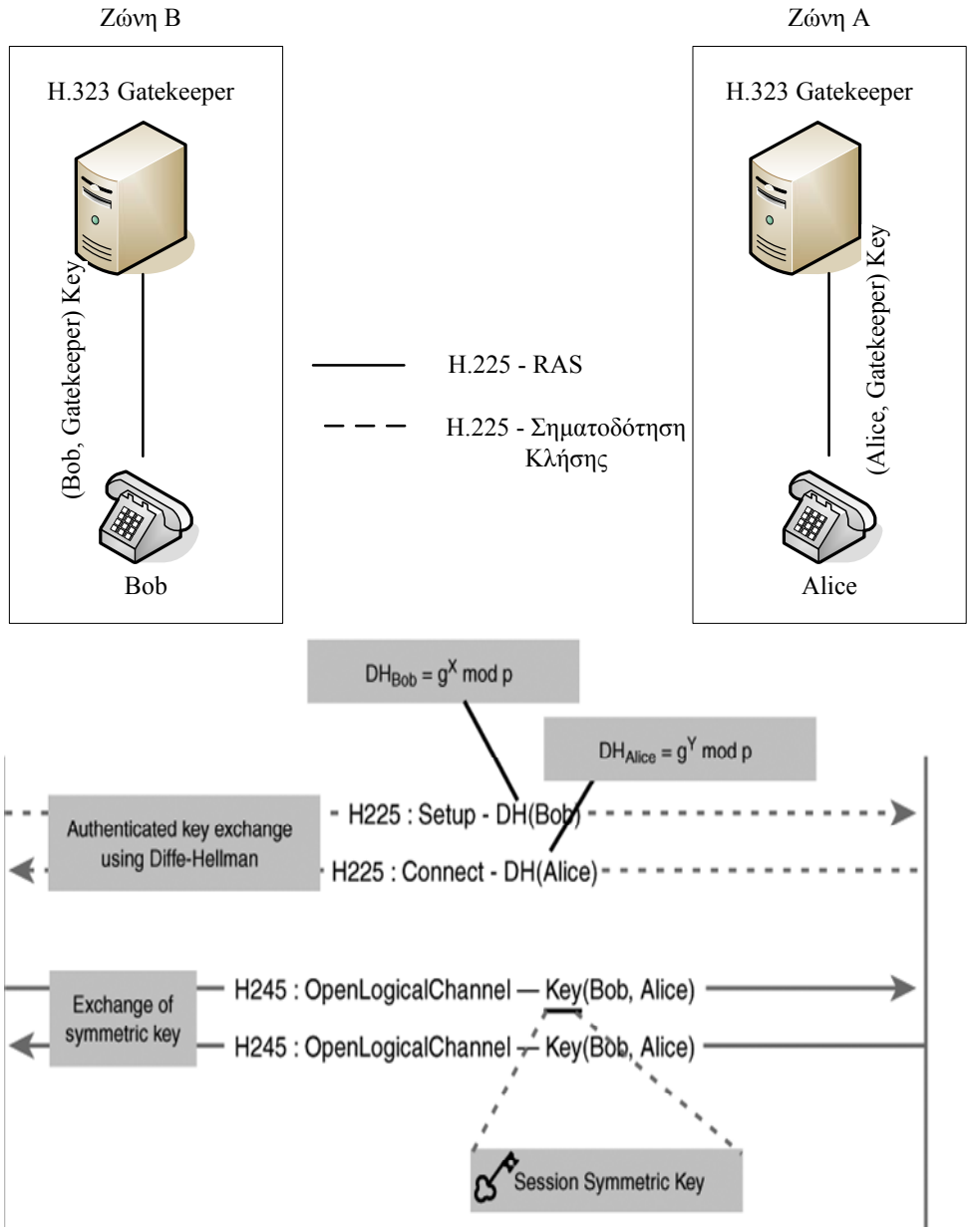
Εικόνα 32: Η.235 μικτός τρόπος αυθεντικοποίησης.

Η Η.235.1 σύσταση παρέχει πρόσθετες λεπτομέρειες για το πώς ορίζονται τα πεδία στα Η.225 μηνύματα. Επιπλέον, το Η.235.1 προφίλ μπορεί να χρησιμοποιηθεί από κοινού με τα προφίλ 2 μέχρι 7 για την παροχή πρόσθετης προστασίας των Η.225 και Η.245 μηνυμάτων.

3.6.3. Η.235.2 Προφίλ ασφάλειας υπογραφής

Η Η.235.2 σύσταση είναι ένα προαιρετικό προφίλ που εφαρμόζει τις ψηφιακές υπογραφές για τα Η.225.0 μηνύματα σηματοδοσίας χρησιμοποιώντας τους SHA1 ή MD5 ως hashing αλγόριθμους. Αυτή η σύσταση παρέχει καλύτερη δυνατότητα εξέλιξης και διαχείρισης σε σύγκριση με την Η.235.1 επειδή μπορεί να χρησιμοποιηθεί ασύμμετρη αυθεντικοποίηση για περιβάλλοντα με πολλά τερματικά (παραδείγματος χάριν, μεγάλο δίκτυο επιχειρήσεων). Εκτός από την ακεραιότητα και την αυθεντικοποίηση, η μη απόρριψη μπορεί να υποστηριχθεί επειδή η χρήση των πιστοποιητικών είναι εφικτή. Συγχρόνως, αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί για την ανταλλαγή ενός κοινού μυστικού κλειδιού ώστε να

χρησιμοποιηθεί στην κρυπτογράφηση της RTP κυκλοφορίας (φωνή ή βίντεο). Η εικόνα 33 απεικονίζει αυτήν την μέθοδο.



Εικόνα 33: H.235 ανταλλαγή κοινού μυστικού χρησιμοποιώντας τον Diffie-Hellman.

Αυτό το παράδειγμα απεικονίζει την ανταλλαγή ενός κοινού μυστικού μέσω του H.245. Όταν το κλειδί έχει ανταλλαχθεί, μπορεί να χρησιμοποιηθεί με το SRTP (Secure Real Time Protocol) για να κρυπτογραφήσει τα media streams.

Η σύσταση διευκρινίζει τις διαδικασίες για τα εξής:

- Ψηφιακές υπογραφές χρησιμοποιώντας δημόσια/ιδιωτικά ζευγάρια κλειδιών
- Πολυσημειακή σύσκεψη
- Από άκρο σε άκρο αυθεντικοποίηση
- Μόνο αυθεντικοποίηση
- Χειρισμός των πιστοποιητικών

Αυτές οι διαδικασίες μπορούν να χρησιμοποιηθούν για να προστατεύσουν τα H.225 (RAS και πληροφορίες σηματοδοσίας κλήσης) και H.245 μηνύματα.

3.6.4. H.235.3 Υβριδικό προφίλ ασφάλειας

Το υβριδικό προφίλ ασφάλειας χρησιμοποιεί έναν συνδυασμό συστάσεων από τα H.235.1 και H.235.2 με σκοπό την δημιουργία ενός εξελικτικού προφίλ βασισμένου στα PKI πιστοποιητικά. Συνδυάζει τις δυνατότητες και από τα δύο προφίλ για να υποστηρίξει μια μεγάλη VoIP ανάπτυξη σε βαθμό επιχειρήσεων.

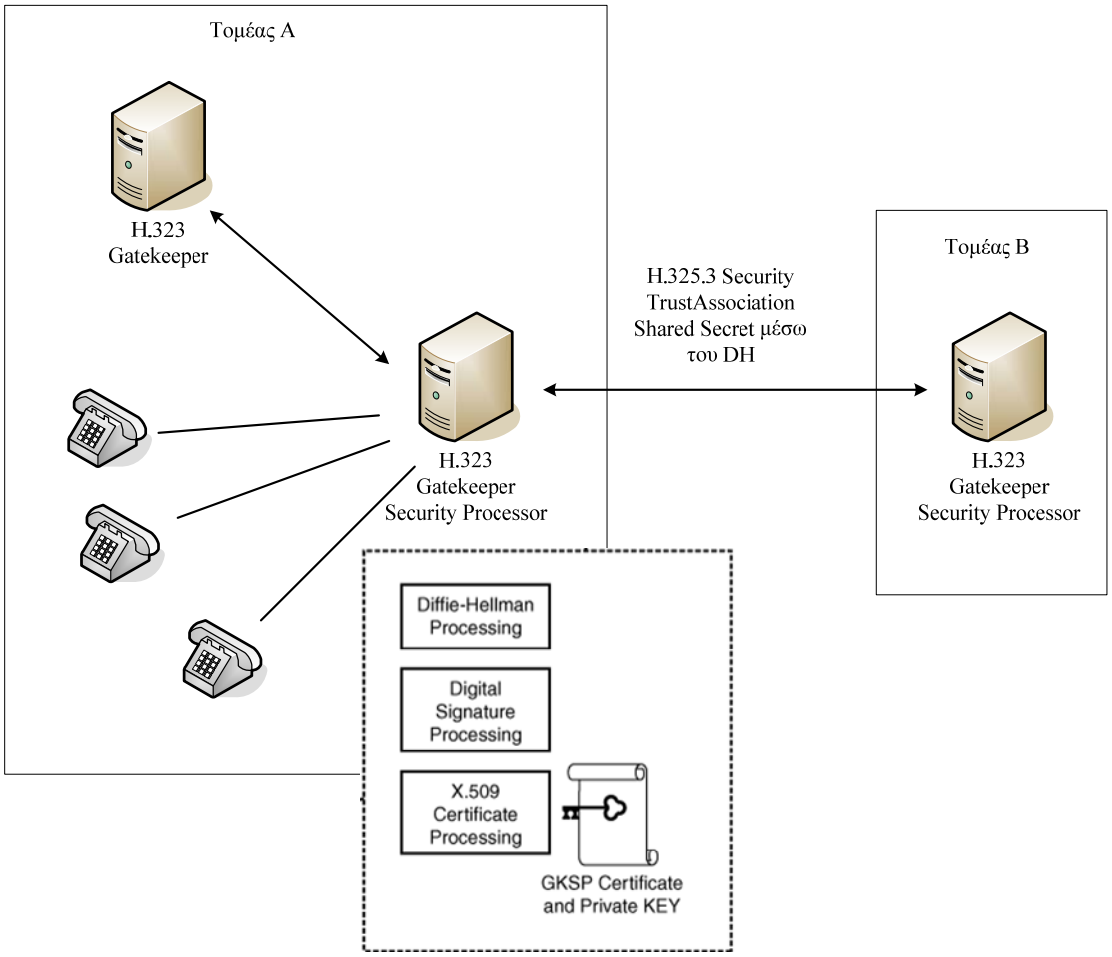
Αυτό το προφίλ εξουσιοδοτεί τη χρήση ενός GK-routed προτύπου, όπου όλα τα μηνύματα δρομολογούνται μέσω του τοπικού gatekeeper αντί να διαβιβαστούν άμεσα στα τελικά σημεία. Για να προσαρμοστούν η κινητικότητα του χρήστη και οι χρονικές εξαρτώμενες εφαρμογές, χρησιμοποιείται η μέθοδος της γρήγορης σύνδεσης σηματοδοσίας κλήσης. Επιπλέον, υποστηρίζει την σύναξη των H.245 μηνυμάτων ελέγχου κλήσης μαζί με τα H.225.0 μηνύματα σηματοδοσίας κλήσης, το οποίο παρέχει έμφυτη ασφάλεια.

Οι διαδικασίες που περιγράφονται στο H.235.3 περιλαμβάνουν τα εξής:

- Ασφάλεια Hop-by-hop (συνδυάζοντας την πρόταση 7 του H.235.1 και τη διαδικασία II της πρότασης 7 του H.235.2).
- Η σχέση ασφάλειας για ταυτόχρονες κλήσεις που εγκαθίστανται μεταξύ δύο οντοτήτων (παραδείγματος χάριν, σύσκεψη) υποστηρίζει τη χρήση ενός ενιαίου κλειδιού για να χειριστεί την κρυπτογράφηση όλων των ρευμάτων αντί χωριστών κλειδιών.

- Ενημέρωση κλειδιών για να υποστηρίξει την ανανέωση των κλειδιών.

Αν και αυτό το προφίλ παρέχει διαδικασίες για διαβάθμιση σε μεγάλη VoIP εφαρμογή, επιβάλλει γενικά έξοδα επεξεργασίας μέσω της χρήσης των κρυπτογραφικών λειτουργιών στο gatekeeper. Για την ανακούφιση μερικών από τα φορτία επεξεργασίας, ένας ξεχωριστός Gate Keeper Security Processor (GKSP) καθορίζεται. Η εικόνα 34 απεικονίζει αυτό το συστατικό.



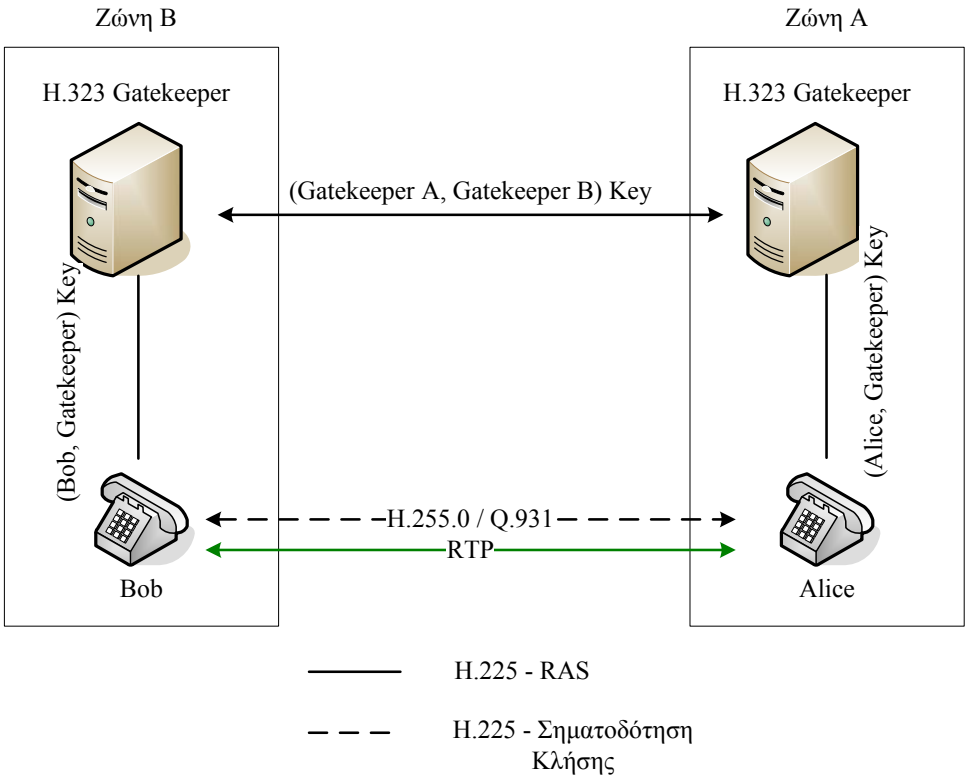
Εικόνα 34: H.323/235 Gate Keeper Security Processor.

Αυτή η εικόνα απεικονίζει έναν gatekeeper για την περιοχή Α, όπου όλες οι κρυπτογραφικές λειτουργίες ασφάλειας, όπως οι Diffie-Hellman διαδικασίες, οι ψηφιακοί υπολογισμοί, οι επαληθεύσεις υπογραφών και η X.509 επεξεργασία πιστοποιητικών εκτελούνται από τον GKSP. Ο gatekeeper ανατίθεται με την επεξεργασία των H.225 (RAS και σηματοδοσία κλήσης) και H.245 μηνυμάτων. Αυτή η προσέγγιση είναι μόνο μια σύσταση και δεν έχει εξεταστεί λεπτομερώς από την

ITU από την άποψη των ροών μηνυμάτων και των αποδεκτών παραλλαγών των σχέσεων εμπιστοσύνης που απαιτούνται μεταξύ των gatekeepers και των Gate Keeper Security Processors.

3.6.5. H.235.4 Άμεση και επιλεκτική δρομολογημένη ασφάλεια κλήσης

Το κατευθυνόμενο και επιλεγμένο προφίλ ασφάλειας δρομολόγησης κλήσης προσπαθεί στην παροχή μιας εύκαμπτης εναλλακτικής λύσης στο gatekeeper routed πρότυπο για την βελτίωση της απόδοσης και την δυνατότητα εξέλιξης κατά τον χειρισμό των πολλαπλών παράλληλων καναλιών. Η εικόνα 35 απεικονίζει αυτήν την διαμόρφωση.



Εικόνα 35: Κατευθυνόμενη και επιλεγμένη τοπολογία ασφάλειας δρομολόγησης κλήσης.

Αυτή η διαμόρφωση υποθέτει ότι τα τελικά σημεία επικοινωνούν μέσω ενός επισφαλές δικτύου. Κάθε ένα από τα τελικά σημεία έχει εδραιώσει μια σχέση εμπιστοσύνης με τον αντίστοιχο gatekeeper του χρησιμοποιώντας τη RAS σηματοδοσία, και μερικές φορές οι δύο gatekeepers έχουν επίσης εδραιώσει μια

σχέση εμπιστοσύνης μεταξύ τους χρησιμοποιώντας τη RAS σηματοδοσία. Αυτή η σχέση επιτρέπει στα δύο τελικά σημεία να διαπραγματευτούν ένα κοινό κλειδί μέσω του επισφαλές δικτύου για να προστατεύσουν τα μηνύματα σηματοδοσίας κλήσης και τα media streams. Αυτό είναι ιδανικό για τα περιβάλλοντα στα οποία η άμεση εγκατάσταση κλήσης απαιτείται μεταξύ των τελικών σημείων και ο gatekeeper επικεντρώνεται στη διαχείριση της εγγραφής, της αποδοχής, της ανάλυσης διεύθυνσης, και του ελέγχου εύρους ζώνης. Η σύσταση παρέχει τις ακόλουθες διαδικασίες για την δρομολόγηση επιλεγμένης κλήσης:

- Corporate environment (DRC1)
- Interdomain environment I (DRC2)
- Interdomain environment II (DRC3)

Επιπλέον, η σύσταση παρέχει τις ακόλουθες διαδικασίες παραγωγής κλειδιών:

- PRF-based key-derivation procedure
- FIPS 140-based key-derivation procedure

Και οι δύο διαδικασίες καθορίζουν πώς να αντλήσουν το υλικό κλειδιού από το κοινό μυστικό και άλλες παραμέτρους στα κατευθυνόμενα και επιλεγμένα σενάρια δρομολόγησης κλήσης.

3.6.6. Η.235.5 Προφίλ για την ασφάλεια της RAS αυθεντικοποίησης χρησιμοποιώντας αδύναμα κοινά μυστικά

Σε ορισμένες εφαρμογές, οι ιδιότητες του κοινού μυστικού (παραδείγματος χάριν, παραδοσιακός στατικός κωδικός πρόσβασης), που χρησιμοποιείται για να εδραιώσει μια σχέση εμπιστοσύνης μεταξύ δύο οντοτήτων (παραδείγματος χάριν, τελικό σημείο και gatekeeper), δεν είναι επαρκείς για να αντισταθούν στις επιθέσεις που χρησιμοποιούν την εξαντλητική αναζήτηση (brute force).

Η Η.235.5 σύσταση εισάγει ένα πλαίσιο στο οποίο ένα τελικό σημείο και ο gatekeeper του, ή μεταξύ δύο gatekeeper, μπορούν να χρησιμοποιήσουν τα αρχικά

RAS μηνύματα για να διαπραγματευτούν ένα σύνολο ισχυρών κοινών μυστικών μεταξύ τους, και να χρησιμοποιήσουν αυτά τα μυστικά για να κρυπτογραφήσουν και να πιστοποιήσουν τα επιλεγμένα μέρη του επόμενου RAS και των μηνυμάτων σηματοδοσίας κλήσης. Αυτή η μέθοδος ισχύει μόνο για την gatekeeper-routed σηματοδοσία, όχι για την άμεση δρομολόγηση σηματοδοσίας.

Δύο προφίλ συζητούνται μέσα στο πλαίσιο:

- Specific security profile (SP1), το όποιο χρησιμοποιείται για να κατασκευάσει ένα κοινό μυστικό ισοδύναμο με έναν 80-bit τυχαίο αριθμό (δείτε επίσης NIST SP 800-57)
- Improved Security Profile (SP2), το όποιο είναι βασισμένο στο SP1, αλλά μεταξύ άλλων συστάσεων παρέχει βελτιώσεις για την προστασία από τις replay και λεξικού επιθέσεις

Το SP2 εισάγει τη χρήση των αριθμών ακολουθίας της σηματοδοσίας κλήσης για προστασία από τις replay και reflection. Αν και αυτός ο μηχανισμός δεν μετριάζει αυτό το ζήτημα εντελώς, ελαχιστοποιεί την πιθανότητα για μια επιτυχή επίθεση. Η προστασία ενάντια στις dictionary επιθέσεις επιτυγχάνεται με την παραγωγή ενός νέου κλειδιού που χρησιμοποιεί τον αρχικό κωδικό πρόσβασης και το τελικό pointID χρησιμοποιώντας τα εξής:

K = Trunc(SHA1(user_password || end pointID), 16)

Όπου η Trunc (SHA1,16) αποκόπτει την προκύπτουσα συμβολοσειρά από την SHA1 σε 16 octets.

Η σύσταση συζητά πρόσθετες επεκτάσεις για την παροχή πρόσθετης ασφάλειας στην εδραίωση των σχέσεων εμπιστοσύνης και στη διατήρηση της εμπιστευτικότητας των μηνυμάτων σηματοδοσίας, όπως η χρησιμοποίηση ενός κύριου κλειδιού για την ασφάλεια του καναλιού σηματοδοσίας κλήσης πάνω από το TLS και τη χρήση των πιστοποιητικών για την αυθεντικοποίηση του gatekeeper.

3.6.7. H.235.6 Προφίλ κρυπτογράφησης φωνής με την «εγγενή» H.235/H.245 διαχείριση κλειδιών

Το προφίλ κρυπτογράφησης φωνής χρησιμοποιείται από κοινού με το H.235.1 προφίλ βασικής ασφάλειας για την παροχή της εμπιστευτικότητας των media streams. Το προφίλ κρυπτογράφησης ανταλλάσσεται μεταξύ των τελικών σημείων ως τμήμα της τελικής διαπραγμάτευσης των δυνατοτήτων ασφάλειας. Μπορεί να κάνει χρήση διαφόρων αλγορίθμων κρυπτογράφησης, συμπεριλαμβανομένων των AES, RC2, DES, ή 3DES χρησιμοποιώντας την OFB μέθοδο (Output Feed Back μέθοδος, ISO/IEC 10116). Η διαπραγμάτευση των αλγορίθμων κρυπτογράφησης εκτελείται μέσω του H.245, όπου κάθε αλγόριθμος κρυπτογράφησης μπορεί να εφαρμοστεί σε έναν συγκεκριμένο codec και μαζί να διαμορφώσουν μια ευδιάκριτη ικανότητα για το τελικό σημείο. Αυτή η λεπτομέρεια επιτρέπει στα τελικά σημεία να διαβαθμίσουν τις επικοινωνίες τους σε μεγάλα κατανεμημένα περιβάλλοντα με άλλα τελικά σημεία όπως απαιτείται.

Ένα άλλο αρχιτεκτονικό συστατικό της σύστασης είναι η δημιουργία ενός ρόλου master στον οποίο ένα τελικό σημείο είναι αρμόδιο για την παραγωγή και τη διάδοση των κλειδιών κρυπτογράφησης. Αυτό ισχύει ιδιαίτερα σε έναν πολλαπλής διανομής ελεγκτή για το χειρισμό των πολλαπλών καναλιών.

Για να υποστηρίξει τις κινητές και τις ευαίσθητες στην καθυστέρηση εφαρμογές (παραδείγματος χάριν, βίντεο, παιχνίδι, και φωνή), εισάγεται η χρήση της ασφάλειας γρήγορης σύνδεσης. Αυτή είναι η ίδια με την H.323 μέθοδο γρήγορης-σύνδεσης αλλά χρησιμοποιεί τους μηχανισμούς ασφάλειας που συζητούνται σε αυτό το πρότυπο για να προστατεύσει τη σηματοδοσία και συνεπώς τα μηνύματα μέσων. Η σύσταση συζητά επίσης την DTMF κρυπτογράφηση (Dual Tone Multi Frequency). Σημειώστε ότι οι DTMF τόνοι στο H.323 μπορούν να μεταφερθούν μέσα στα μηνύματα σηματοδοσίας ή το RTP, ενώ στις SIP ή στις MGCP εφαρμογές, οι DTMF τόνοι μεταφέρονται μέσα στο RTP. Στις H.323 εφαρμογές, όπου οι DTMF τόνοι μεταφέρονται μέσα στο RTP (με τον καθορισμό του rtpPayloadIndication), συνιστάται ότι το RTP ωφέλιμο φορτίο επίσης να κρυπτογραφείται επειδή είναι

τετριμμένο να αποκωδικοποιηθούν οι DTMF τόνοι από την μη κρυπτογραφημένη RTP κυκλοφορία.

Για την ανταλλαγή των κλειδιών μεταξύ των H.323 οντοτήτων, αυτή η σύσταση παρέχει δύο βασικούς μηχανισμούς μεταφορών:

- Απλή μεταφορά κλειδιών για την υποστήριξη των τελικών σημείων με μια προηγούμενη έκδοση H.323 (έκδοση 1 και έκδοση 2) χρησιμοποιώντας το KeySyncMaterial πεδίο.

- Βελτιωμένη μεταφορά κλειδιών για την αντιμετώπιση των αδυναμίων που βρίσκονται στην απλή μέθοδο μεταφοράς κλειδιών στην οποία η σύνταξη του KeySyncMaterial πεδίου και η εφαρμογή της ENCRYPTED λειτουργίας παρέχουν επαρκείς πληροφορίες (παραδείγματος χάριν, το generalID του αφέντη) για την επιτυχή πραγματοποίηση μιας brute-force επίθεσης.

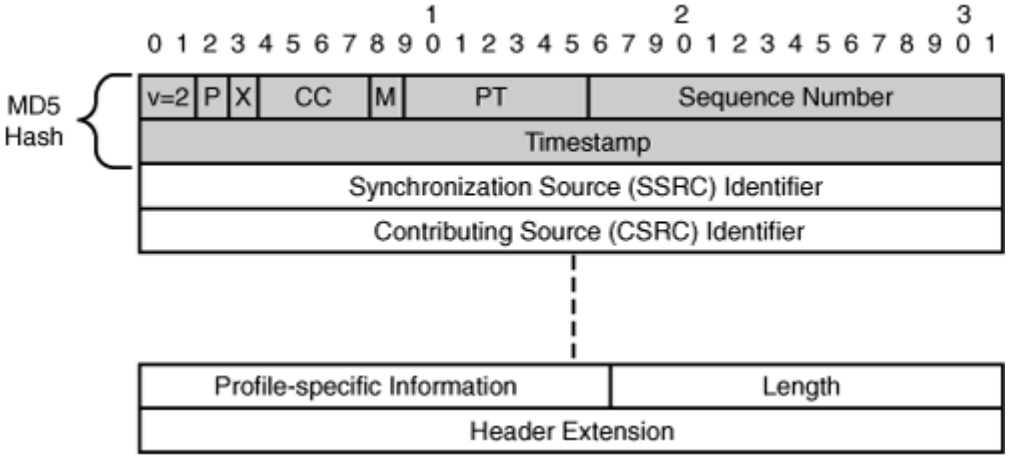
Η μέθοδος της γρήγορης-έναρξης χρησιμοποιείται για την διαπραγμάτευση των δυνατοτήτων ασφάλειας μεταξύ των τελικών σημείων και την εγκατάσταση ένος κοινού μυστικού (Diffie -Hellman) στην έναρξη σύνδεσης. Αυτό το Diffie -Hellman κλειδί χρησιμοποιείται έπειτα ως κύριο κλειδί για την ασφαλή διανομή ενός ασφαλούς κλειδιού για την κρυπτογράφηση των media συνεδριών (RTP).

Η VoIP σύσκεψη είναι μια ουσιαστική εφαρμογή, και η προστασία της μπορεί να είναι προκλητική επειδή απαιτεί τον συντονισμό των δυνατοτήτων ασφάλειας μεταξύ διάφορων συμμετεχόντων που μπορούν ή δεν μπορούν να υποστηρίξουν όλες τις απαραίτητες απαιτήσεις ασφάλειας. Η H.235.6 σύσταση υποστηρίζει την αυθεντικοποίηση στις πολυσημειακές συνδέσεις με τον ίδιο τρόπο που υποστηρίζεται μεταξύ δύο τελικών σημείων.

Για το ιδιοαπόρρητο, ο πολλαπλής διανομής ελεγκτής είναι ο master και οι συμμετέχοντες είναι οι slaves, έτσι ώστε ο master να μπορεί να διαπραγματευτεί τις ιδιότητες ασφάλειας, συμπεριλαμβανομένων των κλειδιών και των αλγορίθμων κρυπτογράφησης ανάλογα με τις ανάγκες. Τα media κλειδιά συνεδρίας μπορούν να

προστατευθούν από το μηχανισμό προστασίας που χρησιμοποιείται στην H.245, χρησιμοποιώντας πιστοποιητικά (που χρησιμοποιούν το δημόσιο κλειδί) ή χρησιμοποιώντας έναν άλλο μηχανισμό κρυπτογράφησης, όπου στην περίπτωση αυτή το κλειδί απεικονίζεται στο sharedSecret πεδίο του H.235 μηνύματος.

Ένας μηχανισμός που προσφέρεται για να μετριάσει τις DOS ή τις annoyance επιθέσεις ενάντια στις media πόρτες είναι η εφαρμογή του antispamming, στην οποία ο δέκτης πιστοποιεί τα RTP πακέτα χρησιμοποιώντας τον κώδικα αυθεντικοποίησης μηνυμάτων μέσω ειδικών πεδίων του RTP πακέτου. Ο μηχανισμός ισχύει για τα media streams όπου τα πακέτα κρυπτογραφούνται ή δεν κρυπτογραφούνται. Εάν δεν κρυπτογραφούνται, η πλευρά αποδοχής υπολογίζει τη MAC της RTP επιγραφής (συμπεριλαμβανομένου του αριθμού ακολουθίας και του timestamp) χρησιμοποιώντας τον αλγόριθμο διαπραγμάτευσης (στο antiSpamAlgorithm πεδίο). Η εικόνα 36 επεξηγεί αυτήν την έννοια.



Εικόνα 36 Παράδειγμα της αυθεντικοποίησης του H.235.6 RTP για το antispam

Εάν το RTP πακέτο κρυπτογραφείται, ο antispam μηχανισμός θα πρέπει να ελέγξει την αυθεντικότητα του πακέτου πριν από την αποκρυπτογράφηση του ωφέλιμου φορτίου. Αν και η RTP επιγραφή δεν κρυπτογραφείται, οι επιγραφές των audio και video codecs πρέπει να κρυπτογραφηθούν.

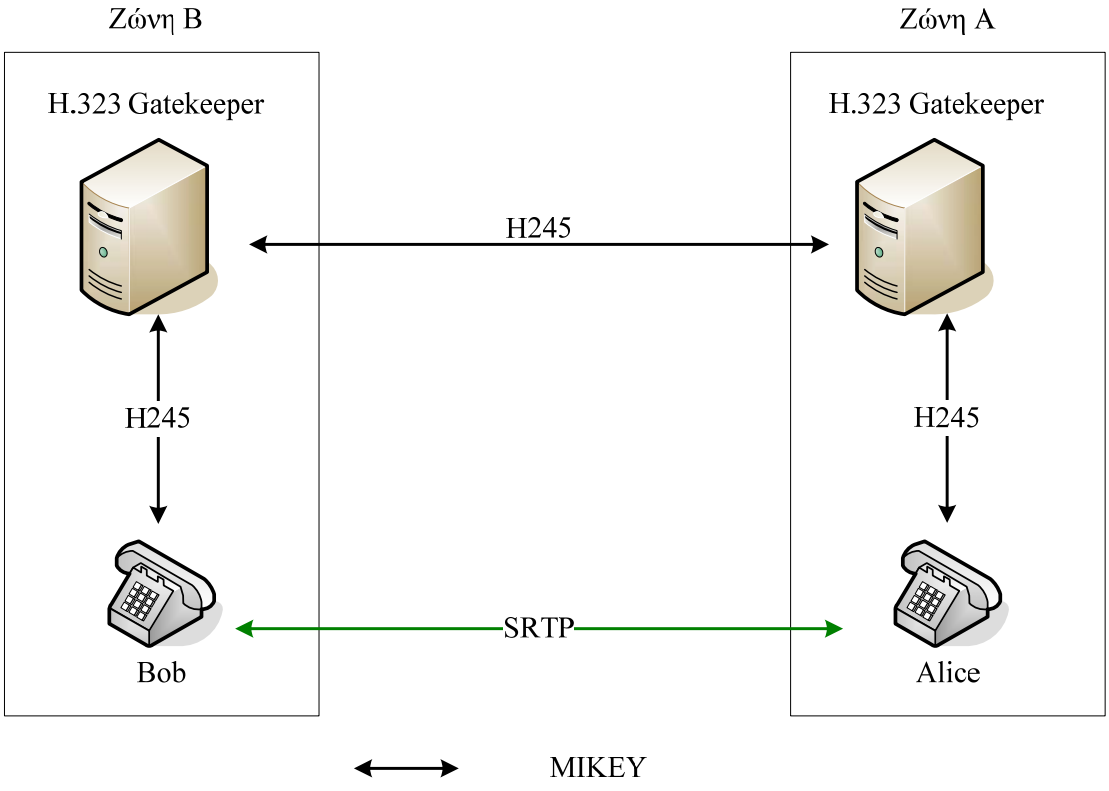
3.6.8. H.235.7 Προφίλ ασφάλειας χρησιμοποιώντας τα MIKEY + SRTP μαζί με το H.235

Η H.235.7 σύσταση συζητά τη χρήση του MIKEY με το SRTP για την διαπραγμάτευση των κλειδιών κρυπτογράφησης και την προστασία των media streams. Η σύσταση συζητά τα ακόλουθα δύο προφίλ ασφάλειας:

- Symmetric key-based υποδομή ασφάλειας που υποστηρίζει πολλαπλούς gatekeepers

- Asymmetric key-based υποδομή ασφάλειας (PKI) που υποστηρίζει πολλαπλούς gatekeepers

Η εικόνα 37 είναι μια λογική απεικόνιση της χρήσης του MIKEY μέσα σε ένα H.323 περιβάλλον.

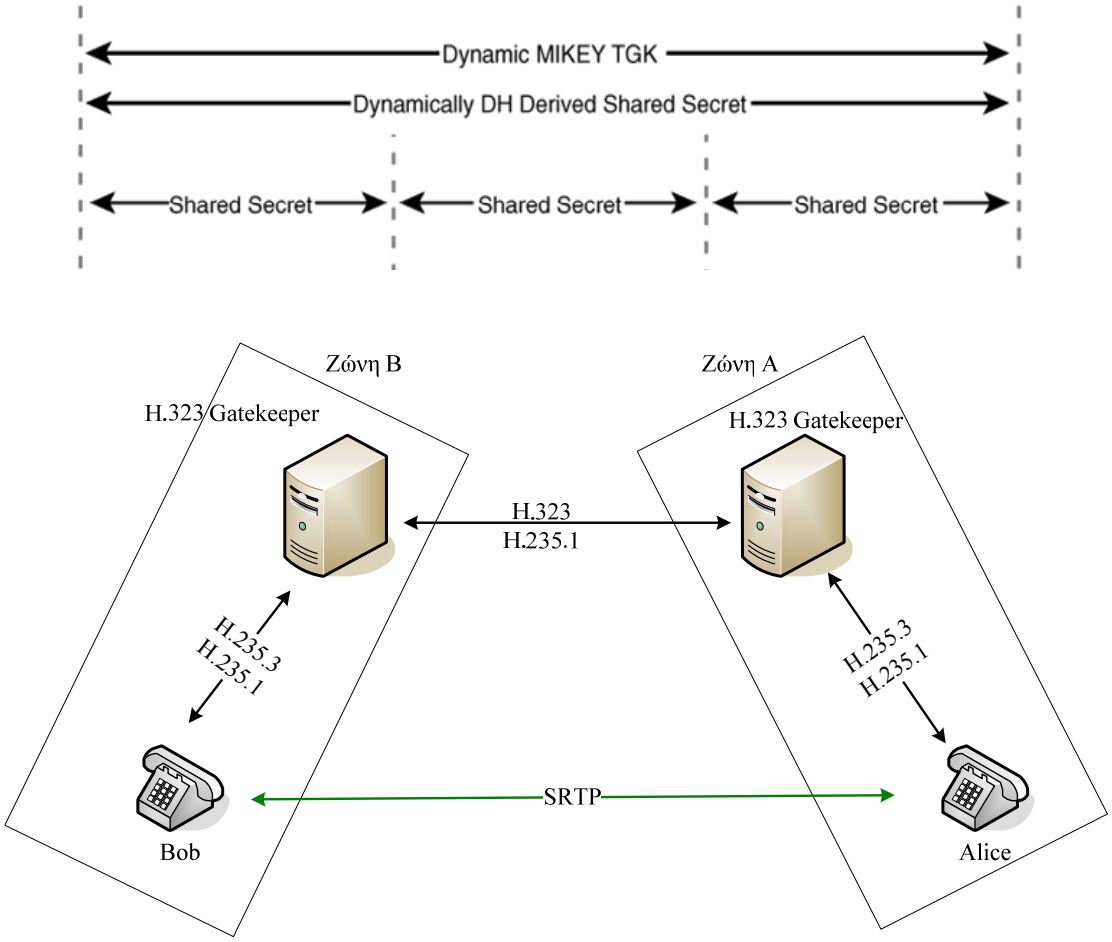


Εικόνα 37: Χρήση του MIKEY στο H.323.

Τα MIKEY μηνύματα μεταφέρονται μαζί με τα H.245 handshake μηνύματα σηματοδοσίας κατά μήκος στα τελικά σημεία, διαφανή στους ενδιάμεσους gatekeepers. Τα handshake μηνύματα περιλαμβάνουν τα TerminalCapabilitySet, RequestMode, OpenLogicalChannel, και MiscellaneousCommand.

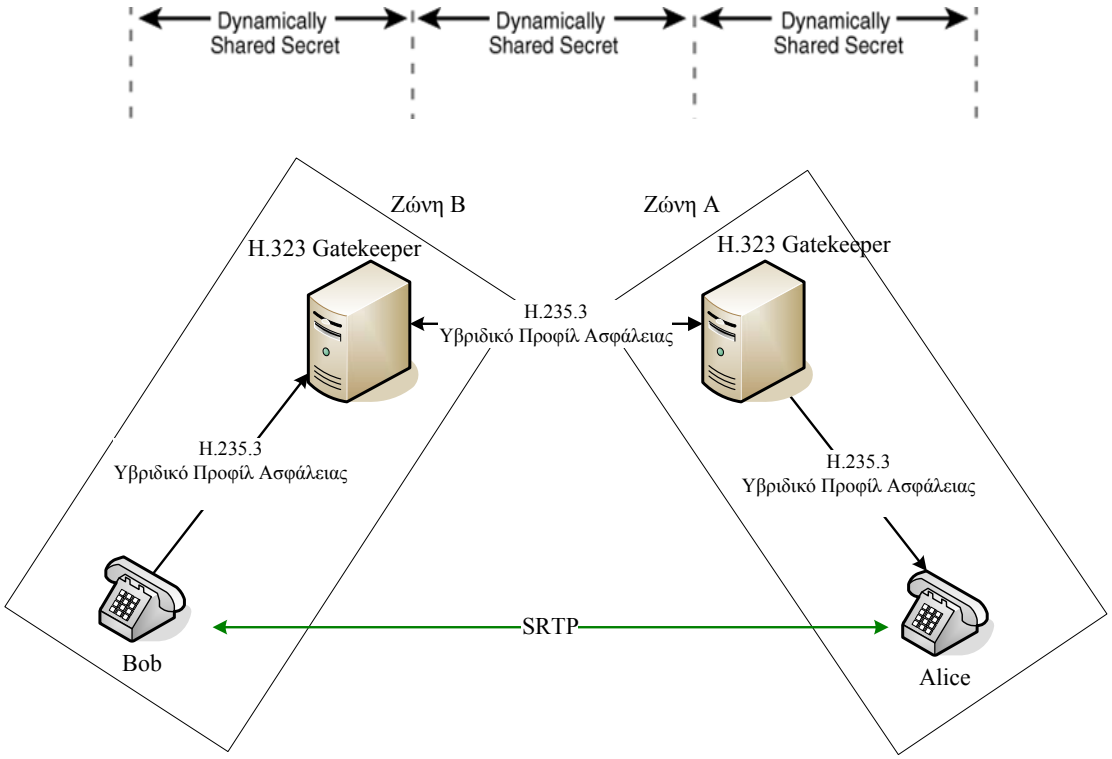
Το MIKEY πρωτόκολλο μπορεί να εφαρμοστεί στο επίπεδο συνεδρίας με το H.323 (πολλαπλά media streams) και στο media επίπεδο (ένα συγκεκριμένο λογικό κανάλι).

Επιπλέον, το προφίλ παρέχει τη δυνατότητα της διαπραγμάτευσης του υλικού κλειδιών μέσω της χρήσης των συμμετρικών και ασυμμετρικών τεχνικών. Στην περίπτωση όπου τα προ-κοινά κλειδιά χρησιμοποιούνται για να υποστηρίξουν το MIKEY, η H.235.1 βασική γραμμή εφαρμόζεται μεταξύ των hops, όπως φαίνεται στην εικόνα 38.



Εικόνα 38: Χρήση των προ-κοινών κλειδιών για την υποστήριξη του MIKEY.

Σε αυτό το σενάριο, μια σχέση εμπιστοσύνης έχει εδραιωθεί χρησιμοποιώντας κοινά μυστικά μεταξύ κάθε hop και χρησιμοποιώντας το H.235.1 προφίλ βασικής ασφάλειας. Αν και αυτή η διαμόρφωση μπορεί να είναι αποτελεσματική για τις μικρές ομάδες, δεν είναι εξελικτική για τις επικοινωνίες στα μεγάλα κατανεμημένα περιβάλλοντα. Για την υποστήριξη των επικοινωνιών στα μεγάλα κατανεμημένα περιβάλλοντα, ένας εξελικτικός μηχανισμός πρέπει να χρησιμοποιηθεί για την δυναμική διαπραγμάτευση των κρυπτογραφικών κλειδιών. Η εικόνα 39 απεικονίζει αυτήν την προσέγγιση.



Εικόνα 39: Δυναμικά διατιθέμενα κλειδιά για την υποστήριξη του MIKEY.

Αυτή η διαμόρφωση απαιτεί τη χρήση μιας PKI υποδομής για την δυναμική διαπραγμάτευση των κοινών κλειδιών. Μια σημαντική πτυχή για οποιοδήποτε πρωτόκολλο διαχείρισης κλειδιών είναι ο χρονικός συγχρονισμός. Η H.235 σύσταση υποθέτει ότι ο κατάλληλος συγχρονισμός ρολογιών ρυθμίζεται αυτόματα από το δίκτυο.

3.6.9. H.235.8 Ανταλλαγή κλειδιών για το SRTP σε ασφαλή κανάλια σηματοδοσίας

Το H.235.8 προφίλ παρέχει τους μηχανισμούς για την υποστήριξη της ανταλλαγής κλειδιών μαζί με τις παραμέτρους της αυθεντικοποίησης και του αλγορίθμου κρυπτογράφησης για τα SRTP ρεύματα μεταξύ των H.323 τερματικών. Το προφίλ εστιάζει στις επικοινωνίες μονής εκπομπής και η ITU σκοπεύει να ερευνήσει τις επιλογές για πολλαπλής εκπομπής στο μέλλον.

Το SrtpCryptoCapability πεδίο χρησιμοποιείται για την γνωστοποίηση των ικανοτήτων του SRTP που υποστηρίζονται από το H.323 τερματικό και μπορούν να χρησιμοποιηθούν κατά τη διάρκεια της διαπραγμάτευσης. Αυτό το υπό-πεδίο βρίσκεται μέσα στο genericH235SecurityCapability πεδίο κάτω από τον encryptionAuthenticationAndIntegrity κλάδο του H.245μηνύματος. Το SrtpCryptoCapability περιέχει το SrtpCryptoInfo υπό-πεδίο που περιέχει τις παραμέτρους της crypto-ακολουθίας και της συνεδρίας που χρησιμοποιούνται στην αντίστοιχη συνεδρία πολυμέσων.

Το υλικό κλειδιών που χρησιμοποιείται στο SRTP ανταλλάσσεται μέσω της χρήσης της SRTP SrtpKeyParameters crypto παραμέτρου, η οποία είναι ένα υπό-πεδίο του SrtpKeys και μεταβιβάζεται μέσω του H.245 OpenLogicalChannel μηνύματος. Οι συντάκτες του H.235.8 σχεδίασαν τη SRTP crypto παράμετρο ώστε να είναι σε θέση να δημιουργήσει τις SRTP κρυπτογραφικές παραμέτρους σε ένα μοναδικό μήνυμα ή μια μοναδική μετ' επιστροφής ανταλλαγή μηνυμάτων. Επιπλέον, ένα μοναδικό μήνυμα μπορεί να χρησιμοποιηθεί για την ανταλλαγή των SRTP crypto παραμέτρων, εξαλείφοντας κατά συνέπεια τη φάση της διαπραγμάτευσης.

Για κάθε επικοινωνία μονής εκπομπής, δύο ομοιοκατευθυνόμενα κανάλια διατηρούν SRTP ευδιάκριτες παραμέτρους. Για κάθε κατεύθυνση, ένα ευδιάκριτο H.245 OpenLogicalChannel μήνυμα χρησιμοποιείται για να δημιουργήσει τις crypto SRTP παραμέτρους. Το αρχικό H.323 τερματικό στέλνει μια crypto-προσφορά στο απομακρυσμένο τερματικό. Η προσφορά περιέχει το SrtpCryptoCapability πεδίο, το

οποίο περιέχει μια SrtpCryptoInfo δομή και μια SrtpKeys δομή με μία ή περισσότερες SrtpKeyParameters.

Οι εξ' ορισμού κρυπτογραφικές μετατροπές για το H.235.8 είναι οι AES με την μέθοδο μέτρησης και χρησιμοποιούν το μήκος των 128-bit. Ο εξ' ορισμού κώδικας αλγόριθμου της αυθεντικοποίησης μηνυμάτων είναι ο SHA1, με μήκος είτε 80-bit είτε 32-bit. Επιπλέον, η AES f8 υποστηρίζεται με κλειδί των 128-bit και η SHA1 με μήκος 80-bit για το UMTS (Universal Mobile Telecommunications System).

Το H.323 έχει παρόμοια προβλήματα με το SIP με τα πρώιμα media και την παραγωγή των αιτημάτων σηματοδοσίας. Το πρόβλημα με τα πρώιμα media είναι ότι αφότου στέλνεται η αρχική προσφορά σε ένα απομακρυσμένο τερματικό, το αρχικό τερματικό μπορεί να λάβει τα media (πρώιμα media) από το καλούμενο τερματικό του συμβαλλόμενου μέρους πριν λάβει μια απάντηση (παραδείγματος χάριν, λόγω ψαλιδίσματος ή καθυστέρησης) για το ποιες crypto ικανότητες υποστηρίζονται από το μακρινό H.323 τερματικό. Επομένως, το αρχικό τερματικό πρέπει να είναι σε θέση να χειριστεί ένα τέτοιο σενάριο επειδή το δεν γνωρίζει ποιο κλειδί το μακρινό τερματικό χρησιμοποιεί για τα media. Σε αυτήν την περίπτωση, το πρότυπο συστήνει έναν μηχανισμό, όπως οι H.460.11 διαδικασίες εγκατάστασης καθυστερημένων κλήσεων. Στην περίπτωση όπου πολλαπλές προσφορές έχουν παραχθεί, το αρχικό τερματικό δεν ξέρει ποια προσφορά έγινε αποδεκτή από το μακρινό τερματικό έως ότου παραλάβει την απάντηση. Την ίδια στιγμή, τα media μπορεί να παραληφθούν πριν ληφθούν οι απαντήσεις για όλες τις προσφορές. Ομοίως, ένας μηχανισμός όπως η H.460.11 διαδικασία εγκατάστασης καθυστερημένης κλήσης θα πρέπει να χρησιμοποιηθεί.

3.6.10. H.235.9 Πύλη ασφαλείας υποστηρίζοντας το H.323

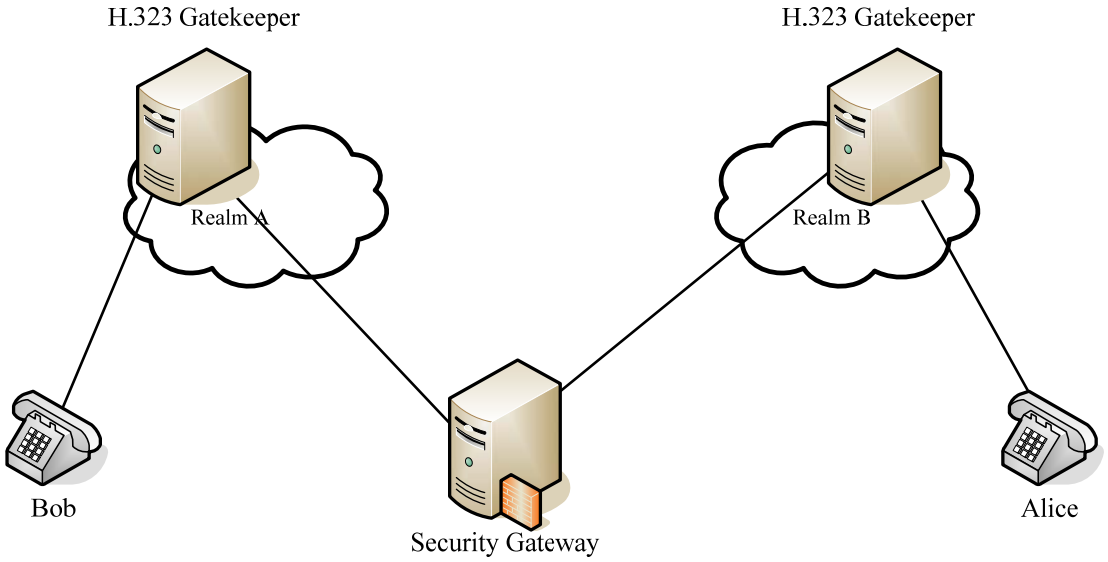
Οι έλεγχοι ασφαλείας που καθορίζονται στις H.235.x συστάσεις παρέχουν επαρκή υποστήριξη στην προστασία ενάντια στις διάφορες επιθέσεις και στην δημιουργία ασφαλών επικοινωνιών μεταξύ των συμμετεχόντων ενός H.323 δικτύου. Μερικές από τις επιθέσεις περιλαμβάνουν την παραποίηση και την παραπλάνηση μηνυμάτων, την eavesdropping, και το SPIT. Συγχρόνως, αυτοί οι έλεγχοι ασφαλείας παρεμποδίζουν

τις ροές κλήσης που διασχίζουν τα τμήματα δικτύου, όπως τα firewalls ή ALGs (application layer gateways), που τροποποιούν τα μηνύματα της σηματοδοσίας και των media, να ανταλλάσσονται. Το H.323 δεν είναι το μόνο πρωτόκολλο που επηρεάζεται από αυτήν την κατάσταση. Παρόμοια ζητήματα συνδέονται με τη SIP σηματοδοσία, όπου οι πληροφορίες της μεταφοράς μηνυμάτων, όπως οι IP διευθύνσεις και πόρτες, αλλάζουν από μια ενδιάμεση συσκευή (παραδείγματος χάριν, NAT).

Αυτές οι τροποποιήσεις ακυρώνουν την ακεραιότητα και την αυθεντικότητα των μηνυμάτων, αναγκάζοντας τους ελέγχους της αυθεντικότητας και της ακεραιότητας να αποτύχουν σε τέτοια περιβάλλοντα. Επομένως, η ITU έχει εισάγει τη H.235.9 σύσταση, η οποία περιγράφει τρόπους για την μετρίαση αυτών των ζητημάτων δίνοντας άδεια στην πύλη ασφαλείας να παραποιήσει τα μηνύματα της σηματοδοσίας και των media όπως απαιτείται.

Με βάση τον καθορισμό των προτύπων, μια πύλη ασφαλείας είναι μια «συσκευή που εγκαθίσταται μεταξύ δύο ή περισσότερων IP περιοχών δικτύου για την πραγματοποίηση λειτουργιών ασφάλειας, όπως η επικύρωση ή ο περιορισμός των ροών πακέτων και η χαρτογράφηση των διευθύνσεων μεταφοράς μεταξύ των περιοχών δικτύου.»

Η πύλη ασφαλείας πρέπει να εδραιώσει μια σχέση εμπιστοσύνης με τον τοπικό gatekeeper που χρησιμεύει για την λήψη, την επεξεργασία, την τροποποίηση και την διαβίβαση των μηνυμάτων της σηματοδοσίας και των media. Αυτή η σχέση εδραιώνεται όταν η πύλη ασφαλείας εγγράφεται στον τοπικό gatekeeper. Αυτή η σχέση εμπιστοσύνης επιτρέπει στην πύλη ασφαλείας να αποκτήσει πρόσβαση στο κλειδί αυθεντικοποίησης που διαπραγματεύεται μεταξύ του gatekeeper και του τελικού σημείου που θέλει να διαβιβάσει μηνύματα της σηματοδοσίας ή των media. Η κατοχή πρόσβασης στο κλειδί αυθεντικοποίησης επιτρέπει στην πύλη ασφαλείας να παραποιεί μη ιδιωτικά δεδομένα (παραδείγματος χάριν, διευθύνσεις μεταφοράς) στα μηνύματα σηματοδοσίας και να αναπαραγάγει πληροφορίες αυθεντικοποίησης του μηνύματος πριν το διαβιβάζει στον προορισμό του. Η εικόνα 40 απεικονίζει την τοποθέτηση της πύλης ασφαλείας.



Εικόνα 40: H.323 πύλη ασφαλείας.

Η δυνατότητα τροποποίησης των ιδιοτήτων των πρωτοκόλλων ασφάλειας (παραδείγματος χάριν, TLS, IPSec) είναι τρωτή στις bid-down επιθέσεις. Παραδείγματος χάριν, εάν ένα τελικό σημείο είναι σε θέση να προστατεύσει τα μηνύματα των media χρησιμοποιώντας ποικίλους μηχανισμούς (παραδείγματος χάριν, DES, AES, κανένα) και ιδιότητες (μήκος κλειδιού των 64, 128, 192, 256), μια πύλη ασφαλείας απατεώνων μπορεί να προσπαθήσει να υποβαθμίσει το μέγεθος του μήκους κλειδιού ή να ζητήσει μη κρυπτογράφηση ώστε να αποκτήσει πρόσβαση στην RTP κυκλοφορία. Συνιστάται να επιβάλλεται ρητά η πολιτική τοπικής ασφάλειας χωρίς χώρο για απόκλιση στη διαπραγμάτευση των πιο αδύναμων μηχανισμών και ιδιοτήτων κρυπτογράφησης υπό οποιουσδήποτε όρους.

Επιπλέον, η κατοχή πρόσβασης στο κλειδί διαπραγμάτευσης της τελικής συσκευής και του gatekeeper εισάγει μια ευκαιρία για επίθεση. Παραδείγματος χάριν, μια πύλη ασφαλείας απατεώνων μπορεί να εγγραφτεί σε έναν gatekeeper και να χρησιμοποιήσει το κλειδί διαπραγμάτευσης αυθεντικοποίησης για να κατασκευάσει κακόβουλα μηνύματα παραποιώντας τις πληροφορίες δρομολόγησης (IP διεύθυνση, πόρτες, αρχικός αριθμός τηλεφώνου) ώστε να υποδυθεί έναν χρήστη. Επομένως, οι πύλες ασφαλείας πρέπει να έχουν κωδικούς πρόσβασης, να εκτελούν τις διαδικασίες πρόκλησης - απάντησης αυθεντικοποίησης για την επιβολή της αμοιβαίας

αυθεντικοποίησης μεταξύ του gatekeeper και της καταχωρημένης πύλης ασφαλείας και να ακλουθούν τις συστάσεις που καθορίζονται σε H.235.1, H.235.2, H.235.3, και H.235.5.

3.6.11. Δυνατότητες και περιορισμοί του H.235

Το H.235 παρέχει διάφορους μηχανισμούς για την υποστήριξη της αυθεντικοποίησης, της εμπιστευτικότητας, και της ακεραιότητας, μαζί και τη διασύνδεση με τα πρωτόκολλα ανταλλαγής κλειδιών, όπως το MIKEY, για την υποστήριξη των κατανεμημένων επικοινωνιών. Η ακόλουθη λίστα συνοψίζει μερικές από τις δυνατότητες και τους περιορισμούς του H.235 που μπορούν να μελετηθούν κατά τον σχεδιασμό ενός VoIP δικτύου ή της αξιολόγησης μιας VoIP εφαρμογής.

- Δυνατότητες

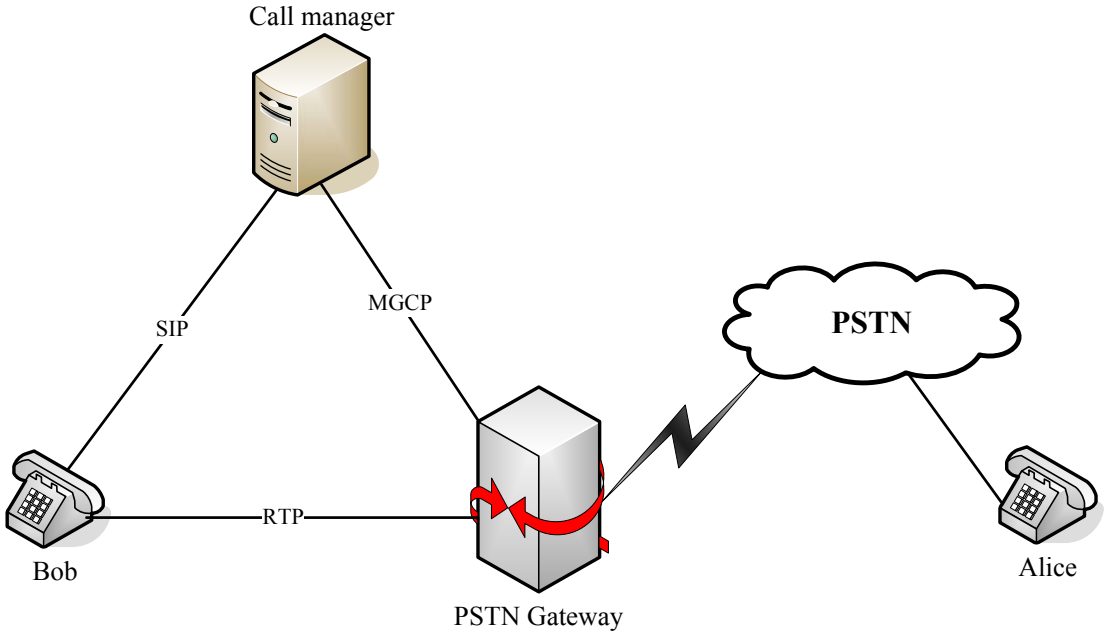
  - ✓ Μπορεί να παρέχει από άκρο σε άκρο ασφάλεια, ανάλογα με το συνδυασμό συστάσεων ασφάλειας (προφίλ) που χρησιμοποιούνται.
  - ✓ Μπορεί να υποστηρίξει ασφάλεια πολλαπλής και μονής εκπομπής.
  - ✓ Μπορεί να προστατεύσει από διάφορες επιθέσεις χρησιμοποιώντας συνδυασμούς των H.235 προφίλ, συμπεριλαμβανομένων των DOS επιθέσεων, τις man-in-the-middle επιθέσεις, επιθέσεις replay, spoofing, connection hijacking, και eavesdropping.

- Περιορισμοί

  - ✓ Δεν διαβαθμίζεται καλά για τις επικοινωνίες Διαδικτύου.
  - ✓ Μεγαλύτερο επίπεδο πολυπλοκότητας εφαρμογής έναντι του SIP.
  - ✓ Το H.235 δεν είναι ευρέως εφαρμοσμένο στα προϊόντα, και η λειτουργικότητα μεταξύ των προμηθευτών είναι αμφισβητήσιμη.

3.7. Μηχανισμοί προστασίας του MGCP

Το Media Gateway Control Protocol (RFC 3435) χρησιμοποιείται από τις PSTN πύλες για την εγκατάσταση των κλήσεων μεταξύ των IP δικτύων ή μεταξύ των IP δικτύων και του PSTN. Σε μερικές περιπτώσεις, η PSTN πύλη μπορεί να αποσυντεθεί σε μια πύλη σηματοδοσίας και μια media πύλη. Για τη συζήτησή μας, θα συνδυάσουμε την πύλη της σηματοδοσίας και των media σε ένα συστατικό και θα αναφερθούμε σε αυτήν ως PSTN πύλη. Η εικόνα 41 απεικονίζει τον προσδιορισμό θέσης μιας PSTN πύλης στο δίκτυο.



Εικόνα 41: Προσδιορισμός θέσης της PSTN πύλης σε ένα δίκτυο.

Σε αυτό το παράδειγμα, ο τελικός χρήστης δημιουργεί μια κλήση μέσω του call manager, ο οποίος στη συνέχεια καθοδηγεί την PSTN πύλη στο να διαθέσει ένα κανάλι για την κλήση του Bob. Ο call manager είναι αρμόδιος για το συντονισμό της οργάνωσης, της τροποποίησης και της λήξης κλήσης μεταξύ των τελικών συσκευών και των PSTN πυλών. Μετατρέπει τα μηνύματα σηματοδοσίας μεταξύ διάφορων πρωτοκόλλων, συμπεριλαμβανομένου των SIP/H.323 και MGCP. Αφότου διαθέσει η PSTN πύλη τους πόρους, αποκρίνεται πίσω στον call manager με τις αντίστοιχες πληροφορίες τι οποίες το τηλέφωνο του Bob πρέπει να χρησιμοποιήσει για την

αποστολή της RTP κυκλοφορίας του (παραδείγματος χάριν, UDP πόρτες, η IP διεύθυνση της PSTN πύλης, codecs, και ούτω καθεξής).

Το MGCP πρωτόκολλο δεν παρέχει ελέγχους ασφαλείας, αλλά συστήνει ότι πρωτόκολλα ασφάλειας, όπως το IPSec, πρέπει να χρησιμοποιούνται για την παροχή της απαραίτητης προστασίας. Δυστυχώς, πολλοί προμηθευτές (εάν όχι όλοι) δεν υποστηρίζουν το IPSec με το MGCP. Διάφορες επιθέσεις μπορούν να πραγματοποιηθούν ενάντια στις πύλες που χρησιμοποιούν το MGCP. Το άνοιγμα του MGCP επιτρέπει σε διάφορες επιθέσεις να πραγματοποιηθούν ενάντια σε μια πύλη που χρησιμοποιεί το MGCP. Ένας επιτιθέμενος μπορεί να στείλει μηνύματα σηματοδοσίας για να αποσυνδέσει τις κλήσεις, να εκτρέψει τα RTP πακέτα σε έναν άλλο host, ή να πάρει μέρος σε μια υπάρχουσα συνομιλία χωρίς τη γνώση των συμμετεχόντων.

3.7.1. Συστάσεις για την προστασία του MGCP από επιθέσεις

Η ακόλουθη λίστα παρέχει συστάσεις που είναι αποτελεσματικές στην προστασία ενάντια στις επιθέσεις στο MGCP:

- Επιβολή του ACLs δικτύου για τον περιορισμό της πρόσβαση στις MGCP πόρτες από μη εξουσιοδοτημένες πηγές. Αυτό θα προστατεύσει από τις κακόβουλες προσπάθειες παραποίησης των υπαρχουσών συνεδρίων.
- Επιβολή των ένα προς ένα σχέσεων μεταξύ των call managers (ή call agents) και των PSTN πυλών για την ανταλλαγή των MGCP μηνυμάτων.
- Εάν η PSTN πύλη υποστηρίζει το IPSec, ενεργοποίηση του για την κρυπτογράφηση της κυκλοφορίας μεταξύ των call managers και των PSTN πυλών.

3.7.2. Δυνατότητες και περιορισμοί του MGCP

Το MGCP χρησιμοποιείται σε πολλές εφαρμογές για την υποστήριξη της σηματοδοσίας στην δημιουργία καναλιών μεταξύ των IP και των PSTN δικτύων, αλλά στερείται των κατάλληλων μηχανισμών ασφάλειας που προστατεύουν από τις

επιθέσεις. Η ακόλουθη λίστα συνοψίζει τις δυνατότητες και τους περιορισμούς που πρέπει να εξεταστούν κατά την ανάπτυξη του MGCP στα VoIP δίκτυα.

- Δυνατότητες

  - ✓ Εξελικτικό για τα δίκτυα επιχειρήσεων και μεταφορέων.
  - ✓ Από την άποψη της ασφάλειας, δεν υπάρχουν άλλες δυνατότητες εκτός από τη σύσταση στο πρότυπο για την χρησιμοποίηση του IPSec.

- Περιορισμοί

  - ✓ Δεν παρέχει αυθεντικοποίηση, ακεραιότητα, ή εμπιστευτικότητα για να την προστασία των μηνυμάτων του.
  - ✓ Χρησιμοποιεί το UDP ως πρωτόκολλο μεταφοράς, και επομένως διάφορες επιθέσεις είναι εφαρμόσιμες (παραδείγματος χάριν, message masquerading).

Συμπεράσματα

Στην παρούσα πτυχιακή συζητήθηκαν τα δημοφιλέστερα πρωτόκολλα σηματοδοσίας κλήσης, οι επιθέσεις που μπορεί να πραγματοποιηθούν, μαζί με τους μηχανισμούς προστασίας που μπορούν να χρησιμοποιηθούν για να υποστηρίξουν την εμπιστευτικότητα, την ακεραιότητα, και την επικύρωση των μηνυμάτων. Με την εφαρμογή αυτών των μηχανισμών προστασίας, ο κίνδυνος ελαχιστοποιείται αρκετά και μετριάζεται η επιτυχής πραγματοποίηση επιθέσεων όπως των eavesdropping, replay, call hijacking, unauthorized network access, και άλλων.

Ένα κρίσιμο σημείο της ασφάλειας ενός VoIP δικτύου είναι η διαμόρφωση και η εφαρμογή του λογισμικού που υποστηρίζει τα ρεύματα σηματοδοσίας και media. Εάν ένα VoIP δίκτυο είναι κακώς διαμορφωμένο και δεν χρησιμοποιεί την εμπιστευτικότητα, την ακεραιότητα, και την επικύρωση για τα μηνύματα σηματοδοσίας και media, θα είναι τρωτό σε επιθέσεις, οι οποίες μπορεί να έχουν επιπτώσεις είτε στις λειτουργίες του οργανισμού είτε στο προφίλ του ή και ακόμα στην οικονομική του σταθερότητά. Επομένως, οι σχεδιαστές των VoIP δικτύων πρέπει να εξετάσουν τις απαιτήσεις ασφάλειας που θα πρέπει να υποστηρίζονται από το VoIP δίκτυο. Οι οργανισμοί που έχουν ήδη εφαρμόσει την VoIP τεχνολογία θα πρέπει να εξετάσουν την κατάσταση ασφάλειας του VoIP δικτύου τους και να προσδιορίσουν τις αδυναμίες που μπορεί να επηρεάζουν τις λειτουργίες ή άλλους τομείς τους.

Εκτός από τις επιθέσεις που αναφέρονται στην παρούσα εργασία και επικεντρώνονται στην περιοχή της σηματοδοσίας, υπάρχουν ακόμα ευπάθειες σε άλλες περιοχές, όπως στην διαχείριση των κλειδιών ή στην μετάδοση των media streams, που πρέπει να μελετηθούν ώστε να αποτραπεί η κακόβουλη εκμετάλλευσή τους από τους επιτιθεμένους.

Βιβλιογραφία

1. J. Rosenberg, H., et al. *SIP: Session Initiation Protocol*. RFC 3261, June 2002.
2. F.Cao. *Response Identity in Session Initiation Protocol*, IETF 2006.
3. T. Dierks, E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.1*, IETF RFC 4346.
4. E. Rescorla, N. Modadugu, *Datagram Transport Layer Security*, IETF RFC 4347.
5. E. B. Ramsdell. S/*MIME Version 3 Message Specification*. RFC 2633, June 1999.
6. S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol (IPSec)*. RFC 2401, November 1998.
7. ITU-T Recommendations H.225, H.245, and H.235.0 through H.235.9.
8. Spirent Communications, Inc., *Voice over IP (VoIP)*, http://www.spirentcom.com/documents/100.pdf
9. Handley, M., Schulzrinne, H., Schooler, E. and Rosenberg, J. March 1999. *SIP: Session Initiation Protocol.* Request for Comment 2543, http://www.ietf.org/rfc/rfc2543.txt.
10. ITU-T Recommendation H.323. (1999). *Packet-based multimedia communications systems*. http://www.itu.int/rec/T-REC-H.323-199909-S/en
11. Dalgic, I. & Fang, *H. Comparison of H.323 and SIP for IP Telephony Signalling*. Retrieved February, 2006 at URL:http://www.iptel.org/info/references/papers/misc/Dalg9909_Comparison.pdf.
12. Mark Collier, *Voice Over IP (VoIP) Denial of Service (DoS)*, http://download.securelogix.com/library/DoS.pdf
13. *VoIP Security Risks*.(2004). http://searchenterprisevoice.techtarget.com/searchEnterpriseVoice/downloads/VoIPsecurityChap7.pdf
14. Thermos, P. (2006). *Two attacks against VoIP*. Retrieved April, 2006 at http://www.securityfocus.com/infocus/1862/1.
15. VOIPSA, *VoIP Security and Privacy Threat Taxonomy* http://www.voipsa.org/Activities/taxonomy.php, October 2005.

16. Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., Ehlert, K.S., Sisalem, D. *Survey of security vulnerabilities in session initiation protocol*, Communications Surveys & Tutorials, IEEE Volume 8, Issue 3, 3rd. Qtr. 2006 Page(s):68 – 81
17. Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., *Session Initiation Protocol Security Mechanisms: A state-of-the-art review*, INC'05 International Network Conference, July 2005, Pages: 147-156
18. Sisalem, D.; Kuthan, J.; Ehlert, S., *Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms*, IEEE Network, Volume 20, Issue 5, Sept.-Oct. 2006 Page(s): 26 – 31
19. Dunte, M.; Ruland, C., *Secure Voice-over-IP*, IJCSNS International Journal of Computer Science and Network Security, Volume7 No.6, June 2007
20. Eduardo B. Fernandez, Juan C. Pelaez, Maria M. Larrondo-Petrie, *Security patterns for Voice over IP Networks*, JOURNAL OF SOFTWARE, Volume 2, NO. 2, AUGUST 2007