Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Σταύρος Υψηλάντης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Μάιος 2013

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ασφάλεια σε Περιβάλλον Διαδικτυακής Τηλεφωνίας (VoiceOverIp–VoipSecurity)

Σταύρος Υψηλάντης

Επιβλέπων Καθηγητής
Στέφανος Γκρίτζαλης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2013

Περίληψη

Σήμερα η επικοινωνία μέσω διαδικτύου κερδίζει όλο και περισσότερο έδαφος. Προκύπτουν όμως θέματα ασφαλείας όπως σε όλες τις εφαρμογές διαδικτύου που πρέπει να αντιμετωπιστούν. Η συγκεκριμένη μεταπτυχιακή διατριβή θα παρουσιάσει μία state-of-the-art αναφορά αυτών των θεμάτων.

Στόχος αυτής της μεταπτυχιακής διατριβής είναι να συγκεντρωθούν τα θέματα ασφαλείας και οι μηχανισμοί ασφαλείας που υπάρχουν σε περιβάλλοντα διαδικτυακής τηλεφωνίας και το προσδοκώμενο αποτέλεσμα είναι να παρουσιαστούν λεπτομερώς όλα αυτά.

Αρχικά αναζητήθηκε η υπάρχουσα βιβλιογραφία που αναφέρεται στο συγκεκριμένο θέμα. Μετά έγινε η καταγραφή των θεμάτων ασφαλείας που προκύπτουν και των μηχανισμών ασφαλείας που συναντώνται σε περιβάλλοντα διαδικτυακής τηλεφωνίας και στη συνέχεια έγινε αναλυτική μελέτη αυτών και η κατηγοριοποίηση τους.

Τα αποτελέσματα της έρευνας είναι η καταγραφή των θεμάτων ασφαλείας που προκύπτουν σε περιβάλλοντα διαδικτυακής τηλεφωνίας και η μελέτη του καθενός από αυτά. Συγκεντρώνονται όλα αυτά τα θέματα και παρουσιάζονται οι μηχανισμοί με τους οποίους μπορούν αυτά να αντιμετωπιστούν. Επίσης αναφέρεται πως αυτοί οι κίνδυνοι θα μπορούσαν να αποφευχθούν. Επιπλέον, μελετούνται τα υπάρχοντα πρωτόκολλα ασφαλείας για τον χειρισμό αυτών των κινδύνων και παρουσιάζονται οι λόγοι για τους οποίους δημιουργούνται αυτοί οι κίνδυνοι.Τέλος, καταγράφονται τα οφέλη που έχουν οι κακόβουλοι χρήστες που ξεκινάνε τις επιθέσεις εναντίον της τηλεφωνίας μέσω διαδικτύουκαι αναφέρονταιτασυμπεράσματαπουπροκύπτουν από την παρούσα μεταπτυχιακή διατριβή.

Summary

NowadaysVoice over Internet Protocol (Voip)is constantly developing. Nevertheless,security issues that need to be addressed arearising,as in allweb applications. This master thesiswillpresent astate-of-the-artreport of theseissues.

The aimof this masterthesis isto gathersafety andsecurity mechanismsthat exist inVoip telephonyenvironmentsandthe expected outcomeis a detailed report ofall these issues.

Initially, the existing literature mentioned to this topic was searched. After that, security issuesthat ariseandsecurity mechanisms that found inVoip telephonyenvironments were recorded and then a categorization and an analyticalstudy of thesewas done.

The resultsof the surveyis to record thesecurity issuesthat arise inVoip telephonyenvironmentsand the researchof each ofthem. All these issues are gathered and themechanisms, with whichthey can beaddressed, are presented. Moreover, the ways that theserisks couldbe avoided are reported.Furthermore,the existingsecurity protocols for the handling of these risks are studied and thereasons forcreatingsuch risks are presented. Finally, the benefits of the malicious users that start the attacks against Voip are recordedand the conclusions of the present master thesis arehighlighted.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Στέφανο Γκρίτζαλη για τη βοήθεια και την καθοδήγηση του στη συγγραφή της παρούσας μεταπτυχιακής διατριβής.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Η παρούσα μεταπτυχιακή διατριβή είναι μία έρευνα η οποία καταγράφει τους κινδύνους ασφαλείας και τα τρωτά σημεία των Voip επικοινωνιών εστιάζοντας στο Sipπρωτόκολλο, ένα πολύ διαδεδομένο πρωτόκολλο ανοιχτού κώδικα που χρησιμοποιείται στις Voip επικοινωνίες.

Στην παρούσα μεταπτυχιακή διατριβή μελετήθηκαν προηγούμενες έρευνες πάνω στο συγκεκριμένο θέμα και συγκεντρώθηκαν τα θέματα ασφαλείας που προκύπτουν σε αυτού του είδους τις επικοινωνίες καθώς και οι τρόποι αντιμετώπισης τους μέχρι σήμερα.

Στο 2ο κεφάλαιο παρουσιάζεται αναλυτικά το Sip πρωτόκολλο, πάνω στο οποίο εστιάζει η παρούσα μεταπτυχιακή διατριβή. Στο 3ο κεφάλαιο καταγράφονται αναλυτικά οι κακόβουλες επιθέσεις που μπορούν να γίνουν εναντίον του συγκεκριμένου πρωτοκόλλου και παρουσιάζονται τα θέματα ασφαλείας που προκύπτουν. Στο 4ο κεφάλαιο παρουσιάζονται οι υφιστάμενοι μηχανισμοί ασφαλείας όπως αυτοί προκύπτουν από τη μελέτη των διαθέσιμων ερευνητικών κειμένων, ταξινομημένοι ανάλογα με το επίπεδο που αυτοί λειτουργούν (ανίχνευση, αντιμετώπιση, πρόληψη).

Τέλος παρουσιάζονται τα συμπεράσματα που προκύπτουν από την παραπάνω έρευνα.

Κεφάλαιο 2

Το SipΠρωτόκολλο

2.1. Αρχιτεκτονική Sip

Το Sip[02]είναι ένα πρωτόκολλο σηματοδοσίας επιπέδου εφαρμογής για τον χειρισμό συνεδριών που πραγματοποιούνται μέσω διαδικτύου. Το Sip προτυποποιήθηκε από την Ietf και σχεδιάστηκε να υποστηρίζει αμφίδρομη αλλά όχι με όριο επικοινωνία, συμπεριλαμβάνοντας Voip κλήσεις. Η υποδομή ενός δικτύου που χρησιμοποιεί το Sip πρωτόκολλο αποτελείται από τα εξής στοιχεία:

UserAgents: Το UserAgent[01] δραστηριοποιείται στο τερματικό. Αποτελείται από το UserAgentClient που είναι υπεύθυνο να δημιουργεί αιτήσεις και το UserAgentServer που είναι υπεύθυνο να επεξεργάζεται και να απαντά στις αιτήσεις που δημιουργεί το UserAgentClient.

Εξυπηρετητής εγγραφών: Το Uasεπικοινωνεί με τους εξυπηρετητές εγγραφώνγια να δηλώσει την παρουσία του στο δίκτυο. Οι Sipεξυπηρετητές εγγραφών είναι μια βάση δεδομένων που περιέχει τοποθεσίες με βάση τις προτιμήσεις των χρηστών όπως αυτές έχουν καταγράφει από το Uas.

Διαμεσολαβητής:Ο διαμεσολαβητής δέχεται την αίτηση και την προωθεί στην τοποθεσία που καλεί κατευθείαν ή σε έναν άλλο εξυπηρετητή που έχει καλύτερη πληροφόρηση για την τοποθεσία που καλείται.

Εξυπηρετητής επαναπροώθησης: Ο εξυπηρετητής επαναπροώθησης δέχεται την αίτηση και ενημερώνει το Ua (UserAgent) αυτού που κάνει την κλήση για τον επόμενο ενδιάμεσοεξυπηρετητή. OUa αυτού που καλεί τότε επικοινωνεί με τον επόμενο ενδιάμεσοεξυπηρετητή απευθείας.

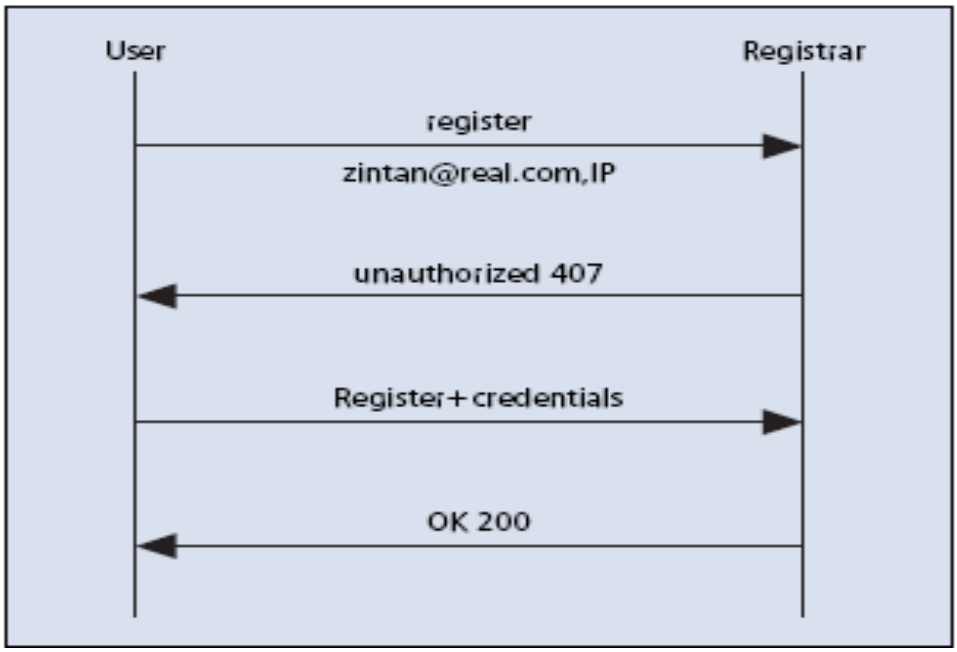
Το SIP[02]μοιάζει σε κάποια πράγματα με το Http: βασίζεται σε μηνύματα κειμένου, έχει δομή αίτηση-απάντηση και χρησιμοποιεί μηχανισμό HttpDigestAuthentication για την αυθεντικοποίηση του χρηστή. Το πρωτόκολλο είναι από τη φύση του Stateful (ο πελάτης συνδέεται στον εξυπηρετητή, διεξάγει μια σειρά λειτουργιών μέσω της σύνδεσης και μετά αποσυνδέεται. Τότε ο εξυπηρετητής μπορεί να συνδέσει όλες τις

αιτήσεις μαζί και να γνωρίζει ότι όλες έγιναν από τον ίδιο χρήστη) που υποστηρίζει διάδραση με διαφορά στοιχεία του δικτυού (Pstn γέφυρα) και ασύγχρονες ειδοποιήσεις.Ενώ η μηχανή πεπερασμένων καταστάσεων είναι φαινομενικά απλή, στην πράξη γίνεται μεγάλη και περίπλοκη. Μία παρατήρηση που οφείλεται στο ότι το κύριο SIPRFC είναι ένα από τα μεγαλύτερα που έχουν οριστεί ποτέ και μαζί με πρόσθετα RFC μεγαλώνουν κι άλλο τον ορισμό.

Το Sip[02] είναι πρωτόκολλο σηματοδοσίας (η σηματοδοσία χρησιμοποιείται για να ορίσει την κατάσταση της σύνδεσης μεταξύ τηλεφώνων ή Voip τερματικών) που βασίζεται στο Rtp για τη μετάδοση πολυμέσων. Υπάρχει ένα Rtp προφίλ που υποστηρίζει την κρυπτογράφηση και την ακεραιότητα αλλά ακόμα δεν χρησιμοποιείται ευρέως. Η οικογένεια των Rtp πρωτοκόλλων περιλαμβάνει το Rtcp που χρησιμοποιείται να διαχειρίζεται βασικές Rtp παραμέτρους μεταξύ των σημείων επικοινωνίας.

Το SIP μπορεί να λειτουργήσει πάνω από πολλά πρωτόκολλα μεταφοράς ανάμεσα στα οποία είναι το Tcp, Sctp, Udp. Το Udp είναι αυτό που προτιμάται λόγο της απλότητας και της απόδοσης του αλλά το Tcp έχει το πλεονέκτημα ότι υποστηρίζει Tls προστασία για την κλήση. Το Sctp έχει πολλά πλεονεκτήματα που έχουν μαζί το Udp και το Tcp, όπως η αντοχή στην άρνηση της υπηρεσίας, είναι πολλών κατευθύνσεων, παρέχει κινητή υποστήριξη και πολυπλεξία σύνδεσης πάνω σε ένα απλό κανάλι.

Στο Sip[01]έχουν εισαχθεί διάφοροι τύποι μηνυμάτων κειμένου που βασίζονται στην δομή του Http.Τα μηνύματα Sip πρέπει να ταυτοποιούν τον αποστολέα, που αντιστοιχεί σε μία μοναδική διεύθυνση. Ο κάθε χρήστης Sip έχει μία μοναδική διεύθυνση (SIP-URI) που είναι της μορφής user@domain π.χ. ipsilantis@michailides.com . Αυτή η διεύθυνση μπορεί να διαχειριστεί από έναν SIP διαμεσολαβητή που είναι υπεύθυνος για τα πεδία των χρηστών. Η διαδικασία εγγραφής φαίνεται στην εικόνα 1.



Εικόνα 1. Διαδικασία Εγγραφής

2.2 Εγκαθίδρυση της επικοινωνίας στο Sip

Η διαδικασία[01] ώστε να χρησιμοποιήσει κάποιος μια υπηρεσία Sip είναι η εξής: Αρχικά πρέπει να ορίσει την τοποθεσία του με βάση την Ip του. Στη συνέχεια πρέπει να καταχωρήσει τον συνδυασμό Ip-Sip διεύθυνση στον Sipεξυπηρετητή εγγραφών που είναι υπεύθυνος για το πεδίο του.

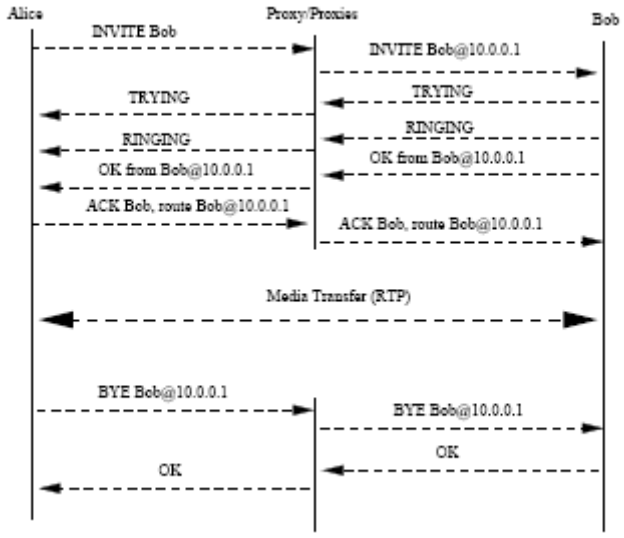
Όταν καλείται κάποιος, αυτός που τον καλεί στέλνει μια πρόσκληση Sip στον Sipδιαμεσολαβητή ο οποίος ελέγχει τη βάση δεδομένων του εξυπηρετητή εγγραφών ή τη βάση δεδομένων του Dnsεξυπηρετητή ώστε να βρει την τοποθεσία αυτού που καλείται και προωθεί την κλήση στον καλούμενο. Ο τελευταίος μπορεί να αποδεχτεί ή να απορρίψει την κλήση. Κατά τη διάρκεια της ανταλλαγής των μηνυμάτων ο καλών και ο δέκτης ανταλλάσουν τις διευθύνσεις και τις θύρες που θέλουν να λαμβάνουν τα δεδομένα όπως και το είδος των δεδομένων που θα λάβουν (βίντεο, φωνή, κτλ). Μετά την ολοκλήρωση της δημιουργίας της σύνδεσης τα τερματικά μπορούν να ανταλλάσουν δεδομένα χωρίς την παρεμβολή Sipδιαμεσολαβητή.

Ωστόσο κάτω υπό συγκεκριμένες συνθήκες μπορεί ο εξυπηρετητής να μην είναι διαθέσιμος, εκεί χρειάζεται ο εξυπηρετητής επαναπροώθησης που αναλαμβάνει να πληροφορήσει τον καλούντα για εναλλακτικές διαδρομές. Όταν ληφθεί η πληροφορία

από τον καλούντα ξαναδημιουργεί και στέλνει το πακέτο από την εναλλακτική διαδρομή.

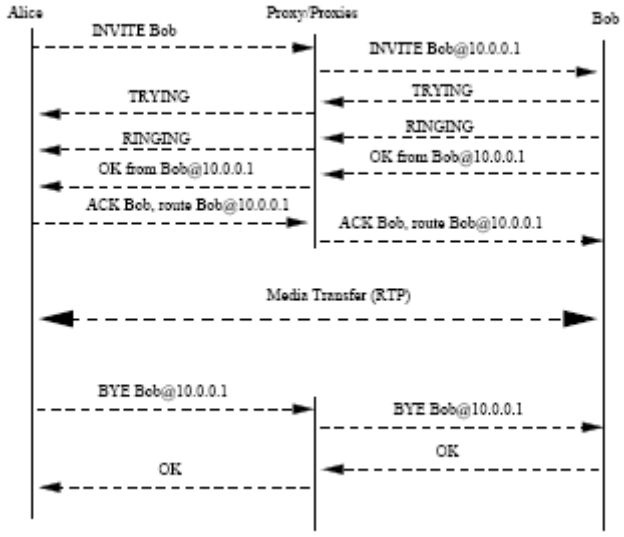
Κατά τη διάρκεια του ορισμού των παραμέτρων της κλήσης[02], το τερματικό επικοινωνεί με τον διαμεσολαβητή που χρησιμοποιεί τον εξυπηρετητή τοποθεσιών ώστε να ορίσει που πρέπει να δρομολογήσει την κλήση. Μπορεί να υπάρχει και άλλο τερματικό (ίδια εταιρεία) στο ίδιο δίκτυο ή ένας άλλος διαμεσολαβητής σε άλλο δίκτυο. Εναλλακτικά μπορεί το τερματικό να χρησιμοποιήσει τον εξυπηρετητή επαναπροωθήσεων ώστε απευθείας να ορίσει που πρέπει να δρομολογήσει την κλήση, ο εξυπηρετητής επαναπροωθήσεων μιλάει με τον εξυπηρετητή τοποθεσίας με τον ίδιο τρόπο που ο διαμεσολαβητής λειτουργεί κατά τον ορισμό της κλήσης. Μόλις το κανάλι από άκρο σε άκρο δημιουργηθεί μεταξύ 2 τερματικών, το Sip ορίζει τις πραγματικές παραμέτρους της συνεδρίας χρησιμοποιώντας το Sdp πρωτόκολλο.

Η εικόνα 2 δείχνει την ανταλλαγή μηνυμάτων κατά τη διάρκεια της εγκαθίδρυσης μιας κλήσης μεταξύ δύο μερών. Η Alice στέλνει ένα μήνυμα πρόσκλησης στον διαμεσολαβητή, προαιρετικά έχοντας σαν περιεχόμενο πληροφορίες για την παραμετροποίηση της συνεδρίας κωδικοποιημένες με το Sdp. Ο διαμεσολαβητής προωθεί απευθείας το μήνυμα στον Bob, αν η Alice και ο Bob είναι χρήστες του ίδιου τομέα. Αν ο Bob έχει εγγραφεί σε άλλοντομέα, το μήνυμα θα μεταφερθεί στον διαμεσολαβητή του Bob και από εκεί στον Bob. Το μήνυμα μπορεί να μεταφερθεί σε πολλά τερματικά αν ο Bob έχει εγγραφεί από πολλές τοποθεσίες. Όσο η εγκαθίδρυση της κλήσης είναι σε αναμονή, Ringing μηνύματα στέλνονται πίσω στην Alice. Μόλις η κλήση εγκαθιδρυθεί ένα μήνυμα Οκ αποστέλλεται στην Alice, περιλαμβάνοντας τις παραμέτρους της κλήσης του Bob κωδικοποιημένες με το Sdp. Η Alice απαντάει με ένα Ack μήνυμα. Οι παράμετροι κλήσης της Alice μπορούν να κωδικοποιηθούν στο μήνυμα πρόσκλησης ή στο Ack μήνυμα.



Εικόνα 2. Ανταλλαγή μηνυμάτων κατά τη διάρκεια εγκαθίδρυσης μίας σύνδεσης μεταξύ 2 μερών επικοινωνίας στο Sip.

Για την αυθεντικοποίηση των τερματικών οι εξυπηρετητές εγγραφών και οι διαμεσολαβητές χρησιμοποιούν το HttpDigestAuthentication όπως φαίνεται στην εικόνα 3. Αυτό είναι ένα απλό πρωτόκολλο πρόσκλησης-απάντησης που χρησιμοποιεί ένα κοινό κλειδί μαζί με ένα όνομα χρήστη,ένα όνομα τομέα,ένα κλειδί bit μιας χρήσης, και ειδικά πεδία από το Sip μήνυμα για να υπολογιστεί μια κρυπτογραφική συνάρτηση (CryptographicHash).Οι κωδικοί δε, μεταφέρονται σε PlaintextForm μέσω του δικτυού. Σημειώνεται ότι η αυθεντικοποίηση μπορεί να ζητηθεί σε οποιαδήποτε στιγμή κατά τη διάρκεια της ρύθμισης της κλήσης (CallSetup) .



Εικόνα 3. SipDigestAuthentication

Για πιο πολύπλοκα σενάρια αυθεντικοποίησης το Sip μπορεί να χρησιμοποιήσει την ενθυλάκωση S/Mime για να μεταφέρει μεγάλα φόρτια που συμπεριλαμβάνουν δημόσια κλειδιά και πιστοποιητικά. Όταν το Tcp χρησιμοποιείται σαν πρωτόκολλο μεταφοράς στο Sip, το Tls μπορεί να χρησιμοποιηθεί για να προστατεύσει τα μηνύματα Sip. Το Tls χρειάζεται για την επικοινωνία μεταξύ των διαμεσολαβητών, των εξυπηρετητών εγγραφών και των εξυπηρετητών επαναπροώθησης και απλά προτείνεται για επικοινωνία μεταξύ τερματικών με τους διαμεσολαβητές ή τους εξυπηρετητές εγγραφών. Εναλλακτικά το Ipsec μπορεί να χρησιμοποιηθεί για την προστασία όλων των επικοινωνιών ανεξάρτητα από το πρωτόκολλο μεταφοράς. Ωστόσο επειδή λίγες υλοποιήσεις ενσωματώνουν Sip,Rtp, και Ipsec είναι στην ευχέρεια των διαχειριστών να διαχειριστούν και να παραμετροποιήσουν τέτοιες ρυθμίσεις.

2.3 Μεταφορά δεδομένων στο Sip

Μετά την εγκαθίδρυση της κλήσης[02], τα τερματικά μπορούν να ξεκινήσουν μεταφορά ήχου και εικόνας χρησιμοποιώντας συνήθως το Rtp. Ενώ η διαδικασία της ανταλλαγής των μηνυμάτων για την εγκατάσταση της σύνδεσης μπορεί να αναμεταδίδεται μέσω ενός αριθμού Sipδιαμεσολαβητών, η κίνηση των δεδομένων (ήχος, εικόνα) ανταλλάσσεται απευθείας μεταξύ των τερματικών. Όταν γεφυρώνονται διαφορετικά δίκτυα Pstn και Sip, οι πύλες των δεδομένων μπορεί να διαταράξουν την από τερματικό σε τερματικό φύση της μεταφοράς των δεδομένων. Αυτές οι οντότητες (πύλες δεδομένων) μεταφράζουν μεταξύ των format που υποστηρίζονται από τα διαφορετικά δίκτυα.

Επειδή η μεταφορά των δεδομένων και η διαδικασία της εγκατάστασης της σύνδεσης λειτουργούν ανεξάρτητα, τα τερματικά είναι υπεύθυνα να δηλώσουν στους διαμεσολαβητές ότι η κλήση τερματίστηκε με τη χρήση ενός BYE μηνύματος που αναμεταδίδεται μέσω των διαμεσολαβητών μέσα από το ίδιο μονοπάτι που γίνεται η παραμετροποίηση της κλήσης.

Η κίνηση του Sip μεταφέρεται μέσω της θύρας 5060 ωστόσο μπορεί να διαφέρει ανάλογα με την παραμετροποίηση. Οι θύρες που χρησιμοποιούνται για τη μεταφορά των δεδομένων είναι δυναμικές και αποφασίζονται κατά τη διάρκεια της εγκαθίδρυσης της κλήσης μέσω του Sdp. Αυτό δημιουργεί κάποια προβλήματα όταν το Natκαι το ανάχωμα ασφαλείας διασταυρώνονται. Τυπικά αυτά είναι stateful και καταλαβαίνουν

τις αλλαγές στο Sip οπότε μπορούν να αλλάζουν τις κατάλληλες Rtp θύρες για τη μεταφορά των δεδομένων. Στην περίπτωση της εμπλοκής του Natπρωτοκόλλου τα τερματικά μπορούν να χρησιμοποιούν πρωτόκολλα σαν το Stun για να ενεργοποιήσουν την επικοινωνία. Εναλλακτικά το πρωτόκολλο PlugandPlay μπορεί να χρησιμοποιηθεί σε κάποια περιβάλλοντα.

Για τη μεταφορά των δεδομένων σε πραγματικό χρόνο το Sip χρησιμοποιεί το Rtp πρωτόκολλο. Το Rtp αναπτύχθηκε από την Ietf για τη μεταφορά ήχου και εικόνας μέσω Ip δικτύων. Το Rtp παρέχει από άκρο σε άκρο μεταφορά δεδομένων αλλά δεν παρέχει κανέναν μηχανισμό ασφαλείας για την επιβεβαίωση του χρόνου μεταφοράς ή την εγγυημένη ποιότητα της υπηρεσίας. Ενώ ο ήχος είναι ανθεκτικός σε μικρή απώλεια πακέτων αλλά μη ανθεκτικός στην καθυστέρηση, το Rtp συνήθως χρησιμοποιεί το Udp για τη μεταφορά πακέτων ήχου.

Το Rtp αποτελείται από 2 μέρη:

Το ένα που μεταφέρει δεδομένα με απαιτήσεις για μεταφορά σε πραγματικό χρόνο και το άλλο, Rtcp (RTPControlProtocol) το οποίο παρέχει εγγύηση για την ποιότητα της υπηρεσίας και μεταφέρει πληροφορίες στους συμμετέχοντες για την συνεδρία που βρίσκεται σε εξέλιξη. Μόλις ολοκληρωθεί η εγκαθίδρυση της κλήσης, το Rtp ενσωματώνει τα δεδομένα ήχου. Κάθε τερματικό κωδικοποιεί τα δεδομένα ήχου π.χ. με την G.711 κωδικοποίηση και ενσωματώνει το φορτίο σε Rtp κεφαλίδες.

2.4 Μηχανισμοί ασφαλείας στο Sip

Ipsec και Sip: Η χρήση του Ip[01] για μετάδοση Sip μηνυμάτων είναι ευάλωτη σε επιθέσεις, κακόβουλη πρόσβαση, ανάλυση κίνησης κτλ. Το Ip προσφέρει μηχανισμούς ασφάλειας με τα πρωτοκολλά Esp και AuthenticationHeader. Με το Ipsec στο Sip προστατεύονται οι επικοινωνία και τα δεδομένα που ανταλλάσσονται από δικτυακές απειλές.

TransportSecureLayer: Κατά τη διάρκεια της χειραψίας η αυθεντικοποίηση μπορεί να είναι κοινή με την ανταλλαγή των πιστοποιητικών. Αυτό έχει πολλά πλεονεκτήματα σε σχέση με το Ipsec και η εισαγωγή του στο καλωδιακό διαδίκτυο αποδεικνύει τη χρησιμότητα και την αποτελεσματικότητα του. Αυτό τρέχει πάνω από το επίπεδο Tcp/Ip και με πρωτόκολλα υψηλού επιπέδου όπως το Http και Ftp. Δε μπορεί να

συνδυαστεί με το Udp. Αφήνοντας όμως πολλές ανοιχτές συνδέσεις Tcp αυτό μπορεί να επιβαρύνει πολύ τους διαμεσολαβητέςSip. Σημειώστε ότι αυτό το πρωτόκολλο δεν έχει ακόμα πλήρη εφαρμογή στο Sip.

Αυθεντικοποίηση, πιστοποίηση, παρακολούθηση κίνησης: Για την αυθεντικοποίηση, πιστοποίηση και για την χρησιμοποίηση των αντίστοιχων υπηρεσιών είναι πιο βολικό για τους χρήστες του Sip να επικοινωνούν με εξυπηρετητές που θα κάνουν τα παραπάνω παρά να αποθηκεύουν τοπικά τα συνθηματικά τους όπως χρειάζεται στοHttp. Επίσης το ΑΑΑ (αυθεντικοποίηση, πιστοποίηση, παρακολούθηση κίνησης) δίνει τη δυνατότητα στους διαχειριστές να ορίζουν τον τύπο της αυθεντικοποίησης, πιστοποίησης που θα χρησιμοποιείται. Η εσωτερική σύνδεση ενός ετερογενούς δικτύου δίνει εντολές πρόσβασης στις Sip συσκευές ανεξαρτήτως από το δίκτυο που χρησιμοποιείται. Αυτό δίνει τη δυνατότητα στους χρήστες κινητών συσκευών να έχουν πρόσβαση όταν αλλάζουν το πεδίο στο οποίο βρίσκονται. Παράδειγμα ένας χρήστης κινητού χρησιμοποιεί έναν διαμεσολαβητή που βρίσκεται στην περιοχή που είναι ο χρήστης εκείνη τη στιγμή άλλα τα μηνύματα του πρέπει να δρομολογηθούν σε έναν διαμεσολαβητή που βρίσκεται στο σπίτι του. Οι χρήστες κινητών δημιουργούν την ανάγκη για δημιουργία νέων μηχανισμών ΑΑΑ και τη δημιουργία νέων πρωτοκόλλων όπως το Radius που πρέπει να ενσωματωθούν στον πυρήνα του Sip. Εφαρμογές Radius μπορούν να χρησιμοποιηθούν σε Sip περιβάλλον που με την αντίστοιχηδιεπαφήΑΑΑ θα χρειάζεται ώστε να αυθεντικοποιηθούν και να πιστοποιηθούν ώστε να χρησιμοποιήσουν τους Sip πόρους.

S/MimekaιSip: ΤαSipμηνύματαμπορούνναμεταφέρουνκύρια μέρη μηνυμάτων Mime (MultipurposeInternetMailExtensions). Για να υπάρξει ασφάλεια δημιουργήθηκε το SecureMime. Το Sip χρησιμοποιεί ένα μέρος του SecureMime πρωτοκόλλου. Την ακεραιότητα και την επαλήθευση της ταυτότητας. Αυτό απαιτεί την εισαγωγή των καθολικών κλειδιών (Pki). Τα ανταλλασσόμενα κλειδιά πρέπει να είναι υπογεγραμμένα από τους χρήστες, αυτό κάνει την ανταλλαγή των κλειδιών ευαίσθητη σε επιθέσεις Mitm (Maninthemiddle).

2.4.1 Ανάλυση των μηχανισμών ασφαλείας του Sip

Ο πιο συχνά χρησιμοποιούμενος από το Sip μηχανισμός ασφαλείας είναι ο Http αλγόριθμος αυθεντικοποίησης. Αυτός μπορεί να προσφέρει μονόδρομη

αυθεντικοποίηση μηνύματος και προστασίας της απάντησης αλλά δεν προσφέρει ακεραιότητα και εμπιστευτικότητα μηνύματος. Είναι πιθανό ένας κακόβουλος χρήστης να κάνει ενοχλητικές κλήσεις. Αυτή η μέθοδος είναι τρωτή επειδή χρησιμοποιεί κείμενο που ενεργοποιεί τις Mitm επιθέσεις και αυτό το κείμενο μπορεί να καταστραφεί από κάποιον απλά ανιχνεύοντας την κίνηση του δικτύου. Επίσης χρειάζεται ένα ασφαλές περιβάλλον για τη διανομή κωδικών ασφαλείας. Οι κωδικοί αποθηκεύονται στον εξυπηρετητή. Το ψηφιοκείμενο δεν προσφέρει ασφάλεια καθώς είναι εφικτό να βρεθούν τα στοιχεία του μηνύματος με μια επίθεση στον κρυπτογραφημένο κωδικό. Εκτός αυτού λόγο της απουσίας οποιασδήποτε συσχέτισης μεταξύ του ονόματος χρήστη και του Sip/Uri μπορεί ένας κακόβουλους χρήστης να παρουσιαστεί σαν νόμιμος. Έχουν προταθεί λύσεις γι' αυτό αλλά δυστυχώς για την υλοποίηση τους χρειάζεται αλλαγή στο SipUserAgent που φυσικά δεν είναι πάντα εύκολο να γίνει. Αν συνυπολογίσουμε ότι δεν υπάρχει κάποιο μοντέλο πιστοποίησης, ένας επιτιθέμενος μπορεί να χρησιμοποιήσει υπηρεσίες που κανονικά μπορούν να χρησιμοποιήσουν μόνο νόμιμοι χρήστες. Άλλο πρόβλημα είναι ότι οι ενδιάμεσοι Sipδιαμεσολαβητές δεν είναι σίγουροι ότι οι SipUa είναι αυθεντικοποιημένοι. Τα Sip μηνύματα πρέπει να έχουν ένα κρυπτογραφημένο Token που θα επιβεβαιώνει ότι η προέλευση της ταυτότητας του χρήστη έχει επιβεβαιωθεί από το αντίστοιχο δίκτυο. Ζητήματα απόδοσης επίσης αναφέρονται για διαδικασίες αυθεντικοποίησης.

Σχετικά με την αυθεντικοποίηση, είναι επίσης σημαντικό να προστατευτούν τα προσωπικά δεδομένα του χρήστη και η ταυτότητα του, παρέχοντας του ανωνυμία, ιδιωτικότητα και ιδιωτικότητα περιοχής. Το SipUasto παρέχει έχοντας ασφαλίσει τηνFrom κεφαλίδα στις Sip αιτήσεις. Δε μπορούν όλες οι κεφαλίδες να είναι ασφαλείς. Πχ. Η κεφαλίδα Contactχρειάζεται για αιτήσεις δρομολόγησης και δε μπορεί να προστατευτεί. Ασφάλεια δε μπορεί να επιτευχτεί χωρίς την επαρκή υποστήριξη των διαμεσολαβητώνSip.

Η ασφάλεια που προσφέρει το Ipsec προϋποθέτει ότι οι 2 χρήστες έχουν εμπιστοσύνη ο ένας στον άλλον και μπορεί να χρησιμοποιηθεί μόνο σε επικοινωνία με ενδιάμεσους εξυπηρετητές. Το Ipsec υλοποιείται σε επίπεδο λειτουργικού συστήματος, οπότε οι Sipπελάτες δε μπορούν να το υλοποιήσουν ακόμα. Γι' αυτό το Ipsec προστατεύει την επικοινωνία μόνο από εξυπηρετητή σε εξυπηρετητή. Οι προδιαγραφές του Sip δεν προτείνουν κάτι για διαχείριση κλειδιών που χρειάζεται το Ipsec. Πρόσφατα έχουν προταθεί κάποιες προσωρινές απαιτήσεις για να χρησιμοποιηθεί το Ipsec στο Sip.

Σε αντίθεση με το Ipsec το Tls δε χρειάζεται εμπιστευτικότητα ανάμεσα στους επικοινωνούντες. Το Tls μπορεί να χρησιμοποιηθεί είτε από μονόδρομα είτε από αμφίδρομα συστήματα αυθεντικοποίησης και ίσως είναι πιο κατάλληλο για διεθνή αυθεντικοποίηση τομέα. Φυσικά λαμβάνουμε υπόψη ότι το μήνυμα μπορεί να χαθεί μέσα στο δίκτυο του παραλήπτη καθώς η τελευταία μετάδοση δεν είναι κρυπτογραφημένη. Το Tls χρησιμοποιείται από το Sip για να προσφέρει ασφάλεια από άκρο σε άκρο. Ωστόσο αυτό αποτυγχάνει γιατί μέχρι τώρα δεν υπάρχει μηχανισμός που να σιγουρεύει ότι το Tls χρησιμοποιείται από όλα τα μέρη (αποστολέας έως τον παραλήπτη) μιας επικοινωνίας με ενδιάμεσους διαμεσολαβητές. Το Tls προστατεύει μόνο πρωτόκολλα βασισμένα στην επικοινωνία. Απλοποιώντας το, η έλλειψη Pki μηχανισμού στο Voip δεν προσφέρει το περιβάλλον που χρειάζεται για να χρησιμοποιηθεί το Tls.

Το S/Mimeχρησιμοποιείται για να εξασφαλίσει την ακεραιότητα ή την εμπιστευτικότητα σε μια από άκρο σε άκρο επικοινωνία. Σημειώνεται ότι το S/Mimeεπιβαρύνει τα μηνύματα Sip. Σημαντικό είναι ότι η ακεραιότητα και η εμπιστευτικότητα όλου του Sip μηνύματος δε μπορεί να προστατευτεί λόγο περιορισμών στην αλλαγή της κεφαλίδας του μηνύματος, οι ενδιάμεσοι κόμβοι πρέπει να έχουν πρόσβαση στην κεφαλίδα ώστε να προωθήσουν το μήνυμα στον κατάλληλο προορισμό. Τέλος, όπως και το Tls η έλλειψη του Pki είναι άλλος ένας περιορισμός στη χρήση του από το Sip.

Εκτός των παραπάνω περιορισμών , σε κάποιες περιπτώσεις η ασφάλεια μπορεί να χρειάζεται συνδυασμό Tls και S/Mime. Αυτό συμβαίνει όταν το Tls χρησιμοποιείται για να δώσει ακεραιότητα και εμπιστευτικότητα ενώ το S/Mimeγια να δώσει ιδιωτικότητα σε μερικά κομμάτια της μεταφερόμενης πληροφορίας. Ωστόσο μερικοί Sipεξυπηρετητές μπορεί να χρειάζεται να διαβάσουν αυτά τα δεδομένα. Αυτό απαιτεί έναν μηχανισμό ασφαλείας που να ασφαλίζει το κύριο μέρος του μηνύματος ή την κεφαλίδα μεταξύ Ua και διαμεσολαβητή ενώ την ιδία στιγμή η πληροφορία πρέπει να φαίνεται μόνο σε όσους πρέπει. Αυτό λέγεται από άκρο στο μέσο ασφάλεια.

2.4.2 Ασφάλεια πληροφορίας

Το πρώτο στάδιο προστασίας είναι η προστασία της σύνδεσης ώστε να γίνει η μεταφορά της πληροφορίας, μετά πρέπει να προστατευτεί και η πληροφορία που

μεταφέρεται. Το θέμα της ασφαλείας της πληροφορίας είναι στενά συνδεδεμένο με την ασφάλεια της μετάδοσης. Για τη δημιουργία της σύνδεσης χρησιμοποιείται το Dsp. Μετά, για τη μεταφορά της πληροφορίας σε πραγματικό χρόνο χρησιμοποιείται το Rtp. Η μεταφορά σε πραγματικό χρόνο πρέπει να γίνεται γρήγορα. Δυο παραδείγματα είναι η επικοινωνία ήχου μεταξύ 2 χρηστών και η αναπαραγωγή βίντεο. Επιπλέον αυτή η μεταφορά έχει συγκεκριμένες απαιτήσεις για τη μεταφορά από άκρο σε άκρο. Το Rtp παρέχει αυτές τις υπηρεσίες που χρειάζονται για τη μεταφορά σε πραγματικό χρόνο. Ωστόσο το Rtp δεν έχει κάποιο μηχανισμό ασφαλείας για την προστασία της μεταφερόμενης πληροφορίας από επιθέσεις αλλά προτείνει τη χρησιμοποίηση των υφιστάμενων μηχανισμών ασφαλείας των δικτύων. Έτσι σχεδιάστηκε συγκεκριμένα γι' αυτό το Srtp που παρέχει τους αντίστοιχους μηχανισμούς ασφαλείας για πακέτα δεδομένων όπως η εμπιστευτικότητα, η αυθεντικότητα και η προστασία της απάντησης στο Rtp. Το Srtp ορίζει αυστηρά τις υπηρεσίες ασφαλείας, ορίζει αλγορίθμους και τελικά παρέχει έναν μηχανισμό παροχής κλειδιών. Σημειώνουμε ότι το Srtp κρυπτογραφεί μόνο την πληροφορία από ένα πακέτο φωνής χωρίς να προσθέτει άλλες κεφαλίδες.

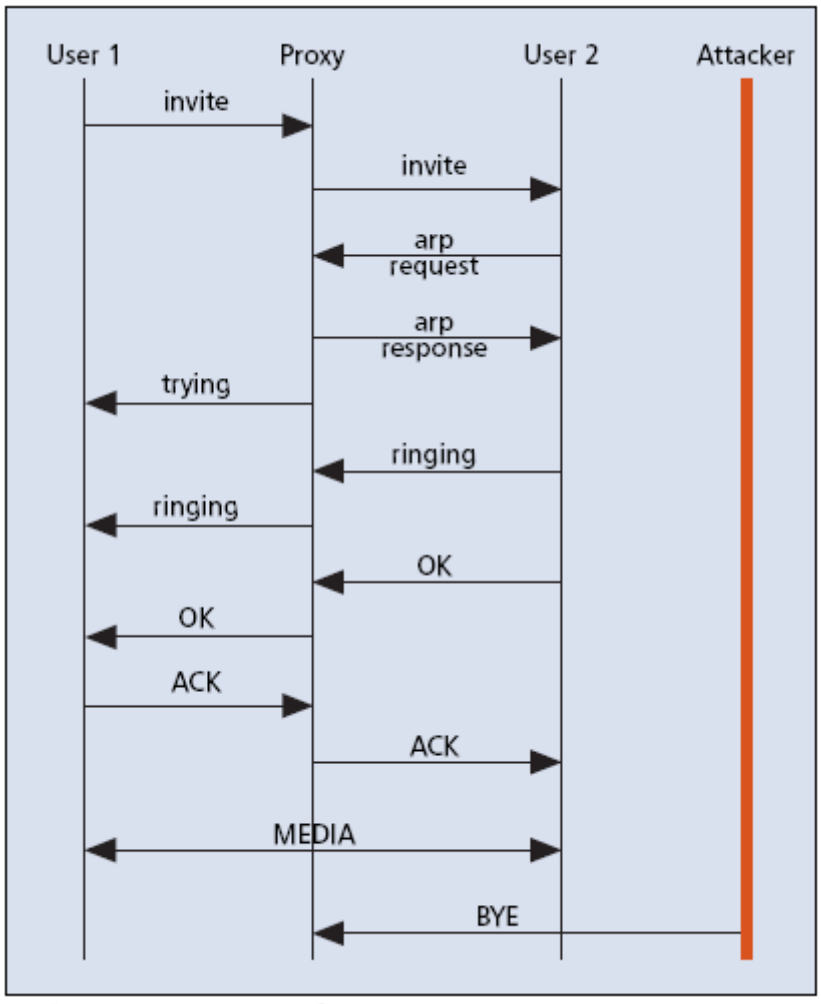
Επειδή έχει σχεδιαστεί αποκλειστικά για ζωντανή ροή το Rtp είναι πιο έξυπνο από το Ipsec σε ότι έχει να κάνει με το ρυθμό μετάδοσης. Επιπλέον το Srtp είναι πιο κατάλληλο για ιδιωτικότητα φωνής και εμπιστευτικότητα σε τοπικά δίκτυα για την προστασία από εσωτερικές επιθέσεις. Για παράδειγμα τα δεδομένα φωνής προστατεύονται από υποκλοπές, αν ένας χρήστης ξεκινήσει μια ασφαλή κλήση προς τον συνομιλητή του. Η ανάγκη για τέτοιες υπηρεσίες είναι σημαντική στο Voip σε αντίθεση με το Pstn, επειδή η πιθανότητα υποκλοπής στο Voip είναι πολύ μεγαλύτερη. Για παράδειγμα, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ελευθέρα εργαλεία και να πιάσει τα πακέτα Rtp.

Κεφάλαιο 3

Ζητήματα ασφαλείας και τρωτά σημεία στο Sip πρωτόκολλο

3.1 Επιθέσεις με σκοπό την άρνηση-διαταραχή της υπηρεσίας

3.1.1 Επίθεση τερματισμού



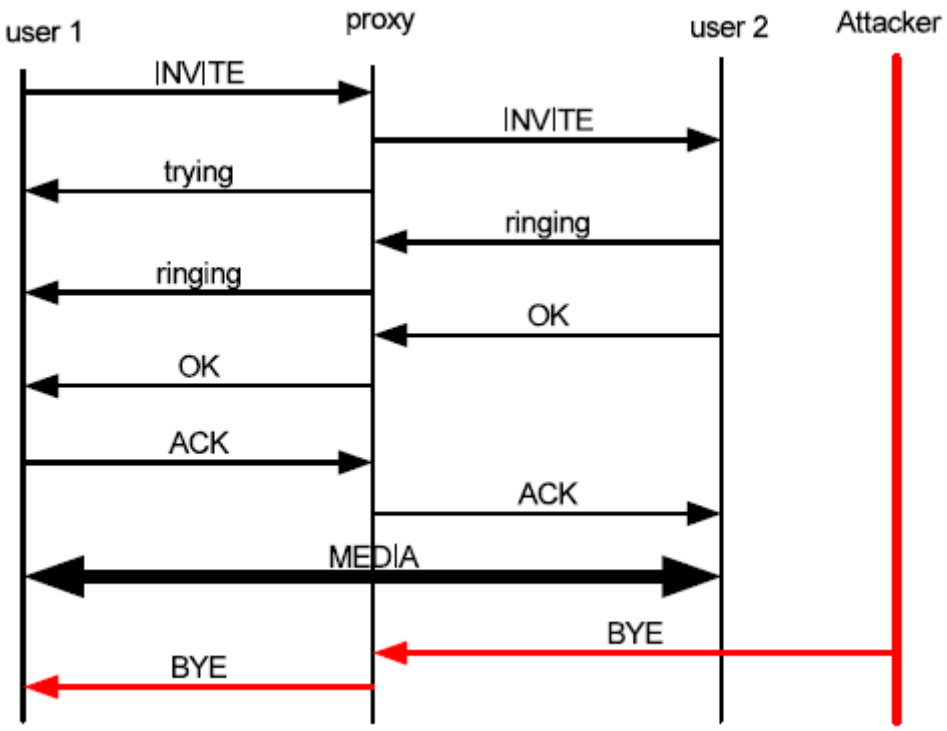
Εικόνα 4. BYE επίθεση

Η αίτηση τερματισμού[01] χρησιμοποιείται για να λήξει μια συνεδρία. Ο επιτιθέμενος μπορεί να στείλει μια αίτηση τερματισμού σε σημείο που δε θέλει ο νόμιμος χρήστης,

εικόνα 4. Για να ξεκινήσει η επίθεση πρέπει ο επιτιθέμενος να ξέρει όλες τις απαραίτητες πληροφορίες της συνεδρίας. Αυτό μπορεί να γίνει με την παρακολούθηση του δικτύου ή με επίθεση Mitm ώστε να εισάγει μια αίτηση τερματισμού στη συνεδρία. Αυτή η επίθεση μπορεί να είναι επιτυχής μόνο αν δεν υπάρχει μηχανισμός αυθεντικοποίησης και λαμβάνοντας υπόψη ότι ο επιτιθέμενος είναι ικανός να έχει όλα τα απαραίτητα στοιχεία της συνεδρίας. Η προστασία αυτών των παραμέτρων πρέπει να γίνει με εμπιστευτικότητα και αυτή να απαιτείται. Τέτοιες υπηρεσίες μπορούν να δώσουν το Ipsec ή το Tls. Επίσης η αυθεντικότητα ενός μηνύματος τερματισμού πρέπει να επαληθεύεται με τη χρήση είτε HttpDigest είτε Tls.

Η εύκολη πρόσβαση στο κανάλι επικοινωνίας θεωρείται μία από τις πιο σοβαρές απειλές που εμφανίζονται στο Voip. Το γεγονός ότι η υποκλοπή είναι σχεδόν το πρώτο βήμα για όλες τις επιθέσεις σε συνδυασμό με την φύση των Sip μηνυμάτων (Text-Based) κάνει τις Sip-Based υπηρεσίες πολύ ελκυστικές σε πολλές επιθέσεις.

Για παράδειγμα θεωρούμε ότι ένας εισβολέας συλλαμβάνει [03] (χρησιμοποιώντας για παράδειγμα Ethereal) την SIP κίνηση για μία συγκεκριμένη συνεδρία. Πιθανές συνέπειες μιας τέτοιας λαθραίας ακρόασης μπορεί να είναι: α) Γνωστοποίηση εμπιστευτικών πληροφοριών (ταυτότητες των επικοινωνούντων μερών), β) κακόβουλη χρησιμοποίηση συγκεκριμένων πληροφοριών της συνεδρίας με σκοπό να προκληθεί άρνηση της υπηρεσίας. Για παράδειγμα ένας επιτιθέμενος μπορεί να δημιουργήσει ένα πλαστό μήνυμα τερματισμού ή μήνυμα ακύρωσης χρησιμοποιώντας τις κατάλληλες παραμέτρους της συνεδρίας με σκοπό να τερματίσει, να ακυρώσει ή να αλλάξει μη νόμιμα μία συνεδρία. Αυτού του είδους οι επιθέσεις είναι γνωστές σαν επιθέσεις σηματοδοσίας.



Εικόνα 5. Μη νόμιμος τερματισμός κλήσης

Σαν παράδειγμα [03] θα περιγράψουμε με περισσότερες λεπτομέρειες την επίθεση τερματισμού. Ένας επιτιθέμενος για να ξεκινήσει μία επίθεση τερματισμού είναι απαραίτητο να ‘’εξερευνήσει’’ τις σωστές παραμέτρους της συνεδρίας. Αυτές οι παράμετροι περιλαμβάνονται στα μηνύματα σηματοδοσίας που ανταλλάσσονται πριν την εγκαθίδρυση της σύνδεσης. Συγκεκριμένα οι απαιτούμενες παράμετροι είναι: Callid, το σήμα στην FROM κεφαλίδα και το σήμα στην TO κεφαλίδα. Πρέπει να τονιστεί ότι το σήμα στην TO κεφαλίδα περιλαμβάνεται στο OK μήνυμα και επιπλέον ο επιτιθέμενος πρέπει να πιάσει το αντίστοιχο OK μήνυμα, προκειμένου να αποκτήσει όλες τις απαραίτητες πληροφορίες για να ξεκινήσει η επίθεση. Παρόλα αυτά σε μερικές περιπτώσεις το μήνυμα τερματισμού χρησιμοποιείται για τον τερματισμό μιας μη ολοκληρωμένης συνεδρίας χωρίς να χρειάζεται OK μήνυμα. Συνεπώς ένας εισβολέας μπορεί επίσης να ξεκινήσει μια επίθεση τερματισμού χωρίς το τελικό OK μήνυμα αλλά αυτό εξαρτάται από την υλοποίηση του SipUserAgent.

Γνωρίζοντας όλες τις παραμέτρους, ο επιτιθέμενος μπορεί να δημιουργήσει ένα πλαστό μήνυμα τερματισμού για τον τερματισμό/ακύρωση της αντίστοιχης συνεδρίας (εικόνα 5). Ο χρήστης που λαμβάνει το πλαστό μήνυμα τερματισμού δεν γνωρίζει ότι αυτό στάλθηκε από το κάποιον παράνομο χρήστη.

3.1.2 Επίθεση ακύρωσης

Επίθεση ακύρωσης: αυτή η αίτηση [01] υπάρχει για να ακυρώνει μια προηγούμενη αίτηση που έχει στείλει ο πελάτης. Συγκεκριμένα λέει στον εξυπηρετητή να ακυρώσει την επεξεργασία της αίτησης και να δημιουργήσει μια απάντηση σφάλματος που αφορά τη συγκεκριμένη αίτηση. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτή την αίτηση ώστε να ακυρώσει μια αίτηση από έναν νόμιμο χρήστη. Μια αίτηση ακύρωσης μπορεί να σταλεί μόνο για να ακυρώσει μια αίτηση πρόσκλησης. Αν ο εξυπηρετητής πάρει μία αίτηση ακύρωσης για κάποιο άλλο είδος αίτησης την απορρίπτει αλλά θα δημιουργήσει μια απάντηση σφάλματος. Επιπλέον μια εισερχόμενη αίτηση ακύρωσης δεν επεξεργάζεται αν η αυθεντική αίτηση έχει ήδη δημιουργήσει μια τελική απάντηση. Αυτό συμβαίνει γιατί η αίτηση ακύρωσης δεν έχει καμία επίπτωση σε αιτήσεις που έχουν πάρει έγκριση επεξεργασίας.

Οι αιτήσεις ακύρωσης μεταφέρονται με στρατηγική αποστολής σε ενδιάμεσους κόμβους και προώθηση από αυτούς και δε μπορούν να ξαναυποβληθούν. Σαν αποτέλεσμα, (αυτές δε μπορούν να αμφισβητηθούν από έναν εξυπηρετητή και έτσι τα κατάλληλα συνθηματικά μπαίνουν σε μια κεφαλίδα αυθεντικοποίησης). Η χρησιμοποίηση ενός μηχανισμού ασφαλείας όπως το Ipsec ή το Tls απαιτείται. Ωστόσο η επεξεργασία ενός ληφθέντος μηνύματος ακύρωσης από ένα διαφορετικό Sip τομέα είναι ακόμα άλυτο και ανοιχτό θέμα. Το να φαίνονται τα μηνύματα πρόσκλησης που δεν έχουν πάρει ακόμα την τελική έγκριση επεξεργασίας πιθανώς θα βοηθούσε να επιβεβαιωθεί οποιαδήποτε παράνομη αίτηση ακύρωσης.

3.1.3 Επίθεση αναφοράς

Επίθεση αναφοράς: η αναφορά είναι ο μηχανισμός που το ένα μέρος (αναφερόμενος) παρέχει σε ένα άλλο μέρος (επιβλέπων) μια διεύθυνση Sip που αναφέρεται σε αυτόν. Ο επιβλέπων θα στείλει μια αίτηση πρόσκλησης στον αναφερόμενο σε αυτή τη διεύθυνση αναφοράς. Η αναφορά μπορεί να χρησιμοποιηθεί για την ενεργοποίηση πολλών εφαρμογών όπως η μεταφορά κλήσης. Το RFC3892 εμπλουτίζει αυτή τη μέθοδο με το να επιτρέπει στον αναφερόμενο να δίνει πληροφορίες για την αίτηση αναφοράς που αναφέρεται στον στόχο αναφοράς χρησιμοποιώντας τον επιβλέποντα σαν μεσάζων. Ο στόχος αναφοράς μπορεί να χρησιμοποιήσει αυτή την πληροφορία ώστε να ξέρει πότε να απορρίψει την αίτηση αναφοράς από τον διαχειριστή και πότε όχι. Αυτό επιτρέπει

στον επιβλέπων να λειτούργει σαν υποκλοπέας και να έχει την ικανότητα να ξεκινάει Mitm επιθέσεις. Παράδειγμα ο επιβλέπων μπορεί να δώσει μέσω κάποιας κεφαλίδας ψευδείς πληροφορίες στον αναφερόμενο. Ο επιβλέπων επίσης μπορεί να αντιγράψει αυτές τις πληροφορίες σε μελλοντικά άσχετα μηνύματα. Ωστόσο ο ορισμός χρησιμοποιεί ένα S/Mime μηχανισμό που δίνει τη δυνατότητα στον στόχο αναφοράς να ανιχνεύει πιθανές χειραγωγήσεις του επιβλέποντα με κάποιες κεφαλίδες, αυτή η προστασία είναι προαιρετική.

3.1.4 Επίθεση επαναπρόσκλησης

Επίθεσηεπαναπρόσκλησης: Όταν ξεκινήσει μια συνεδρία, επόμενα μηνύματα μπορούν να σταλούν ώστε να τροποποιήσουν παραμέτρους της επικοινωνίας (πχ την πόρτα). Έτσι οποιαδήποτε μη εξουσιοδοτημένη τροποποίηση από έναν επιτιθέμενο μπορεί να προκαλέσει άρνηση της υπηρεσίας.

3.1.5 Επίθεση ενημέρωσης

Επίθεση ενημέρωσης: Η μέθοδος ενημέρωσηςSip δίνει σοβαρές δυνατότητες στους χρηστές, όπως η σίγαση, η αναμονή κλήσης και συζήτηση για αλλά γνωρίσματα των συνεδριών όπως την επανάκληση. Η μόνη διαφορά είναι ότι η επανάκληση μπορεί να χρησιμοποιηθεί μόνο όταν μια σύνδεση έχει δημιουργηθεί ενώ το μήνυμα ενημέρωσης χρησιμοποιείται για να αλλάξει τις παραμέτρους πριν την τελική απάντηση στην αρχική πρόσκληση της δημιουργίας της σύνδεσης. Όμοια με τη επίθεση επαναπρόσκλησης και στην επίθεση ενημέρωσης ο επιτιθέμενος μπορεί να στέλνει πλαστά μηνύματα ενημέρωσης με σκοπό να αλλάξει τις αρχικές παραμέτρους της σύνδεσης ώστε να προκαλέσει άρνηση της υπηρεσίας.

3.1.6 Επίθεση πληροφόρησης

Επίθεση πληροφόρησης: Σε πολλές περιπτώσεις τα Sip δίκτυα χρησιμοποιούνται για να συνδέσουν ενδιάμεσα Pstn σταθμούς. Το σκεπτικό σε αυτή την περίπτωση περιλαμβάνει την χρησιμοποίηση του Sip για τηλέφωνα με σκοπό τη μεταφορά του σήματος από τον έναν σταθμό στον άλλον και αντίστροφα. Αυτή η μέθοδος

περιγράφεται σαν ένας μηχανισμός που μεταφέρει πληροφορίες σε επίπεδο εφαρμογής μέσω του δικτυού Sip και επιτρέπει μηχανισμούς διασωλήνωσης. (για να ελαχιστοποιηθούν οι εξαρτήσεις κατά τη διάρκεια της μεταφοράς, όλοι οι δρομολογητές στη διαδρομή μεταξύ δύο Ipv6 κόμβων, δε χρειάζεται να υποστηρίζουν Ipv6. Αυτός ο μηχανισμός ονομάζεται διασωλήνωση). Έχει προταθεί για πολλές λειτουργίες όπως: μεταφορά ενδιάμεσου Pstn σήματος μεταξύ πυλών Pstn, μεταφορά Dtmf ψηφίων που δημιουργούνται σε μια συνεδρία Sip, μεταφορά πληροφοριών λογαριασμού. Το κύριο μέρος ενός μηνύματος πληροφόρησης μπορεί να κρυπτογραφηθεί για λόγους ασφαλείας. Ωστόσο δεν υπάρχει καμία πρόταση για μηχανισμό ασφαλείας που θα δίνει ακεραιότητα και αυθεντικοποίηση στην μέθοδοπληροφόρησης. Κακόβουλες τροποποιήσεις της μεθόδουπληροφόρησης είναι πιθανές και μπορούν να προκαλέσουν σοβαρά προβλήματα στα επικοινωνούντα μέρη όπως μη εξουσιοδοτημένη πρόσβαση σε κλήση, λάθος χρέωση, άρνηση της υπηρεσίας στην αρχική πρόσκληση.

3.1.7 ΕπίθεσηParser

Parser ονομάζεται η διαδικασία ανάλυσης κειμένου που δημιουργεί κλειδιά ασφαλείας. Αφού το Sip είναι ένα πρωτόκολλο βασισμένο σε κείμενο πρέπει να υπάρχει και ένας έξυπνος μηχανισμός που θα αναλύει μόνο τα έγκυρα μηνύματα. Ακόμα και τέλεια δημιουργημένα να είναι αυτά τα μηνύματα υπάρχουν τρόποι που εμποδίζουν την σωστή ανάλυση τους. Παρακάτω παρατίθεται μια λίστα πιθανών σεναρίων που εμποδίζουν την ανάλυση των μηνυμάτων.

Ο επιτιθέμενος μπορεί να δημιουργήσει αχρείαστα μεγάλα μηνύματα προσθέτοντας κεφαλίδες σε συνδυασμό με πολύ μεγάλα κύρια μέρη των μηνυμάτων. Κάποια Sip μηνύματα μπορεί να έχουν κύρια μέρη, αν και αυτό δεν είναι απαραίτητο πάντα. Εκτός της επεξεργαστικής ισχύος τα μεγάλα μηνύματα ανεβάζουν και τη χρησιμοποίηση του δικτύου όπως και της μνήμης. Ο επιτιθέμενος σε αυτή την περίπτωση χρειάζεται μόνο να κάνει έξυπνες κεφαλίδες καθώς οι άλλες κεφαλίδες θα αγνοούνται από έναν κάλο Parser εξυπηρετητή. Ο εξυπηρετητής θα πρέπει να τσεκάρει τα μηνύματα για το μέγεθος τους και να απορρίπτει αυτά τα οποία ξεπερνάνε το όριο που έχει οριστεί.

Κάτω από συγκεκριμένες συνθήκες οι πελάτες στέλνουν μηνύματα χρησιμοποιώντας πρωτόκολλο αποφυγής συμφόρησης, το οποίο γενικώς οδηγεί στη χρησιμοποίηση του Tcp. Για να αποφευχθεί ο κατακερματισμός πρέπει η αίτηση να είναι μέσα στα 200 byte

του MTU η να είναι μεγαλύτερη από τα 1300 byte και να είναι άγνωστο το MTU. Ένας εξυπηρετητής με το να αποδέχεται συνδέσεις Tcp γίνεται τρωτός σε γενικές Tcp επιθέσεις άρνησης υπηρεσίας, μια πρόσθετη κατάσταση δημιουργείται ακόμα και σε διαμεσολαβητές που δεν διατηρούν ιστορικό. Ως αντίμετρο οι Sip οντότητες μπορούν να παραμετροποιηθούν ώστε να μην υποστηρίζουν Tcp μηνύματα. Αυτή η συμπεριφορά είναι εντάξει με το τρέχων Sip αλλά αναμένεται να χαθεί σε επόμενες αναμορφώσεις του πρωτοκόλλου.

Ο κακός ορισμός του parser μηχανισμού μπορεί να τον καταστήσει άχρηστο αν περνάνε μηνύματα μεγέθους τέτοιου που δεν ταιριάζουν στο μέγεθος του περιεχομένου που υποδεικνύεται στην κεφαλίδα.

Το Sip πρωτόκολλο δίνει εντολή όταν μια κεφαλίδα έχει πολλές τιμές να σπάει σε ξεχωριστές κεφαλίδες όπου η κάθε μια έχει μόνο μια τιμή. Αν πολλές κεφαλίδες μηνυμάτων του ίδιου πεδίου υπάρχουν μέσα στο μήνυμα και είναι διάσπαρτες μέσα του τότε και αυτό περιπλέκει το Parsing.

Μερικές κεφαλίδες είναι πιο σημαντικές για επεξεργασία σε σχέση με άλλες. Σημαντικές κεφαλίδες είναι αυτές που έχουν να κάνουν με την δρομολόγηση, μηνύματα με αυτά τα πεδία μπαίνουν στο τέλος του μηνύματος και είναι πιο περίπλοκα να αναλυθούν. Μια λύση για αυτό είναι να προσθέσουμε πεδία πληροφορίας πριν τα πεδία δρομολόγησης π.χ. επιτρέπεται, υποστηρίζεται.

Οι επιθέσεις ανάλυσης μπορεί να είναι έξυπνες, π.χ. αναλύοντας μόνο τα κομμάτια που χρειάζονται για τη σωστή λειτουργιά του. Ένας εξυπηρετητής που έχει υπερφορτωθεί με την ανάλυση των μηνυμάτων είναι ένδειξη κακής λειτουργίας του λογισμικού του εξυπηρετητή ή πρόβλημα υλικού. Επιπλέον το να βλέπεις το περιεχόμενο των εισερχόμενων μηνυμάτων ώστε να δεις αν υπάρχει κάτι ύποπτο θα βοηθήσει περισσότερο με αυτού του είδους τις επιθέσεις.

3.1.8 SqlInjection επίθεση

Για να διατηρήσει το Sip τα συνθηματικά των χρηστών του χρησιμοποιεί βάσεις δεδομένων όπως Mysql,Oracle. Αυτό κάνει τις υπηρεσίες του και συγκεκριμένα τη διαδικασία αυθεντικοποίησης τρωτή σε επιθέσεις γνωστές ως SqlInjection επιθέσεις.

Οι υλοποιήσεις ανοιχτού κώδικα του Sip (πχ Ser, Vovida) παρέχουν κομμάτια σχεδιαστικά με σκοπό να υποστηρίξουν σκοπούς διαχείρισης τέτοιων βάσεων δεδομένων. Αυτές οι βάσεις συγκροτούνται από πολλούς πίνακες. Ανάμεσα τους, οι πίνακες της τοποθεσίας και των συνδρομητών είναι πολύ μεγάλης σημασίας γιατί έχουν τα βασικά δεδομένα ώστε να υπάρχει ομαλή λειτουργιά του VOIP. Ο πινάκας συνδρομητών έχει τα στοιχεία των νόμιμων χρηστών ενώ ο πίνακας τοποθεσιών όλα τα ονόματα των πεδίων των συνδρομητών.

Όταν μια τέτοια επίθεση ενεργοποιείται ενάντια σε μια εγκατάσταση Sip οποιαδήποτε καταστροφή στην ακεραιότητα της βάσης ειδικά των συνδρομητών και της τοποθεσίας οδηγεί σε αστοχία της υπηρεσίας. Επιπλέον η χρησιμοποίηση Web διεπαφής για παροχή του Sip κάνει αυτή την επίθεση πιο ελκυστική στους πιθανούς επιτιθέμενους. Η SqlInjection στο Sip είναι παρόμοια με την SqlInjection στο διαδίκτυο.

Η SqlInjection στο Sip μπορεί να ξεκινάει κάθε φορά που μια δικτυακή οντότητα (Sip διαμεσολαβητής) ζητάει αυθεντικοποίηση. Όταν μια δικτυακή συσκευή ζητάει αυθεντικοποίηση η Ua για λογαριασμό του εξουσιοδοτημένου χρηστή υπολογίζει τα κατάλληλα συνθηματικά βάσει του μηχανισμού HttpDigest. Το αποτέλεσμα αυτών των συνθηματικών περιλαμβάνεται στην κεφαλίδα του μηνύματος ταυτοποίησης. Μετά το μήνυμα προωθείται στον Sip εξυπηρετητή, που πρέπει να αυθεντικοποιήσει το εισερχόμενο μήνυμα. Αυτός επαναϋπολογίζει τα συνθηματικά του χρήστη χρησιμοποιώντας τον κωδικό που υπάρχει στον πίνακα των συνδρομητών και παράγει ένα ερώτημα sql σαν το παρακάτω:

SELECT password FROM subscriber WHERE user-name='gkar' AND realm='195.251.164.23'

Όταν κάποιος πάει να κάνει μια sqlinjection υποκλέπτει το μήνυμα SIP και εισάγει τον κακόβουλο sql κώδικα στην κεφαλίδα ταυτοποίησης. Αυτό το μήνυμα μπορεί να είναι οποιοδήποτε μήνυμα που ζητάει αυθεντικοποίηση από τον SIPεξυπηρετητή. Αυτός ο κώδικας μπορεί να μπει είτε στο κυρίως μέρος του μηνύματος είτε σε άλλα πεδία της κεφαλίδας ταυτοποίησης. Μόλις ο διαμεσολαβητής λάβει ένα μήνυμα με πειραγμένη κεφαλίδα ταυτοποίησης δημιουργεί και εκτελεί την παρακάτω πρόταση sql:

SELECT password FROM subscriber WHERE user-
name='gkar';

UPDATE subscribe SET first_name=’malicius’ WHERE username=’gkar’—

Με αποτέλεσμα το μήνυμα αυθεντικοποίησης να αποτυγχάνει αλλά η δεύτερη σειρά της πρότασης να αντικαθιστά το όνομα χρήστη με τη λέξη Malicious. Είναι πιθανό ένας κακόβουλος χρήστης να προσπαθήσει με παρόμοιες προτάσεις Sql να κάνει τη βάση δεδομένων άχρηστη και να προκαλέσει άρνηση της υπηρεσίαςVoip.

Η SqlInjection επίθεση είναι ανεξάρτητη από τον τύπο της βάσης δεδομένων και από την υλοποίηση του Sipεξυπηρετητή. Ο μόνος περιορισμός έχει να κάνει με την Api που χρησιμοποιείται. Παράδειγμα η MysqlCApi 4.1 είναι αρκετά ανθεκτική σε τέτοιες επιθέσεις καθώς μια πρόταση Sql μπορεί να εκτελεστεί σε κάθε κλήση του συστήματος. Για να είναι επιτυχημένη μια τέτοια επίθεση ο μολυσμένος χρήστης (αυτός που ενεργεί για άλλον) πρέπει να έχει τα κατάλληλα δικαιώματα ταυτοποίησης ώστε να εκτελέσει την κακόβουλη πρόταση. Επιπλέον ο επιτιθέμενος μπορεί να προσπαθήσει από την αρχή να υποκλέψει τον πίνακα δικαιωμάτων του χρήστη πριν ξεκινήσει την επίθεση. Φυσικά μπορεί να περιμένει ή να προσπαθεί ενεργά μέχρι να βρει τον χρήστη που έχει τα κατάλληλα δικαιώματα. Ωστόσο οι πάροχοι Sip επιτρέπουν στους χρήστες να εγγράφονται, να αλλάζουν ή και να διαγράφουν τις τρέχουσες ρυθμίσεις τους για τη διάρκεια που χρησιμοποιούν το Sip. Αυτό σημαίνει ότι ο διαχειριστής της υπηρεσίας πρέπει να μεταφέρει τα δικαιώματα (στον Sql χρήστη που δρα για λογαριασμό του αντίστοιχου εξυπηρετητή) εισαγωγή, ενημέρωση, διαγραφή για τους κατάλληλους πίνακες στη βάση. Ως αποτέλεσμα αυτός ο περιορισμός δεν είναι αυστηρός.

3.1.9 Επιθέσεις πλημύρας

Οι επιθέσεις αυτές μπορούν να προκληθούν είτε από μια πηγή είτε από πολλές. Οι επιτιθέμενοι εκμεταλλεύονται απλούς τερματικούς σταθμούς που έχουν πρόσβαση στο διαδίκτυο, οι οποίοι δημιουργούν μεγάλο αριθμό αιτήσεων (Tcp αιτήσεις) προς τα θύματα. Αυτές οι επιθέσεις ονομάζονται αντανακλαστικές διανομές άρνησης της υπηρεσίας. Τέτοιες επιθέσεις χρησιμοποιούνται για να παραλύσουν το Sip. Παρακάτω περιγράφεται πως αυτές οι επιθέσεις μπορούν να ξεκινήσουν προς το Sip.

Πλημμύρα προς τους εξυπηρετητές εγγραφών

Ένα υλικό της Sip τηλεφωνίας είναι ο εξυπηρετητής εγγραφών. Όταν ένας επιτιθέμενος παραλύσει τον εξυπηρετητήεγγραφών, είναι εύκολο να προκαλέσει άρνηση της υπηρεσίας. Αυτό μπορεί να αποφευχθεί μόνο αν ο εξυπηρετητής εγγραφών μπλοκάρει όλα τα μηνύματα που του έρχονται από άγνωστη προέλευση. Μια αίτηση εγγραφής προσθέτει μια νέα σύνδεση μεταξύ της Sip διεύθυνσης του καλούντος και μιας ή πολλών διευθύνσεων των επαφών του (Ip διευθύνσεις) ώστε ο καλών να χρησιμοποιήσει την υπηρεσία της τηλεφωνίας. Όταν ένας επιτιθέμενος ξεκινάει μια επίθεση σε έναν εξυπηρετητή εγγραφών με την αποστολή πολλών αιτήσεων τότε θέλει να πετύχει έναν από τους παρακάτω στόχους:

i. Να βρει κωδικούς χρηστών
ii. Να προκαλέσει άρνηση της υπηρεσίας στον εξυπηρετητή εγγραφών

Ένα σενάριο επίθεσης είναι ο επιτιθέμενος να προσπαθήσει να κάνει εγγραφή σε έναν εξυπηρετητή στέλνοντας συνεχώς κάποια συνθηματικά ελαφρώς αλλαγμένα από τη μια αίτηση στην άλλη με σκοπό να βρει έναν κωδικό που ανήκει σε νόμιμο χρήστη και να προκαλέσει άρνηση της υπηρεσίας. Η διαφορά μεταξύ εγγραφής και απεγγραφής είναι η τιμή λήξης της κεφαλίδας. Η κεφαλίδα γίνεται 0 όταν ο χρήστης θέλει να τερματίσει την επικοινωνία (απεγγραφή). Με αυτόν τον τρόπο ο εισβολέας θα προσπαθήσει να αποφύγει κάτι που θα τον ανιχνεύσει. Και στις 2 περιπτώσεις ο επιτιθέμενος πρέπει να μαντέψει κάποιον κωδικό νόμιμου χρήστη.

Αυτού του είδους οι επιθέσεις μπορούν να ξεκινήσουν και με κατανεμημένο τρόπο. Παράδειγμα πολλοί επιτιθέμενοι προσπαθούν να βρουν κωδικούς νόμιμων χρηστών είτε να διαταράξουν την υπηρεσία στέλνοντας συνεχώς μηνύματα εγγραφής στον εξυπηρετητή εγγραφών, καθώς η διαδικασία ταυτοποίησης είναι υπολογιστικά ακριβή.

Πλημμύρα σε διαμεσολαβητή και σε τερματικά

Ένα από τα πιο συχνά μηνύματα που χρησιμοποιείται από τους Sip εξυπηρετητές είναι το μήνυμα της πρόσκλησης. Αυτό το μήνυμα υπάρχει για να δημιουργεί τη σύνδεση μεταξύ των επικοινωνούντων. Όταν δημιουργηθεί η σύνδεση ο Sip διαμεσολαβητής πρέπει να διατηρεί την κατάσταση της σύνδεσης. Αυτό κάνει τον εξυπηρετητή περισσότερο τρωτό σε επιθέσεις πλημμύρας. Όταν ένα μήνυμα πρόσκλησης προωθηθεί από έναν Sip διαμεσολαβητή τότε ξεκινάει ένας μετρητής που έχει ελάχιστη μέτρηση τα

3 λεπτά. Αν ο μετρητής λήξει, θεωρείται ότι ο καλούμενος δε μπορεί να απαντήσει. Όταν προωθηθεί τελικά η μη απάντηση του καλούμενου, ο εξυπηρετητής χρειάζεται ένα μήνυμα Ack ώστε να ξαναστείλει το μήνυμα του καλούντα. Στην περίπτωση που ο εξυπηρετητής έχει μια αίτηση προς παραπάνω του ενός προορισμούς, πρέπει να διατηρήσει ένα αντίγραφο του μηνύματος όπως και όλων των forked αιτήσεων. Στην περίπτωση που ο εξυπηρετητής λάβει ένα μήνυμα επαναπροώθησης, ο εξυπηρετητής μπορεί να ξεκινήσει την επαναπροώθηση μόνος του. Σε αυτή την περίπτωση ο εξυπηρετητής πρέπει να διατηρήσει την κατάσταση μέχρι να λάβει απάντηση από την επαναπροώθηση που έχει κάνει. Ο αντίστοιχος εξυπηρετητής πρέπει να ξαναστείλει μια απάντηση περιοδικά καθώς αυτό δε μπορεί να εγγυηθεί ότι όλες οι συνδέσεις είναι αξιόπιστες.

Ο επιτιθέμενος μπορεί να ξεκινήσει μια επίθεση πλημμύρας όχι μόνο χρησιμοποιώντας προσκλήσεις προς τους εξυπηρετητές αλλά και προς τους τερματικούς σταθμούς. Παράδειγμα, τα τερματικά έχουν σχεδιαστεί να απαντάνε κάτω υπό συγκεκριμένες συνθήκες, αυτό σημαίνει ότι μπορούν να διαχειρίζονται λίγα εισερχόμενα μηνύματα ταυτόχρονα. Αν πάρουμε την περίπτωση που ένας επιτιθέμενος καταφέρει να παρουσιαστεί ως νόμιμος χρήστης μπορεί πιθανώς να στείλει πολλά μηνύματα ταυτόχρονα. Σε αυτή την κατάσταση ο επιτιθέμενος δημιουργεί αιτήσεις πρόσκλησης χωρίς να περιμένει απάντηση προσπαθώντας να παραλύσει το θύμα. Επιπλέον σε αυτή την περίπτωση ο Sip διαμεσολαβητής χρησιμοποιείται από τον επιτιθέμενο ώστε να ενισχύσει τα μηνύματα αυτά.

Ένα άλλο σενάριο είναι ο επιτιθέμενος να συμπεριφέρεται ως νόμιμος χρήστης. Ο επιτιθέμενος θα δοκιμάσει διαφορετικά σενάρια προσκλήσεων ώστε να δημιουργήσει άρνηση της υπηρεσίας είτε στον διαμεσολαβητή είτε στο τερματικό προσπαθώντας να αποφύγει οποιοδήποτε μηχανισμό αναγνώρισης του. Ακόμα, ένας νόμιμος χρήστης μπορεί να ξεκινήσει αυτή την επίθεση κατά λάθος αν υπάρχει μια κακή εφαρμογή που περιέχει λάθη.

3.1.10 Επιθέσεις ενοχλητικών κλήσεων

Ο όρος ενοχλητική κλήση μπορεί να περιγράφει καλύτερα σαν ένας συνδυασμός κλήσεων τηλέ-προώθησης και ενοχλητικών μηνυμάτων. Η ενοχλητική κλήση λειτουργεί με την ίδια λογική που λειτουργεί και η ενοχλητική αλληλογραφία, επιτρέποντας για

παράδειγμα εγγεγραμμένες κλήσεις 30 δευτερολέπτων να στέλνονται σε χιλιάδες Ip διευθύνσεις μέσα σε ελάχιστα δευτερόλεπτα. Ωστόσο σε αντίθεση με τα μηνύματα ηλεκτρονικού ταχυδρομείου που μπορεί κάποιος να τα σταματήσει και να αναλύσει το περιεχόμενο του, [13] η αναγνώριση και ο προσδιορισμός ενός ήχου σαν ενοχλητικό είναι πολύ δύσκολο έργο για έναν υπολογιστή.

Επίσης και από την πλευρά του χρήστη, η ενοχλητική κλήση είναι διαφορετικό από την ενοχλητική αλληλογραφία ηλεκτρονικού ταχυδρομείου. Ένα ενοχλητικό μήνυμα ηλεκτρονικού ταχυδρομείου εφόσον παραληφθεί είναι εύκολο να σβηστεί. Είναι όμως κακό αν κάποιο συνηθισμένο μήνυμα από κάποιον φίλο κατηγοριοποιηθεί σαν ενοχλητικό και δεν παραδοθεί. Αυτό όμως είναι ανεκτό αν ένα φίλτρο έχει λίγες αστοχίες στην κατηγοριοποίηση των έγκυρων μηνυμάτων σαν ενοχλητικά αλλά αποφεύγει εντελώς την κατηγοριοποίηση σαν έγκυρων, μηνυμάτων που είναι ενοχλητικά.

Τα πράγματα είναι διαφορετικά στις ενοχλητικές κλήσης. Η λήψη ενός ενοχλητικού μηνύματος συχνά σημαίνει ότι το τηλέφωνο χτυπάει, πιθανώς ξυπνώντας τον χρήστη μέσα στη νύχτα. Από την άλλη πλευρά αν ένας φίλος καταλάβει ότι η κλήση του δεν προωθείται, αναγνωρίζει ότι έχει φιλτραριστεί η κλήση και προσπαθεί ξανά, πιθανώς χρησιμοποιώντας διαφορετικό κανάλι επικοινωνίας.

Η ενοχλητική κλήση είναι δεδομένο ότι θα γίνει το κυρίαρχο μέσο για τους κακόβουλους χρήστες λόγω του χαμηλού του κόστους. Μόλις ένας Ip τηλεφωνικός αριθμός γίνει γνωστός δημόσια, αυτό μπορεί να αποτελέσει μία σοβαρή απειλή για την ιδιωτικότητα των χρηστών. Ένας χρήστης μπορεί παράλληλα να δημιουργήσει και να εγκαθιδρύσει έναν μεγάλο αριθμό κλήσεων. Αν μία κλήση πρέπει να συνδεθεί, ο χρήστης δημιουργεί μία επιβεβαίωση και προωθεί την έναρξη της τηλε-προώθησης, μετά τερματίζει την κλήση. Οι μηχανισμοί προστασίας προσωπικών δεδομένων παρέχουν τις κατευθυντήριες γραμμές για τη δημιουργία των μηνυμάτων που δεν αποκαλύπτουν στοιχεία ταυτότητας, ωστόσο στην Ip τηλεφωνία όπως και στην παραδοσιακή όταν ένας χρήστης είναι αναγνωρίσιμος με κάποια μέσα (ψευδώνυμο) η ταυτότητα μπορεί να διανεμηθεί χωρίς τη συγκατάθεση του ιδιοκτήτη.

3.2 Επιθέσεις παρακολούθησης της κίνησης του δικτύου

3.2.1 Υποκλοπήκαιεπίθεση παρεμβολής κακόβουλου χρήστη ενδιάμεσα στην επικοινωνία

Επειδή το Voip [04] είναι μία εφαρμογή που εκτελείται πάνω στο Ip είναι ευαίσθητο σε πολλές γνωστές επιθέσεις του διαδικτύου και των εφαρμογών του. Για παράδειγμα οι Voip εξυπηρετητές μπορεί να είναι τρωτοί σε επιθέσεις άρνησης της υπηρεσίας και η κίνηση του Voip μπορεί να διακόπτεται ή να παραπλανείτε από επιθέσεις εισβολής και διαταραχής του DNSCache. Παρακάτω θα δούμε παραδείγματα επιθέσεων που βασίζονται σε τρωτά σημεία που κληρονομούνται από το Ip, θα θεωρήσουμε ότι υπάρχει ένας ενεργός επιτιθέμενος στην Voip σηματοδοσία ή στη διαδρομή μετάδοσης των δεδομένων που μπορεί να παρακολουθήσει, αλλάξει, ακυρώσει ή ακόμα και να υποκλέψει την κίνηση του Voip. Θα εστιάσουμε στις επιθέσεις που στοχεύουν τερματικά συστημάτων Voip που χρησιμοποιούν το Sip αντί της υποδομής Sip. Αυτές οι επιθέσεις συνήθως δεν επηρεάζουν αλλά τερματικά και Voip εξυπηρετητές αλλά είναι δύσκολο να ανιχνευθούν από τους παρόχους Voip. Παρόλα αυτά δημιουργούν πολλές απειλές σε εκατομμύρια συνδρομητές Voip.

Ειδικότερα, μελετάται μία νέα επίθεση εναντίον Voip χρηστών. Την VoicePharmingAttack, η οποία επηρεάζει τα θύματα και χωρίζει τις κλήσεις σε ψεύτικες και αληθινές. Οι επιθέσεις Phising,Pharming, VoicePhising, voicePharming στοχεύουν να παραπλανήσουν τα θύματα ώστε να δώσουν εμπιστευτικές πληροφορίες στον επιτιθέμενο. Όπως το VoicePhising έτσι και το VoicePharming εκμεταλλεύεται την εμπιστοσύνη των ανθρώπων στις επικοινωνίες ήχου.

Η VoicePharming επίθεση εκμεταλλεύεται ουσιαστικά την εμπιστοσύνη των ανθρώπων ότι η κλήση τους θα φτάσει στον σωστό καλούμενο εφόσον έχουν καλέσει τον σωστό αριθμό. Αν ο επιτιθέμενος με κάποιο τρόπο εκτρέψει την κλήση σε κάποια συσκευή που αυτός έχει επιλέξει, όλοι οι χρήστες Voip είναι ευάλωτοι σε κλοπές ταυτότητας και σε οικονομική ζημιά λόγο της VoicePharming επίθεσης. Άρα είναι σημαντικό να εξεταστεί αν οι κλήσεις που γίνονται μέσω των υπαρχόντων συστημάτων Voip μπορούν να εκτραπούν από τους επιτιθέμενους.

Παίρνοντας τον ρόλο ενός επιτιθέμενου αναζητούνται τα τρωτά σημεία στη Voip σηματοδοσία και στα πρωτόκολλα μεταφοράς που μπορεί να ενεργοποιήσουν επιθέσεις εκτροπής επιλεγμένων Voip κλήσεων.

Παρατηρείται ότι τα Sip μηνύματα δεν μπορούν να κρυπτογραφηθούν από το ένα άκρο στο άλλο λόγο της ανάγκης να επιτρέπεται από τους ενδιάμεσους Sip δρομολογητές να αλλάζουν/προσθέτουν πεδία στα Sip μηνύματα. Αυτό κάνει την σηματοδοσία Sip τρωτή σε επιθέσεις ενδιάμεσου κακόβουλου χρήστη, όπου ο επιτιθέμενος μπορεί να διαβάσει και να αλλάξει αν θέλει τα Sip μηνύματα που ανταλλάσσονται μεταξύ δύο μερών χωρίς κανένα από τα δύο μέρη να γνωρίζει ότι βρίσκεται σε κίνδυνο.

Μεταξύ όλων των ενδιάμεσων κόμβων στο μονοπάτι της Sip σηματοδοσίας, η σύνδεση μεταξύ των τερματικών Sip και των ενδιάμεσων Sip δρομολογητών είναι η πιο αδύναμη λόγω του ότι ενώ ο ορισμός του Sip απαιτεί χρήση Tls μεταξύ των ενδιάμεσων δρομολογητών, δεν απαιτεί κρυπτογράφηση από τα τερματικά. Άρα η σηματοδοσία μεταξύ τερματικών και εξυπηρετητών γίνεται μέσω απλού κειμένου. Επίσης συνήθως ένα τερματικό είναι αρκετά μακριά από τους ενδιάμεσους Sip εξυπηρετητές, αυτή η μεγάλη απόσταση μέσα στο δημόσιο διαδίκτυο δίνει τη δυνατότητα στους επιτιθέμενους να επιχειρήσουν πολλές επιθέσεις σε όλο αυτό το μεγάλο μονοπάτι μεταξύ των τερματικών και των εξυπηρετητών. Τέλος, ένας Sip χρήστης μπορεί εύκολα να αλλάξει την τοποθεσία του και την Ip διεύθυνση του. Αυτό δίνει τη δυνατότητα σε ενδιάμεσους κακόβουλους χρήστες να δημιουργήσουν πλαστά μηνύματα και αυτό κάνει δυσκολότερο τους εξυπηρετητές να αναγνωρίσουν αυτά τα πλαστά μηνύματα. Με την εγκατάσταση ενός δρομολογητή σε δημόσιες περιοχές (αεροδρόμια, βιβλιοθήκες) από κάποιον κακόβουλο χρήστη μπορεί πολύ εύκολα να ξεκινήσουν επιθέσεις ενδιάμεσου κακόβουλου χρήστη.

Τώρα ας δούμε πώς μία κλήση μπορεί να εκτραπεί από κάποιον επιτιθέμενο μέσω μίας συσκευής που αυτός θα διαλέξει. Ο στόχος της απομακρυσμένης εκτροπής είναι να εκτρέψει μία Rtp ηχητική ροή μιας επιλεγμένης κλήσης μέσω ενός άλλου κόμβου που ο επιτιθέμενος έχει επιλέξει πριν αυτή η ροή φτάσει στον τελικό προορισμό της.

Κατά τη διάρκεια της ρύθμισης μίας κλήσης Sip ο καλών και ο καλούμενος μπορούν να διαλέξουν που θα δεχτούν την Rtp ηχητική ροή και ο καθένας ενημερώνει το άλλο μέρος της επικοινωνίας μέσω του μηνύματος πρόσκλησης και του OK μηνύματος. Οι πληροφορίες των τερματικών για το Rtp καθορίζονται στο Sdp μέρος του μηνύματος πρόκλησης και του OK μηνύματος που δεν προστατεύονται από τον SipDigestAuthentication μηχανισμό, ο επιτιθέμενος είναι ελεύθερος να παραποιήσει τις Rtp πληροφορίες των τερματικών. Για λόγους απόδοσης κάποιοι πάροχοι Voip μπορεί να επιλέγουν διαφορετικούς εξυπηρετητές για τη σηματοδοσία Sip και διαφορετικούς

για τη μετάδοση της Rtp ηχητικής ροής. Συνεπώς μια Sip συσκευή αρχικοποιεί την Rtp ροή στην Ip διεύθυνση και στην θύρα που έχει καθοριστεί στο Sdp μέρος του μηνύματος πρόσκλησης και του OK μηνύματος. Από την άλλη πλευρά, ο Sip εξυπηρετητής μπορεί να θυμάται την IP διεύθυνση οποιασδήποτε εγγεγραμμένης συσκευής Sip. Ωστόσο ο Sip εξυπηρετητής δε μπορεί να απαιτήσει ώστε η ροή να αποσταλεί στην εγγεγραμμένη Ip λόγο της ανάγκης να υποστηρίζονται οι Sip συσκευές πίσω από το NAT. Όλα τα παραπάνω βοηθούν έναν ενδιάμεσο κακόβουλο χρήστη να εκτρέψει όποια Rtp ηχητική ροή επιλέξει μέσω μίας απομακρυσμένης συσκευής.

3.2.2 Ανακατεύθυνση (υποκλοπή εισερχόμενης και εξερχόμενης κλήσης) μιας επιλεγμένης Voip κλήσης

Αποτέλεσμα μιας τέτοιας ανακατεύθυνσης είναι ο καλών να νομίζει ότι είναι συνδεδεμένος με τον καλούμενο αλλά αυτός να είναι συνδεδεμένος με κάποιο άλλο μέρος που έχει επιλεγεί από τον επιτιθέμενο. Από την άλλη, ο αυθεντικός καλούμενος δεν έχει λάβει ποτέ την κλήση. Στην ανακατεύθυνση από την πλευρά του καλούμενου όταν αυτός πρόκειται να δεχτεί μία κλήση, ο καλών για να την αρχικοποιήσει στέλνει ένα μήνυμα πρόσκλησης και στο πεδίο Requested-URI φαίνεται ποιον θέλει να καλέσει, όπως έχουμε αναφέρει όμως, αυθεντικοποίηση με τον Digest μηχανισμό δεν υπάρχει ανάμεσα στον εξυπηρετητή και την Sip συσκευή, οπότε ελεύθερα ένας επιτιθέμενος μπορεί να αλλάξει αυτό το πεδίο και η κλήση να ανακατευθυνθεί σε άλλο μέρος και όχι στον πραγματικό καλούμενο. Από την πλευρά του καλούντα επίσης μπορεί να υπάρξει τέτοια επίθεση, σε αυτή την περίπτωση ο επιτιθέμενος προσποιείται τον εξυπηρετητή και ανταλλάσει πλαστά μηνύματα με τον καλούντα.

3.2.3 Χειραγώγηση στην ρύθμιση για την προώθηση της κλήσης

Η προώθηση κλήσης είναι μία δυνατότητα που έχουν οι συνδρομητές για να δηλώσουν που θα δέχονται τις εισερχόμενες κλήσεις. Π.χ. ενώ λείπουν από το γραφείο οι κλήσεις να προωθούνται στο κινητό τους τηλέφωνο. Σε αντίθεση με τις προηγούμενες επιθέσεις αυτές εκμεταλλεύονται τα τρωτά σημεία στην ροή δεδομένων και όχι στη σηματοδοσία των πρωτοκόλλων. Επιπλέον αυτές οι επιθέσεις μπορούν να πετύχουν ακόμα και σε εντελώς προστατευμένη Voip σηματοδοσία. Ένας χρήστης π.χ. πληκτρολογώντας το

αριθμό 72 θέλει να κάνει προώθηση των κλήσεων που δέχεται ο συγκεκριμένος αριθμός σε κάποιον άλλον, μετά την πληκτρολόγηση του 72 πληκτρολογεί τον αριθμό στον οποίο θέλει να προωθούνται οι κλήσεις. Αυτός ο αριθμός μεταφέρεται μέσω Rtp πακέτων στον Rtp εξυπηρετητή, μόλις παραλάβει ο εξυπηρετητής τον αριθμό που θα γίνεται η προώθηση ζητάει επιβεβαίωση από τον χρήστη και αμέσως αρχίζει η εφαρμογή της προώθησης.

Υποθέτοντας ότι ο ενδιάμεσος κακόβουλος χρήστης είναι μεταξύ του εξυπηρετητή και της συσκευής, μπορεί να αλλάξει τον αριθμό που θα γίνεται η προώθηση και να παραπλανήσει τον συνδρομητή ο οποίος πιστεύει ότι η προώθηση θα γίνεται στον αριθμό που έχει δηλώσει.

3.3 Επιθέσεις κατάχρησης της υπηρεσίας

3.3.1 Χειραγώγηση της εγγραφής

Το RFC [05] προτείνει στους εξυπηρετητές να υποστηρίζουν ξεχωριστές αιτήσεις για κατάργηση της εγγραφής του χρήστη. Αυτό βοηθάει επιτρέποντας τους πελάτες να ενημερώνουν τις πληροφορίες της κατάστασης τους και της τοποθεσίας τους στους εξυπηρετητές σε πραγματικό χρόνο. Κατά τη διάρκεια της ενημέρωσης ο εξυπηρετητής μπορεί να αναφέρει στον καλούντα ότι ο καλούμενος δεν είναι διαθέσιμος και να αποφευχθεί η αχρείαστη αποστολή πακέτων. Επιπλέον ο εξυπηρετητής μπορεί να ελευθερώσει πόρους του σβήνοντας πληροφορίες που αφορούν αποσυνδεδεμένους χρήστες.

Ωστόσο όπως θα δούμε αυτός ο μηχανισμός δημιουργεί νέες προϋποθέσεις επιθέσεων. Η ιδέα των επιθέσεων είναι ότι υποκλέπτοντας ένα μήνυμα κατάργησης μιας εγγραφής καταργεί αυτόν τον χρήστη από τον εξυπηρετητή και πλέον αυτός ο χρήστης δε μπορεί να δεχτεί κλήσεις. Αυτός ο χρήστης όχι μόνο παύει να είναι εγγεγραμμένος στον εξυπηρετητή αλλά δε λαμβάνει καμία ειδοποίηση από τον εξυπηρετητή για αυτή την κατάργηση, οπότε νομίζει ότι είναι ακόμη εγγεγραμμένος.

Όπως βρέθηκε, η ρίζα αυτού του προβλήματος είναι η λανθασμένη υλοποίηση του RFC ή οι απαιτήσεις του RFC δεν είναι αρκετά ασφαλείς όσο αναφορά την κατάργηση της εγγραφής των χρηστών.

Παρακάτω παρουσιάζεται μία τέτοια επίθεση: αρχικά ένας πελάτης εγγράφεται σε διαφορετικούς εξυπηρετητές και με διαφορετικές ρυθμίσεις ο καθένας (είτε με υποστήριξη αυθεντικοποίησης είτε χωρίς). Στη συνέχεια ένας επιτιθέμενος προσπαθεί να καταργήσει τον εγγεγραμμένο πελάτη από τον εξυπηρετητή. Μετά την επίθεση γίνεται προσπάθεια να κληθεί το θύμα από κάποιον τρίτο πελάτη. Αυτό επαναλαμβάνεται αρκετές φορές για κάθε διαφορετική ρύθμιση των εξυπηρετητών ώστε να βγουν συμπεράσματα.

3.3.2 Το πρόβλημα της κατάργησης της εγγραφής ενός πελάτη

Η ευκολία της επίθεσης αυτής πηγάζει από την ιδιότητα ότι το Sip εκτελείται πάνω στο Udp, που σημαίνει ότι δεν χρειάζεται τα δύο μέρη να έχουν εγκαταστήσει μία συνεδρία πριν αποστείλουν δεδομένα. Οι αδυναμίες που παρουσιάζονται παρακάτω κατατάσσονται σε δύο κατηγορίες. Η πρώτη κατηγορία έχει να κάνει με λάθη στην υλοποίηση των Sip εξυπηρετητών ή παραλήψεις στο Sip RFC οι οποίες επιτρέπουν μη ασφαλείς εφαρμογές. Η δεύτερη κατηγορία έχει να κάνει με θέματα στα οποία δεν προτείνει λύση το RFC. Αυτό εμφανίζεται όταν ο επιτιθέμενος μπορεί να καταλάβει την κίνηση μεταξύ του πελάτη και του εξυπηρετητή.

Επίθεση κατάργησης της εγγραφής χωρίς τη γνώση της κίνησης και χωρίς ο εξυπηρετητής να υποστηρίζει αυθεντικοποίηση:

Οι Call-Id και Cseq κεφαλίδες στο μήνυμα κατάργησης της εγγραφής πρέπει να αντιστοιχούν στις ίδιες κεφαλίδες του αυθεντικού μηνύματος εγγραφής. Ωστόσο κανένας από τους εξυπηρετητές που έγινε έλεγχος δεν έκανε αυτό τον έλεγχο. Η επίθεση πέτυχε να καταργήσει την εγγραφή του πελάτη από τον εξυπηρετητή εύκολα, απλά στέλνοντας ένα μήνυμα εγγραφής με τιμής λήξης 0 και τυχαίες τιμές Call-Id και Cseq. Επιπλέον καταφέραμε να πλαστογραφήσουμε ένα ψεύτικο μήνυμα εγγραφής σαν νόμιμοι χρήστες μαζί με το όνομα και το τηλέφωνο του θύματος.

Για την επίθεση αυτή χρειάστηκαν μόνο βασικές δημόσιες πληροφορίες (το τηλέφωνο του θύματος και το ψευδώνυμο του) και πληροφορίες που μπορούν να βρεθούν στέλνοντας πακέτα στον εξυπηρετητή και λαμβάνοντας τις απαντήσεις του. Η Ip διεύθυνση μπορεί να βρεθεί με την εγκαθίδρυση μιας κλήσης με τον πελάτη. Ακόμα και

αν ο χρήστης είναι πίσω από NAT ή από κάποιο VOIP-Awareανάχωμαασφαλείας και ο επιτιθέμενος είναι σε άλλο δίκτυο, υπάρχουν κάποια πεδία που δείχνουν την πραγματική Ip του θύματος και δεν αλλάζουν στο πακέτο. Κάποιοι εξυπηρετητές κρύβουν αυτές τις πληροφορίες και σε αυτή την περίπτωση είναι αδύνατο να υποκλαπεί το πακέτο χωρίς να έχει βρεθεί η Ip του χρήστη.

Επίθεση κατάργησης της εγγραφής με γνώση της κίνησης σε εξυπηρετητή χωρίς αυθεντικοποίηση

Σε αυτή την περίπτωση το RFC δεν προτείνει κάποια λύση. Η σωστή υλοποίηση του RFC δε θα βοηθήσει καθώς ο επιτιθέμενος μπορεί να βρει το Call-Id και το Cseq και έτσι μπορεί να υποκλέψει το πακέτο με όλα τα απαραίτητα πεδία.

Επίθεση κατάργησης της εγγραφής με γνώση της κίνησης σε εξυπηρετητή με αυθεντικοποίηση.

Προκαλεί έκπληξη αλλά ακόμα και σε εξυπηρετητή με αυθεντικοποίηση η επίθεση κατήργησε την εγγραφή χωρίς να γνωρίζει τον κωδικό. Αυτό συνέβη γιατί μπορούσε να ελεγχθεί η κίνηση μεταξύ του πελάτη και του εξυπηρετητή. Αν και η αυθεντικοποίηση από μόνη της είναι ασφαλής ωστόσο ελέγχθηκε η πρόσκληση που έστειλε ο εξυπηρετητής και η απάντηση του πελάτη που ήταν και η πιο σημαντική. Όταν ο εξυπηρετητής χρησιμοποιεί αυθεντικοποίηση αρκεί στον επιτιθέμενο να πιάσει το τελευταίο μήνυμα εγγραφής που έχει σταλεί από τον πελάτη και να πάρει το κείμενο που έχει την πιστοποίηση. Με τη χρήση του ίδιου κειμένου, καταργήθηκε η εγγραφή του πελάτη επιτυχημένα.

Αυτό το πρόβλημα δεν έχει να κάνει με το Sip καθώς φαίνεται ότι είναι σφάλμα στον εξυπηρετητή. Ωστόσο το RFC δεν αντιμετωπίζει την επανάληψη των απαντήσεων της αυθεντικοποίησης, περιμέναμε ότι ο εξυπηρετητής δε θα επέτρεπε την επαναχρησιμοποίηση της απάντησης του (κρυπτογραφημένο κείμενο) και θα απέρριπτε το πακέτο που είχε υποκλαπεί.

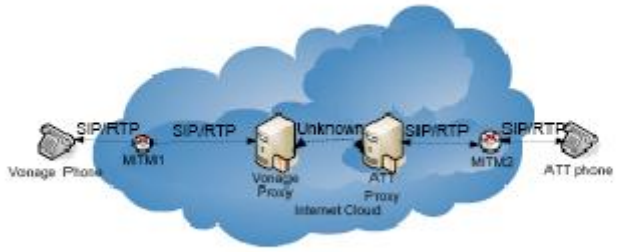
3.3.3 Μη εξουσιοδοτημένη χρήση

Η ByeDelaybilling επίθεση [14] επιδιώκει να παρατείνει την διάρκεια των κλήσεων μεταξύ συνδρομητών Voip καθυστερώντας τα μηνύματατερματισμού. Ο καλών ή ο καλούμενος όταν κλείνει και στέλνει ένα μήνυμα τερματισμού στον Sipεξυπηρετητή, με μία επίθεσηενδιάμεσου κακόβουλου χρήστη υποκλέπτεται το μήνυμα τερματισμού και στέλνει πίσω ένα OK μήνυμα. Αυτό δίνει την εντύπωση στον καλούντα ή στον καλούμενο ότι η κλήση έχει τερματιστεί επιτυχώς ενώ ο ενδιάμεσος κακόβουλος χρήστης έχει πάρει τον έλεγχο της κλήσης. Μετά ο ενδιάμεσος κακόβουλος χρήστης 1 και ο ενδιάμεσος κακόβουλος χρήστης 2 δημιουργούν ψεύτικες Rtp ροές και τις στέλνουν στους αντίστοιχους εξυπηρετητές. Αυτό δίνει την εντύπωση στους παρόχους ότι ο καλούντας και ο καλούμενος είναι ακόμα ενεργοί και έτσι παρατείνουν την κλήση χρεώνοντας κανονικά.

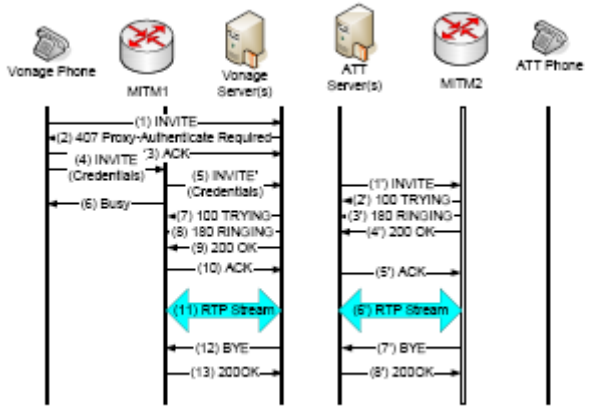
Η ByeDropbilling επίθεση επιδιώκει να παρατείνει την διάρκεια των κλήσεων μεταξύ συνδρομητών Voip απλά απορρίπτοντας τα μηνύματα τερματισμού. Όπως και στη ByeDelaybilling επίθεση ο ενδιάμεσος κακόβουλος χρήστης υποκλέπτει το μήνυμα τερματισμού και στέλνει πίσω ένα OK μήνυμα το οποίο δίνει την εντύπωση στον καλούντα ή στον καλούμενο ότι η κλήση έχει τερματιστεί επιτυχώς ενώ οι ενδιάμεσοι κακόβουλοι χρήστες έχουν πάρει τον έλεγχο της κλήσης.

Η InviteReplayBilling επίθεση έχει ως στόχο να πραγματοποιήσει μη εξουσιοδοτημένες κλήσεις με επαναλαμβανόμενη αποστολή αιτήσεων πρόσκλησης που έχουν υποκλαπεί. Τέτοιες επιθέσεις χρέωσης εκμεταλλεύονται λάθη της εφαρμογής του: αντί της επανάληψης μηχανισμού αυθεντικοποίησης Sip, ακόμα και αν τα μηνύματα πρόσκλησης προστατεύονται από αυθεντικοποίηση Sip. Ο ενδιάμεσος κακόβουλος χρήστης που είναι μεταξύ ενός AT&TSIP τηλεφώνου και ενός AT&TSip εξυπηρετητή μπορεί να παρακολουθεί και να υποκλέψει όλα τα Sip μηνύματα που στέλνονται από ένα AT&TSip τηλέφωνο. Ο ενδιάμεσος κακόβουλος χρήστης μπορεί να στείλει τα μηνύματα πρόσκλησης που έχει υποκλέψει σε έναν άλλον επιτιθέμενο ο οποίος μπορεί να κάνει μη εξουσιοδοτημένες Sip κλήσεις στέλνοντας επαναλαμβανόμενα αλλαγμένα μηνύματα πρόσκλησης. Ο ενδιάμεσος κακόβουλος χρήστης μπορεί να υποκλέπτει τα μηνύματα πρόσκλησης που περιέχουν τα διαπιστευτήρια αυθεντικοποίησης και να τα στέλνει σε έναν απομακρυσμένο ενεργό επιτιθέμενο. Ο απομακρυσμένος επιτιθέμενος μπορεί να τροποποιήσει ελεύθερα τις παραμέτρους της συνεδρίας Rtp (π.χ. την IP και την θύρα) που καθορίζονται στο Sdp μέρος του μηνύματος πρόσκλησης δεδομένου ότι

αυτό δεν προστατεύεται από αυθεντικοποίηση Sip. Στη συνέχεια ο επιτιθέμενος μπορεί να ξεκινάει επανειλημμένες InviteReplayBilling επιθέσεις μέσω της αποστολής επαναλαμβανόμενων τροποποιημένων μηνυμάτων πρόσκλησης. Έτσι εγκαθιδρύεται μία κλήση μεταξύ του επιτιθέμενου και ενός Sip εξυπηρετητή. Στη συνέχεια ο επιτιθέμενος και ο Sip διαμεσολαβητής ανταλλάσουν μεταξύ τους ροές Rtp σύμφωνα με τις παραμέτρους της συνεδρίας που έχουν συμφωνηθεί και καθορίζονται στα μηνύματα πρόσκλησης και στα OK μηνύματα. Τώρα ο επιτιθέμενος μπορεί είτε να μιλάει με τον καλούμενο είτε να αναπαραγάγει ένα ηχητικό μήνυμα.



Εικόνα 6. ΕγκατάστασηδικτύουσεFakeBusy-billing, ByeDelay-billingκαιByeDrop-billingεπιθέσεις



Εικόνα 7. Ροή μηνυμάτων στην FakeBusy-billing επίθεση

Η FakeBusyBilling επίθεση υποκλέπτει κυρίως Voip κλήσεις από στοχευόμενους Voip συνδρομητές και ελέγχει την διάρκεια της κλήσης. Σαν αποτέλεσμα αυτό έχει η κλήση που προσπαθεί να κάνει ο συνδρομητής να αποτυγχάνει αλλά να χρεώνεται ανάλογα με

τη διάρκεια που ορίζει ο επιτιθέμενος. Η Εικόνα 7 δείχνει την εγκατάσταση του δικτύου των FakeBusyBilling επίθεση, ByeDelayBilling επίθεση και ByeDropBilling επίθεση. Υπάρχουν 2 ενδιάμεσοι κακόβουλοι χρήστες, ο ένας ανάμεσα στο τηλέφωνο Sip και στον εξυπηρετητή Sip στο ένα άκρο της επικοινωνίας και ο άλλος ανάμεσα στο τηλέφωνο Sip και στον εξυπηρετητή Sip στο άλλο άκρο της επικοινωνίας. Η εικόνα 7 δείχνει τη ροή μηνυμάτων σε μία FakeBusyBillingεπίθεση όταν ένα σταθερό τηλέφωνο καλεί ένα κινητό, το δεξιά και το αριστερά μέρος δείχνει την ροή μηνυμάτων από την πλευρά του καλούντα και την πλευρά του καλούμενου αντίστοιχα. Σημειώνεται ότι το μονοπάτι της σηματοδοσίας με το μονοπάτι της Rtp ροής δεν είναι απαραίτητα το ίδιο. Χρησιμοποιείται Sip εξυπηρετητής για τη σηματοδοσία και διαμεσολαβητής για την Rtp ροή. Στα βήματα 1-4 ο καλών αυθεντικοποιεί το μήνυμα πρόσκλησης στον εξυπηρετητή Sip. Στο βήμα 4 ο ενδιάμεσος κακόβουλος χρήστης1 υποκλέπτει το μήνυμα πρόσκλησης με αυθεντικοποίηση των συνθηματικών και αλλάζει την Ip και την θύρα της Rtp ροής με τα δικά του στοιχεία. Στο βήμα 5, ο ενδιάμεσος κακόβουλος χρήστης1 στέλνει το αλλαγμένο μήνυμα στον Sip εξυπηρετητή. Μόλις ο εξυπηρετητής λάβει το μήνυμα ενημερώνει τον Sip εξυπηρετητή για τις κινητές συσκευές ότι μία σταθερή συσκευή θέλει να καλέσει την κινητή συσκευή. Εντωμεταξύ ο ενδιάμεσος κακόβουλος χρήστης1 στέλνει ένα μήνυμα απασχολημένου στον καλούντα που θα κάνει τον καλούντα να πιστεύει ότι ο καλούμενος έχει ανοιχτή γραμμή.

Στο βήμα 1 ο Sip εξυπηρετητής κινητών συσκευών στέλνει ένα μήνυμα πρόσκλησης στον καλούμενο. Ο ενδιάμεσος κακόβουλος χρήστης 2 υποκλέπτει το μήνυμα και απαντάει με τα μηνύματα TRYING, RINGING και 200 OK. Ο ενδιάμεσος κακόβουλος χρήστης 2 ορίζει την δική του Ip και την δική του θύρα στο 200 OK μήνυμα. Αυτό θα κάνει τον εξυπηρετητή κινητών συσκευών να στείλει την Rtp ροή στον ενδιάμεσο κακόβουλο χρήστης2 και όχι στην κινητή συσκευή. Ο Sip εξυπηρετητής σταθερών συσκευών τότε στέλνει TRYING, RINGING και 200 OK στον ενδιάμεσο κακόβουλο χρήστη 1. Τώρα η IP και η θύρα υπάρχουν στον εξυπηρετητή Rtp. Ο ενδιάμεσος κακόβουλος χρήστης1 απαντάει με ένα Ack μήνυμα στον Sip εξυπηρετητή σταθερών συσκευών. Ανάλογα ο εξυπηρετητής Sip κινητών συσκευών στέλνει ένα ACK μήνυμα στον ενδιάμεσο κακόβουλο χρήστη2. Τώρα η κλήση έχει ρυθμιστεί επιτυχημένα μεταξύ τουενδιάμεσου κακόβουλου χρήστη1 και του ενδιάμεσου κακόβουλου χρήστη2 και ο πάροχος Voip ξεκινάει να μετράει το χρόνο της κλήσης.

Κεφάλαιο 4

ΜηχανισμοίΑνίχνευσης-Αντιμετώπισης-Αποφυγής Επιθέσεων VOIP

4.1 Μηχανισμοί ανίχνευσης επιθέσεων

Η διαδικασία ανίχνευσης [06] των ενοχλητικών κλήσεωνVOIP δεν αφορά μόνο μία τεχνική ανίχνευσης. Η ανίχνευση απαιτεί τη χρήση διαφόρων τεχνικών σε διαφορετικά στάδια. Σε κάθε στάδιο η διαδικασία ανίχνευσης ενοχλητικών κλήσεωνεξαλείφει τις περισσότερεςενοχλητικές κλήσεις και οποιοδήποτε μεταγενέστερο που περνάει ή προωθείται εξαλείφεται σε επόμενο στάδιο. Οι τεχνικές που χρησιμοποιούνται σε κάθε στάδιο θα καθορίσουν την ενοχλητική συμπεριφορά της κλήσης και με την διαθέσιμη επανατροφοδότηση από τον κληθέντα η κλήση είτε θα σταματήσει είτε θα προωθηθεί στον κληθέντα. Το βασικό κριτήριο από το οποίο εξαρτάται πως θα επεξεργαστεί η κλήση είναι πως έχει οριστεί κάποια παρόμοια κλήση στο παρελθόν, σαν ενοχλητική ή σαν νόμιμη.

4.1.1 Δομικά στοιχεία στην ανίχνευση ενοχλητικών φωνητικών κλήσεων

Αντίληψη για τον καλούντα: κάθε φορά που λαμβάνουμε μία κλήση σηκώνουμε το τηλέφωνο βασιζόμενοι στο τι σκεφτόμαστε για την κλήση αυτή. Άρα ο ορισμός μιας ανεπιθύμητης κλήσης εξαρτάται από το τι σκεφτόμαστε για την κλήση αυτή. Ένα παράδειγμα εκτίμησης της κατάστασης της σκέψης μας είναι να συγχρονιστεί το σύστημα με ένα προσωπικό ημερολόγιο. Η διαδικασία φιλτραρίσματος που λαμβάνει χώρα σε αυτό το στάδιο βασίζεται σε στατικούς/δυναμικούς κανόνες (όπως οι κανόνες ενός αναχώματος προστασίας).

Οριακές τιμές: Βασίζονται σε γνωστά μοντέλα κίνησης, υπογραφές μπορούν να χρησιμοποιηθούν για να ανιχνεύσουν τις τιμές των εισερχόμενων κλήσεων. Παράδειγμα, η ταχύτητα και η επιτάχυνση των ληφθέντων κλήσεων από έναν χρήστη μπορεί να χρησιμοποιηθεί σαν μηχανισμός ανίχνευσης. Όταν οι τιμές αυτών των δύο φτάσουν σε ένα συγκεκριμένο όριο, η τιμής απόρριψης μπορεί να ενημερωθεί μέσω του ελέγχου ανατροφοδότησης. Όπως αναμένεται όσο πιο γρήγορα ανιχνευθέι μία αλλαγή στην εισερχόμενη κίνηση τόσο γρηγορότερα θα υπάρξει μείωση της εξάπλωσης των ανεπιθύμητων κλήσεων.

Μαύρες και λευκές κλήσεις: Οι περισσότερες από τις ανιχνεύσεις ανεπιθύμητων κλήσεων γίνεται με τη χρήση συνόλων από έγκυρες και μη έγκυρες υπογραφές. Αυτές οι υπογραφές κάνουν τον εξυπηρετητή ανίχνευσης ανεπιθύμητων κλήσεων να ξέρει ποιες κλήσεις πρέπει να προωθήσει και ποιες πρέπει να μπλοκάρει. Αυτός είναι ο τρόπος που οι κλήσεις επιβεβαιώνονται σαν νόμιμες όταν γίνονται από ένα σύνολο οντοτήτων που βρίσκονται στην λευκή λίστα και σαν μη νόμιμες όταν γίνονται από ένα σύνολο οντοτήτων που βρίσκονται στην μαύρη λίστα. Βασιζόμενοι στα παραπάνω, οι συγκεκριμένοι χρήστες μπορεί να επιτρέπεται να κάνουν κλήσεις ή να μπλοκάρονται. Οι λίστες είναι προσαρμόσιμες, π.χ. κάθε τελικός χρήστης έχει την ευελιξία να ορίζει τις δικές του εγγραφές. Οι εγγραφές διαφέρουν σε κάθε τελικό χρήστη και η μία λίστα δεν επηρεάζει την άλλη, δηλαδή ο χειρισμός κάθε κλήσης για κάποιον τελικό χρήστη ορίζεται από τον ίδιο τον τελικό χρήστη στον οποίο γίνεται η κλήση. Η μαύρη και η λευκή λίστα κατασκευάζεται χρησιμοποιώντας την ανατροφοδότηση στο σύστημα ανίχνευσης ανεπιθύμητων κλήσεων από τον χρήστη. Όταν μία κλήση προωθείται ο χρήστης απαντά με ένα μήνυμα επανατροφοδότησης ανεπιθύμητων κλήσεων δηλώνοντας τη συγκεκριμένη κλήση σαν ανεπιθύμητη στο σύστημα ανίχνευσης, το σύστημα δημιουργεί μία εγγραφή στη μαύρη λίστα και κάθε μελλοντική κλήση με τις ίδιες παραμέτρους μπλοκάρεται.

Εκμάθηση Bayesian: μαθαίνοντας τη συμπεριφορά των συμμετεχόντων οντοτήτων μας επιτρέπει να παίρνουμε αποφάσεις σχετικά με την κλήση. Η συμπεριφορά των συμμετεχόντων οντοτήτων μπορεί να μαθευτεί κατά τη διάρκεια μιας χρονικής περιόδου. Η συμπεριφορά μπορεί να εκτιμηθεί από το ιστορικό των κλήσεων στους καλούμενους χρήστες. Αυτή η διαδικασία της παρατήρησης των κλήσεων σε μία χρονική περίοδο αναφέρεται σαν εκμάθηση. Η Εκμάθηση αντιπροσωπεύει μία μοντελοποίηση της προηγούμενης συμπεριφοράς των οντοτήτων. Η παρατηρούμενη

συμπεριφορά μέσα με μία χρονική περίοδο θα κατατάξει τις συμμετέχουσες οντότητες σε δημιουργούς ανεπιθύμητων κλήσεων ή νομίμους χρήστες.

Για μια εισερχόμενη κλήση το σύστημα ανίχνευσης θα αναλύσει τις συμμετέχουσες οντότητες, τους διαμεσολαβητές της δρομολόγησης, κτλ με τη βοήθεια συγκεκριμένων πεδίων στις κεφαλίδες των μηνυμάτων. Ο μηχανισμός θα τσεκάρει για αντιστοιχιζόμενη συμπεριφορά ανεπιθύμητων κλήσεων από τις οντότητες που συμμετέχουν βλέποντας την τιμή της εμπιστευτικότητας που είναι διαθέσιμη για αυτές. Αυτή η τιμή θα είναι διαθέσιμη αν αυτές οι οντότητες έχουν ιστορικό κλήσεων.

Δημόσια δίκτυα και φήμη:Τα δημόσια δίκτυα μπορούν να χρησιμοποιηθούν για να παρουσιάσουν τις σχέσεις μεταξύ των χρηστών που προέρχονται από τις διαδρομές του δικτύου. Αυτές οι σχέσεις είναι μεταβατικές και διαφανείς. Αν ο Α σχετίζεται με τον Β και ο Β σχετίζεται με το Γ τότε με μεγάλη σιγουριά μπορεί να διατυπωθεί η πρόταση ότι ο Α σχετίζεται με τον Γ. Αυτά τα δίκτυα μπορούν να χρησιμοποιηθούν για να δείξουν τις σχέσεις μεταξύ των δημοσίων στοιχείων. Με σεβασμό την Voip υπηρεσία, το δημόσιο δίκτυο του χρήστη αντιπροσωπεύει τους έμπιστους γείτονες από τους οποίους ο χρήστης θα λάβει κλήσεις.

Με σεβασμό στον διαμεσολαβητή ένας γράφος μπορεί να δημιουργηθεί χρησιμοποιώντας τους γειτονικούς διαμεσολαβητές και τους χρήστες τους. Ακολούθως ο γράφος μπορεί να χρησιμοποιηθεί ώστε να προκύψει η φήμη του καλούντα. Η φήμη συνεπάγεται κοινωνική κατανόηση. Η φήμη προέρχεται από τα έμπιστα μέρη ενώ η εμπιστοσύνη υπολογίζεται από το ιστορικό. Οι ομότιμοι πληρεξούσιοι παίρνουν τη φήμη από τους δικούς τους έμπιστους ομότιμουςπληρεξούσιους και αυτό συνεχίζεται μέχρι να φτάσουμε στον τελευταίο διαμεσολαβητή στη λίστα 'VIA' ή όταν ο διαμεσολαβητής είναι προσβάσιμος από την πηγή με ένα βήμα. Βασιζόμενοι στην αναφορά φήμης των διαμεσολαβητών και των οντοτήτων που βρίσκονται στο ενδιάμεσο, μπορεί να εξαχθεί η φήμη αυτή.

4.1.2 Ανίχνευση ενοχλητικών κλήσεων με χρήση ημί-επιβλεπόμενης ομαδοποίησης

Κάθε κλήση VOIP[07] αντιμετωπίζεται σαν ένα δεδομένο. Αυτά τα δεδομένα θα ομαδοποιηθούν σε δύο κατηγορίες, η μία θα είναι ενοχλητικές κλήσεις και η άλλη οι

νόμιμες κλήσεις. Θα υπάρχουν υπό-ομάδες μέσα σε κάθε κατηγορία που θα αφορούν τις εντελώς διαφορετικές ενοχλητικές κλήσεις και τις εντελώς διαφορετικές νόμιμες κλήσεις. Η ημι-επιβλεπόμενη ομαδοποίηση έχει σαν στόχο να αντιμετωπίσει το πρόβλημα της επιλογής των κατάλληλων κριτηρίων για την ομαδοποίηση. Αυτού του είδους η ομαδοποίηση επιτρέπει τη χρήση προαιρετικών δεδομένων για ένα υποσύνολο των παρατηρήσεων εκτέλεσης ώστε προοδευτικά να αλλάζουν τα κριτήρια ομαδοποίησης. Αυτό σημαίνει ότι δεν χρειάζεται να οριστεί εξ αρχής ποια γνωρίσματα των δεδομένων θα χρησιμοποιηθούν για την κατηγοριοποίηση. Τα κριτήρια πρέπει να εκπαιδευτούν ώστε να δημιουργούν ομάδες που συμμορφώνονται όσο το δυνατόν περισσότερο με τα προαιρετικά δεδομένα. Δεχόμαστε ότι η επανατροφοδότηση των χρηστών είναι ακριβής.

Γνωρίσματα των VOIP κλήσεων για την ομαδοποίηση:

Η ομαδοποίηση βασίζεται σε 17 γνωρίσματα: 1-2. Πεδία από/σε στο URI, 3. χρόνος έναρξης, 4. Διάρκεια, 5. # του Sip μηνύματος πρόσκλησης, 6. # του Ack μηνύματος, 7-8. # του BYE μηνύματος του καλούντα/καλούμενου, 9. Χρόνος από την τελευταία κλήση του δημιουργού της τρέχουσας κλήσης, 10-15. # των 1xx, 2xx, 3xx, 4xx, 5xx, και 6xx Sip μηνυμάτων απάντησης, 16. Συχνότητα κλήσεων του δημιουργού της τρέχουσας κλήσης, 17. Αναλογία της διάρκειας μη ηρεμίας του καλούμενου στην ροή μετάδοσης των δεδομένων του καλούντα.

Το γνώρισμα 17 βρίσκεται από την ροή Rtp με αισθητήρες στην πλευρά του πελάτη αν η ροή κατευθύνεται απευθείας από πελάτη σε πελάτη ή μπορεί να βρεθεί από αισθητήρες στην πλευρά του εξυπηρετητή αν η ροή κατευθύνεται μέσω SIP διαμεσολαβητή.

4.1.3 Φασματική ανάλυση του ήχου για τον προσδιορισμό ενοχλητικών κλήσεων

Η μέθοδος αυτή [08] επιτρέπει να προσδιοριστούν ενοχλητικές κλήσεις. Είναι παρόμοια με την μέθοδο ανάλυσης του περιεχομένου. Επαναλαμβανόμενες κλήσεις προσδιορίζονται, σημειώνονται και η ταυτότητα του καλούντα μπαίνει σε μαύρη λίστα ώστε να μπλοκάρονται μελλοντικές κλήσεις από αυτόν.

Για τον προσδιορισμό των ενοχλητικών κλήσεων αναλύονται κάποιες ή όλες οι εισερχόμενες κλήσεις. Υπολογίζονται οι φασματικές παράμετροι Sfm και Cfm. Οι

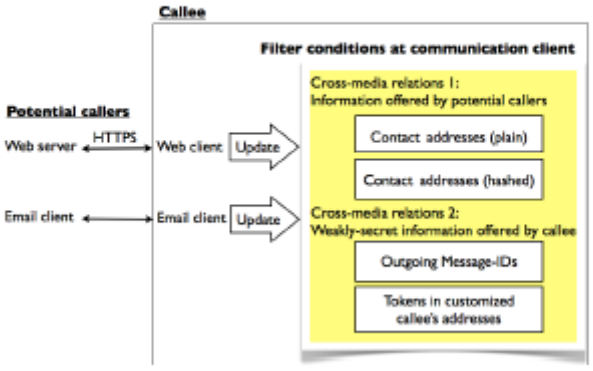
επαναλαμβανόμενες κλήσεις έχουν παρόμοια χαρακτηριστικά Sfm και Cfm. Αυτά τα γνωρίσματα έχουν το χαρακτηριστικό ότι δεν επηρεάζονται από την κωδικοποίηση της ομιλίας ή από κάποια άλλη αλλαγή του ήχου. Έτσι είναι δύσκολο για τον αποστολέα να τροποποιήσει τον ήχο με τέτοιο τρόπο ώστε η μέθοδος να αποτύχει.

Τα Sfm/Scf διανύσματα των εισερχόμενων κλήσεων και οι αντίστοιχοι καλούντες αποθηκεύονται σε μία βάση δεδομένων. Αν υπάρχει μεγάλη ομοιότητα μεταξύ μιας κλήσης και κάποιας προηγούμενης τότε σημειώνονται σαν επαναλαμβανόμενες (πιθανώς ενοχλητική κλήση) και ο καλών μπαίνει σε μαύρη λίστα και οι μελλοντικές κλήσεις του μπλοκάρονται. Ο προσδιορισμός είναι πετυχημένος ακόμα και αν υπάρχει μικρή διαφορά ανάμεσα στα διανύσματα (π.χ. από θόρυβο).

Επιπλέον μία λευκή λίστα μπορεί να δημιουργηθεί με τους καλούντες που επιτρέπεται να κάνουν πανομοιότυπες κλήσεις (π.χ. συναγερμού). Ωστόσο κλήσεις από χρήστες που θέλουν να έχουν πρόσβαση σε ηχογραφημένα μηνύματα (π.χ. πρόγνωση καιρού) δεν επηρεάζονται από το φίλτρο ενοχλητικών κλήσεων καθώς αυτό αναλύει ήχο μόνο από αυτόν που καλεί. Σημειώνεται ότι ο προσδιορισμός απαιτεί 2 επιτυχημένες εγκαθιδρύσεις κλήσεων για πετυχημένη εύρεση επανάληψης. Επιπλέον ενοχλητικές κλήσεις από διάφορους καλούντες μπορούν να ανιχνευθούν αλλά δε μπορούν να μπλοκαριστούν εκ των προτέρων.

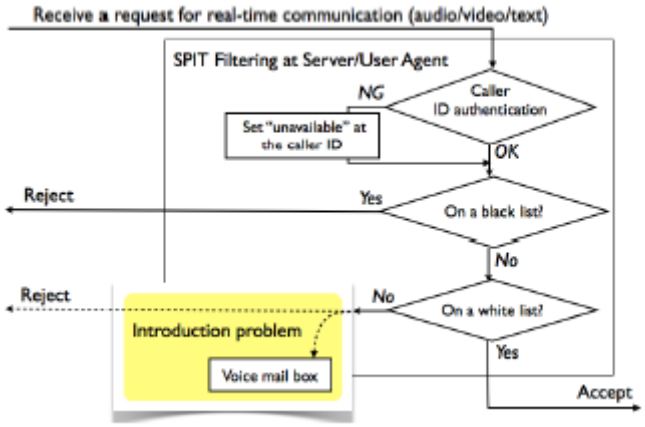
4.2 Μηχανισμοί αντιμετώπισης και μετριασμού των επιθέσεων

4.2.1 Μετριασμός ενοχλητικών κλήσεων με χρήση cross-media σχέσεων



Εικόνα 8. Σύνοψη του προτεινόμενου μηχανισμού

Πριν πραγματοποιηθούν νόμιμες κλήσεις [09] από ανθρώπους ή οργανισμούς με ασθενείς μεταξύ τους σχέσεις συνήθως έχουν προηγηθεί προηγούμενες επαφές μεταξύ του καλούντα και του καλούμενου μέσω ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου ή άλλων ανταλλαγών μέσω διαδικτύου. Επικεντρώνοντας σε αυτές τις προηγούμενες επαφές, προτείνεται η ανταλλαγή συμπληρωματικών πληροφοριών μεταξύ των δύο μερών οι οποίες μπορούν να χρησιμοποιηθούν σε μελλοντικές κλήσεις σαν μία δήλωση νόμιμων προηγούμενων επαφών. Αυτές τις πληροφορίες τις ονομάζουμε cross-media σχέση. Στόχος στη συγκεκριμένη προσέγγιση είναι να επεκταθούν οι συνθήκες του φίλτρου για τις εισερχόμενες κλήσεις με τη χρήση cross-media σχέσεων, εικόνα 8, που επίσης ισχύει και σε άλλες αιτήσεις επικοινωνίας πραγματικού χρόνου. Διακρίνονται 2 τύποι cross-media σχέσεων: διευθύνσεις επαφών που παρέχονται από πιθανούς μελλοντικούς καλούντες και πληροφορίες με ασθενή μυστικότητα που παρέχονται από τον καλούμενο. Στη συνέχεια παρουσιάζονται οι μηχανισμοί που χρησιμοποιούν κάθε τύπο σχέσης και το σύστημα φιλτραρίσματος.



Εικόνα 9. Υπάρχων φίλτρο για τις ενοχλητικές κλήσεις

Διευθύνσεις επαφών από πιθανούς καλούντες

Γενικώς όσο περισσότερες διευθύνσεις επαφών μπορούν να βρεθούν από πιθανούς καλούντες τόσο περισσότερες εισερχόμενες κλήσεις μπορούμε να ταυτοποιήσουμε καθώς ένα τυπικό φίλτρο χρησιμοποιεί την ταυτότητα του καλούντα όπως φαίνεται στην εικόνα 9.

Ανάλογα με τον μηχανισμό των επαφών ο καλούντας χρησιμοποιεί διαφορετικές μεθόδους για να μεταφέρει τις διευθύνσεις των επαφών του, π.χ. Sip:

operator@book.airline.com μεταφέρεται με μία νέα Http κεφαλίδα. Σε μία ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου η διεύθυνση επαφής περιέχεται σε μία vCard επισυναπτόμενη σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που έχει σταλεί από τον πιθανό καλούντα.

Όταν ο καλούμενος λάβει τη διεύθυνση από τον καλούντα την προσθέτει στην λευκή του λίστα. Για αποφυγή κακής χρήσης ζητείται από τον καλούμενο μια επιβεβαίωση της ενημέρωσης της λευκής λίστας για ασφαλείς Http κινήσεις.

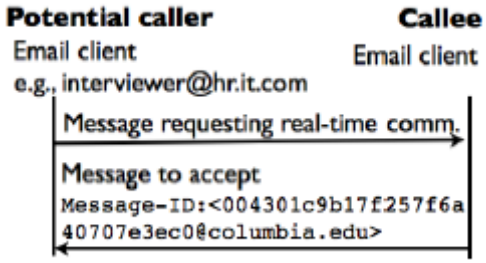
Ο μηχανισμός για τη χρήση αυτού του τύπου Cross-Media σχέσεων είναι κατάλληλος στην περίπτωση που η προηγούμενη επαφή μεταξύ καλούντα και καλούμενου ήταν αντιστοιχισμένη ένας προς έναν. Ωστόσο δε μπορεί να προταθεί αυτός ο μηχανισμός σε πολλές περιπτώσεις, όπως η προηγούμενη επαφή να ήταν για ένταξη σε μία ένωση. Σε αυτή την περίπτωση ο καλούμενος πρέπει να μεταφέρει ασθενείς μυστικά πληροφορίες στους πιθανούς καλούντες.

Μυστικά ασθενής πληροφορία

Η μυστικά ασθενής πληροφορία που παρέχεται από τον καλούμενο είναι επίσης ένα είδος Cross-Media σχέσης. Οι πιθανοί καλούντες μπορούν να χρησιμοποιήσουν αυτή την πληροφορία σε μελλοντικές κλήσεις ώστε να ταυτοποιηθούν σαν κάποιοι που είχαν προηγούμενη επαφή με τον καλούμενο. Αυτός ο μηχανισμός είναι χρήσιμος στις ακόλουθες περιπτώσεις: στην περίπτωση που η προηγούμενη επαφή ήταν ένας προς πολλούς αντιστοιχισμένη μεταξύ του καλούμενου και των πιθανών καλούντων. Π.χ. όταν κατατάσσεσαι σε μία ένωση ο καλούμενος είναι απρόθυμος να λάβει όλες τις διευθύνσεις των πιθανών καλούντων από την ένωση. Άλλη περίπτωση είναι οι πιθανοί καλούντες να χρησιμοποιούν διαφορετική αυθεντικοποίηση ή και καθόλου αυθεντικοποίηση ταυτότητας χρήστη λόγω του τύπου του μέσου επικοινωνίας ή της υπηρεσίας όπως οι δύο-σταδίων κλήση για τις διεθνείς κλήσεις.

Ανάλογα με το μέσο επικοινωνίας της προηγούμενης επαφής, ο καλούμενος παρέχει στον καλούντα διαφορετικό τύπο πληροφορίας. Μία τροποποιημένη διεύθυνση επαφής περιέχει τυχαία περιεχόμενα ή ένα κλειδί μπορεί να χρησιμοποιηθεί όταν ο καλούμενος συμπληρώνει την πληροφορία της επαφής σε μία ιστοσελίδα ή σε μία κάρτα επισυναπτόμενη σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

Ειδικότερα για ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου μπορεί να χρησιμοποιηθεί ένα αναγνωριστικό μηνύματος από ένα μήνυμα ηλεκτρονικού ταχυδρομείου του καλούμενου (εικόνα 10). Ένας πιθανός καλούντας πρώτα στέλνει ένα μήνυμα στον καλούντα ζητώντας του επικοινωνία πραγματικού χρόνου. Μόνο αν ο καλούμενος αποδεχτεί την αίτηση θα απαντήσει με ένα μήνυμα που θα περιέχει την διεύθυνση επαφής του. Με αποτέλεσμα το αναγνωριστικό του μηνύματος της απάντησης που έχει οριστεί στην κεφαλίδα Message-Id μπορεί να χρησιμοποιηθεί σαν πληροφορία με ελαφριά μυστικότητα για να αποδείξει την αποδοχή από τον καλούμενο.



Εικόνα 10. Ανταλλαγή μηνυμάτων ηλεκτρονικής αλληλογραφίας όταν ο καλούμενος μεταφέρει μυστικά ασθενή πληροφορία

Για τον υπολογισμό του αναγνωριστικού μηνύματος σε μία Sip κλήση, ο καλούντας πρέπει να ορίσει μια Sip κεφαλίδα επέκτασης, που αναφέρεται σε αυτή την τιμή. Ωστόσο πρέπει να καθοριστεί μία νέα παράμετρο της κεφαλίδας αναφοράς, η οποία περιορίζει την παράμετρο του αναγνωριστικού της κλήσης. Υποθέτουμε ότι αυτή η κεφαλίδα αναφοράς χρησιμοποιείται για αυτόν τον σκοπό.

Για την ασφάλεια του μηνύματος πρέπει να χρησιμοποιηθεί ο κατάλληλος μηχανισμός για κάθε πρωτόκολλο επικοινωνίας. Για διαδικτυακές κινήσεις χρησιμοποιείται Http με Tls. Για τα μηνύματα ηλεκτρονικού ταχυδρομείου επίσης χρησιμοποιείται το Tls.

4.2.2 Μετριασμός των ενοχλητικών κλήσεων με ανάλυση του πρωτοκόλλου σηματοδοσίας

Στατιστικά Ανίχνευσης

Κάθε πρωτόκολλο σηματοδοσίας Voip[10] έχει τις δικές του συγκεκριμένες αιτήσεις ρύθμισης της συνεδρίας και τερματισμού της συνεδρίας.Η ιδέα είναι να

παρακολουθείται η κίνηση στην σηματοδοσία του Voip στην θύρα του παραλήπτη. Στόχος είναι το πρόβλημα των εξωτερικών κακόβουλων χρηστών μόνο, υποθέτοντας ότι η πρόληψη των ενοχλητικών κλήσεων που βγαίνει από ένα ελεγχόμενο τοπικό δίκτυο είναι κάτι πιο εύκολο. Για κάθε εξωτερική Χ οντότητα που παρακολουθείται, διατηρούνται 4 μετρητές για τον αριθμό των ρυθμίσεων κλήσης και τον αριθμό των τερματισμών κλήσης που εξέρχονται και εισέρχονται από τη θύρα. Βάσει αυτών των μετρητών και με τη βοήθεια μαθηματικών τύπων υπολογίζονται 2 νέες τιμές οι οποίες και παρακολουθούνται. Αν αυτές οι τιμές κάτω υπό συγκεκριμένες προϋποθέσεις επιβεβαιώνουν συγκεκριμένα σενάρια (συμπεριφορές που δείχνουν κακόβουλο χρήστη) που έχουν προταθεί τότε η πηγή αυτών των κλήσεων σημειώνεται σαν κακόβουλη πηγή.

Αντίδραση στις ανιχνευμένες ενοχλητικές κλήσεις

Οι αντιδράσεις απέναντι σε ανιχνευμένες ενοχλητικές κλήσεις μπορούν να ταξινομηθούν σε 3 κατηγορίες:

i. Προειδοποίηση: εμφάνιση μηνύματος προειδοποίησης στην οθόνη του τηλεφώνου και εκπομπή ειδικού ήχου
ii. Καθυστέρηση κλήσης: Αλλαγή της κλήσης στον τηλεφωνητή του καλούμενου, άρνηση της αίτησης και αναφορά του καλούμενου, σε επόμενο στάδιο ορισμός της συγκεκριμένης κλήσης σαν χαμένη
iii. Ακύρωση κλήσης: απόρριψη της ρύθμισης της κλήσης από την πλευρά του παραλήπτη

Γενικά οποιαδήποτε ενέργεια μετριασμού μπορεί να επιδράσει στα στατιστικά ανίχνευσης που εξαρτώνται από την αντίδραση του παραλήπτη. Στην περίπτωση μας καθώς το μεγαλύτερο μέρος των ανεπιθύμητων αιτημάτων για ρύθμιση κλήσης δεν οδηγεί σε μεταφορά δεδομένων μετά τα μέτρα αντίδρασης που έχουν προταθεί αντίστοιχα και τα αιτήματα τερματισμού συνεχώς θα μειώνονται.

4.2.3 Μετριασμός ενοχλητικών κλήσεων με τη χρήση οντότητας ενάντια στις ενοχλητικές κλήσεις στο επίπεδο δικτύου

Τα βασικά στοιχεία του προτεινόμενου αλγορίθμου [11] είναι τα εξής:

i. Χρησιμοποιεί στοιχεία των επιπέδων δικτύου, μεταφοράς και εφαρμογής
ii. Ένας κακόβουλος χρήστης ταυτοποιείται από την Ip του στο επίπεδο δικτύου:Το Sip ψευδώνυμο είναι αναξιόπιστο εκτός αν αυθεντικοποιείται, η Ip διεύθυνση στο VIA πεδίο είναι αξιόπιστη αλλά είναι εφαρμόσιμη μόνο σε τοπικά δίκτυα

iii. Κάθε θετική ανάλυση των δοθέντων κριτηρίων δεν συνεπάγεται και ενοχλητική κλήση αυτόματα: Κάθε ανάλυση ανίχνευσης έχει μία προτεραιότητα. Το άθροισμα τους (επίπεδο ενοχλητικής κλήσης) κατηγοριοποιεί την κλήση σαν ενοχλητική αν αυτό ξεπερνάει ένα δοθέντα όριο

iv. Το όριο αυτό είναι μία παράμετρος σύμφωνα με το προφίλ του αποστολέα και την κατηγορία (συχνά κακόβουλος, σπάνια κακόβουλος, ποτέ κακόβουλος)

v. Μετά το περιεχόμενο επεξεργάζεται για κάθε χρήστη και αποθηκεύεται κατά τη διάρκεια ενός ολισθαίνοντος παραθύρου

vi. Η απόφαση για την κατηγοριοποίηση της κλήσης σαν ενοχλητική εξαρτάται από την ανάλυση της κλήσης, την κατηγορία του χρήση και το ιστορικό του χρήστη

Τα 5 κριτήρια ανίχνευσης του αλγορίθμου:

1. Αριθμός ληφθέντων λάθος μηνυμάτων: Ανάλυση των μηνυμάτων λάθους που απαντάνε σε μηνύματα πρόσκλησης, αν είναι πολλά σημαίνει ότι το ψευδώνυμο του καλούντα είναι πλαστά

2. Αυτοματοποιημένη λογική: Μπορεί να ανιχνεύσει αν ο αποστολέας χρησιμοποίει κάποιον κατάλογο (ελάχιστα διαφοροποιημένες μεταξύ τους διευθύνσεις) (π.χ. dupon@x.net, dupond@x.net, dupont@x.net)

3.Ταυτόχρονες κλήσεις: Πάνω από ένα όριο σημαίνει ότι η μηχανή δημιουργεί τις κλήσεις καθώς ένας άνθρωπος δε μπορεί να χειριστεί πολλές ταυτόχρονες κλήσεις

4. Διάρκεια κλήσης: Αν πολλές κλήσεις έχουν την ίδια διάρκεια τότε σίγουρα είναι ενοχλητική. Ανιχνεύεται στο τέλος της κλήσης που η ενοχλητική κλήση έχει ήδη

μεταδοθεί αλλά μπορεί να βοηθήσει ώστε να μπει σε μαύρη λίστα ο αποστολέας και να μπλοκαριστούν μελλοντικές του κλήσεις.

5. Βομβαρδισμός κλήσεων: Ταυτόχρονες κλήσεις από διαφορετικούς χρήστες προς έναν

Προτεινόμενες αντιδράσεις

i. Περιορισμός του αριθμού των κλήσεων για λιγότερο ενεργούς κακόβουλους χρήστες.
ii. Προσωρινές μαύρες λίστες για πιο ενεργούς κακόβουλους χρήστες.
iii. Μπλοκάρισμα κλήσεων από κάποιον για ένα χρονικό διάστημα.
iv. Προώθηση της κλήσης αλλού.
v. Επαναπροώθηση της κλήσης σε κάποια αυτοματοποιημένη μηχανή
vi. Αρνητική απάντηση στις κλήσεις, ειδοποιήσεις,
vii. Επαναπροώθηση της κλήσης σε κάποιον εξυπηρετητή για κατάταξη των χρηστών ή για στατιστικούς λόγους

Τοποθέτηση της οντότητας

Αν αυτή η οντότητα τοποθετηθεί σε διαμεσολαβητή έχει το πλεονέκτημα ότι δεν υπάρχει κανένα θέμα σχετικό με την κρυπτογράφηση της κίνησης και το μειονέκτημα είναι ότι έχει επίπτωση στην απόδοση του διαμεσολαβητή όταν υπάρχει πολύ κίνηση και αυτή η υπερφόρτωση δε μπορεί να αποφευχθεί

Αν η οντότητα τοποθετηθεί σε κάποιο τυχαίο σημείο χρησιμοποιείται για την ανάλυση όλης της Ip κίνησης του δικτύου με πλεονέκτημα ότι μπορεί να χρησιμοποιηθεί σε άλλου είδους ανιχνεύσεις και μετριασμούς (επιθέσεις άρνησης της υπηρεσίας) και μειονέκτημα ότι απαιτείται κρυπτογράφηση της κίνησης

Αν υπάρχει δρομολογητής σε τυχαίο σημείο σε συνδυασμό με την εξωτερική οντότητα που αντιμετωπίζει τις ενοχλητικές κλήσεις, αυτή η εξωτερική οντότητα αναλύει μόνο την Voip κίνηση. Η Ipκίνηση που ανιχνεύεται σαν Voip από τον δρομολογητή προωθείται στην εξωτερική οντότητα που λειτουργεί ενάντια στις ενοχλητικές κλήσεις. Η οντότητα ξανά διοχετεύει την νόμιμη κίνηση Voip ξανά στο δίκτυο. Πλεονέκτημα σε αυτή την περίπτωση είναι η επεκτασιμότητα του και μειονέκτημα είναι ότι απαιτείται κρυπτογράφηση της κίνησης.

4.3 Μηχανισμοί αποφυγής επιθέσεων

Παρακάτω θα δούμε τις υπάρχουσες προσεγγίσεις για την πρόληψη των Sip [12] ανεπιθύμητων μηνυμάτων που βασίζονται σε παρόμοια λογική με την λογική πρόληψης των ενοχλητικών μηνυμάτων ηλεκτρονικής αλληλογραφίας.

4.3.1 Φιλτράρισμα περιεχομένου

Άχρηστο εφόσον η κλήση απαντηθεί γιατί η συνεδρία εγκαθιδρύεται και το περιεχόμενο μεταφέρεται. Σημειώνεται ότι είναι εξαιρετικά δύσκολο το φιλτράρισμα αποθηκευμένου ηχητικού περιεχομένου όπως ένα ηχητικό μήνυμα.

4.3.2 Μαύρες λίστες

Φιλτράρισμα σύμφωνα με μία μπλοκαρισμένη λίστα διευθύνσεων (μαζί όνομα χρήστη και πεδίο που ανήκει). Άχρηστο καθώς η διεύθυνση ηλεκτρονικού ταχυδρομείου εύκολα υποκλέπτεται και οι διευθύνσεις ηλεκτρονικού ταχυδρομείου είναι σχεδόν απεριόριστες.

4.3.3 Λευκές λίστες

Φιλτράρισμα σύμφωνα με μία λίστα έγκυρων και μη κακόβουλων αποστολέων. Επιτυχής άμυνα ενάντια στην ενοχλητική αλληλογραφία, ωστόσο δεν είναι πολύ ευέλικτη λύση καθώς δεν επιτρέπει την αποδοχή νέων έγκυρων μηνυμάτων.

4.3.4 TuringTests και κρυπτογραφικά παζλ

Οι εντελώς αυτόματες ενοχλητικές κλήσεις που ονομάζονταιbot [13] είναι ένα πολύ φθηνό και ενοχλητικό πράγμα. Για την πρόληψη του μπορούν να χρησιμοποιηθούν διάφορες τεχνικές:

i. ηχητικό μενού: πριν προωθηθεί μία κλήση, ο υπολογιστής ζητάει από τον καλούντα να πληκτρολογήσει ένα συνδυασμό πλήκτρων, π.χ. 4#5$
ii. Μοντέλα προκλήσεων: Πριν μία κλήση προωθηθεί ζητείται από τον καλούντα να κάνει μία απλή μαθηματική πράξη π.χ. 5*2
iii. Διαφορετικός αριθμός: Κάτω από τον κύριο αριθμό ο υπολογιστής δείχνει έναν διαφορετικό αριθμό. Όλες οι παραπάνω μέθοδοι μπορούν να εκτελεστούν εμπλουτισμένες με ένα ηχητικό σήμα θορύβου ή μουσικής. Αυτό αποτρέπει τα Bots ενοχλητικών κλήσεων να χρησιμοποιούν αναγνώριση ομιλίας.

Ενώ αυτά τα τεστ είναι ελκυστικά, συχνά είναι δύσκολο για έναν υπολογιστή να αποκρυπτογραφεί ηχητικές ερωτήσεις, ενώ τα τεστ πρέπει να είναι εύκολα ώστε να μπορούν να τα λύσουν οι χρήστες.

Τα κρυπτογραφικά παζλ επίσης μπορούν να βοηθήσουν στην πρόληψη των κακόβουλων χρηστών. Όταν ο καλών προσπαθεί να εγκαθιδρύσει μία σύνδεση , έχει να λύσει ένα μικρό παζλ χρησιμοποιώντας υπολογιστικούς πόρους (CPU, εύρος ζώνης). Δηλαδή επειδή η υπολογιστική ισχύς έχει κάποιο όριο, ο αριθμός των παράλληλων συνδέσεων παραμένει χαμηλός. Το μειονέκτημα αυτής της λύσης είναι ότι ένας κανονικός χρήστης με ένα αργό υπολογιστή θα έχει επίσης καθυστερήσεις κατά τη διάρκεια της λύσης αυτών των παζλ. Τέλος οι κακόβουλοι χρήστες μερικές φορές χρησιμοποιούν μολυσμένα από ιούς υπολογιστές των οποίων η υπολογιστική ισχύ είναι μεγάλη.

4.3.5 Greylisting

Η Greylisting είναι μία χρήσιμη τεχνική για το φιλτράρισμα ενοχλητικών μηνυμάτων ηλεκτρονικής αλληλογραφίας που μπορεί επίσης να χρησιμοποιηθεί στο Voip. Βάσει αυτής της τεχνική κάθε κλήση μπλοκάρεται εκτός εάν ο ίδιος χρήστης προσπαθεί να κάνει την ίδια κλήση μέσα σε μια συγκεκριμένη χρονική περίοδο. Ωστόσο υπάρχουν αρκετές ανησυχίες για αυτή τη μέθοδο. Αρχικά φαίνεται εύκολο να ξεπεραστεί το φίλτρο απλώς με το να κάνει κάποιος μία δεύτερη προσπάθεια. Επιπλέον η Greylisting μπορεί να μπλοκάρει επείγουσες κλήσεις από φίλους.

4.3.6 Συστήματα που βασίζονται στη φήμη

Η ιδέα που βασίζονται αυτά τα συστήματα είναι ο καλούμενος να έχει μία γνώση για τον καλούντα πριν απαντήσει την κλήση. Αν η φήμη του είναι κακή τότε μπορεί να αποφασίσει αν αποδεχτεί ή όχι την κλήση. Δυστυχώς αυτά τα συστήματα είναι πολύπλοκα και συχνά καταλήγουν σε ψευδή αποτελέσματα. Επιπλέον αν και ένας χρήστης αποκτήσει κακή φήμη πρέπει να ανοίξει καινούργιο λογαριασμό.

4.3.7 Συστήματα με βάση τον όγκο των αιτήσεων

Η ιδέα σε αυτά τα συστήματα είναι ότι ο πάροχος πρέπει να περιορίσει τις αιτήσεις συνδέσεων Voip που μπορεί κάποιος πελάτης να κάνει μέσα σε ένα χρονικό διάστημα. Φυσικά, είναι δύσκολο ο πάροχος να συμμορφωθεί με αυτό καθώς τον συμφέρει να βάζει λιγότερους περιορισμούς στους πελάτες του.

4.3.8 Αυθεντικοποίηση

Το Sip χρησιμοποιεί διάφορα μοντέλα για την αυθεντικοποίηση των χρηστών. Τέτοιες μέθοδοι αυθεντικοποίησης μπορεί να είναι πολύ απαιτητικές για την πρόληψη ανώνυμης Voip κίνησης. Ωστόσο δεν είναι ρεαλιστικό να υπάρξει ένα γενικό μοντέλο πιστοποίησης.

4.3.9 Επιθετική πρόληψη ενοχλητικών κλήσεων

Αυτοί οι μηχανισμοί χωρίζονται σε 2 κατηγορίες:

i. ενεργή δημοσίευση των ψευδών πληροφοριών
ii. αντεπίθεση στους κακόβουλους χρήστες

Η ενεργητική δημοσίευση των ψευδών πληροφοριών, δημοσιεύει SIP διευθύνσεις, είναι ένας τρόπος να γεμίσουν οι βάσεις δεδομένων με τους κακόβουλους χρήστες. Αυτό ανεβάζει το κόστος της επιτυχημένης μεταφοράς ενοχλητικών μηνυμάτων. Οι αντεπιθέσεις στην υποδομή των κακόβουλων χρηστών είναι μία λύση ώστε να μη μπορούν να λειτουργήσουν αυτοί οι κακόβουλοι χρήστες. Αυτός είναι ο πιο

αποτελεσματικός τρόπος αν αρκετά θύματα χρησιμοποιούν αυτή την τεχνική. Αυτή η μέθοδος όμως είναι πολύ ακριβή και επικίνδυνη καθώς κατάχρηση της μπορεί να δημιουργήσει επιθέσεις άρνησης της υπηρεσίας.

Φαίνεται ότι οι πιο επιτυχημένες προσεγγίσεις για την καταπολέμηση της ενοχλητικής αλληλογραφίας ηλεκτρονικού ταχυδρομείου είναι σε μεγάλο βαθμό άχρηστες για την πρόληψη των ενοχλητικών κλήσεων Ip. [13]Υπάρχουν πολλοί λόγοι για αυτή την αποτυχία. Αρχικά ένα μήνυμα ηλεκτρονικού ταχυδρομείου φτάνει πρώτα στον εξυπηρετητή πριν ληφθεί από τον χρήστη, έτσι ο εξυπηρετητής μπορεί να χρησιμοποιήσει διάφορα φίλτρα ώστε να κατηγοριοποιήσει το κάθε μήνυμα αν είναι έγκυρο ή ενοχλητικό.

Προφανώς η πιο αποδοτική πρόληψη γίνεται από τις λευκές λίστες αλλά αυτή δεν είναι ευέλικτη λύση όπως αναφέρθηκε.

4.3.10 Γνώση για τον καλούμενο

Η βασική διαφορά ανάμεσα σε έναν κανονικό καλούντα και σε έναν κακόβουλο χρήστη είναι ότι ο πρώτος έχει γνώση για το άτομο που καλεί. Επομένως φαίνεται φυσικό να ψάχνεις για φίλτρα τα οποία ρωτάνε τον καλούντα να δώσει συγκεκριμένες πληροφορίες για τον καλούμενο. Φυσικά αυτή η πληροφορία είναι εύκολο να δοθεί από έναν κανονικό καλούντα αλλά όχι από έναν κακόβουλο. Αν και αυτή είναι μια εφικτή προσέγγιση το πώς θα γίνει αυτή αποτελεσματική και το πώς θα υλοποιηθεί είναι ένα θέμα για μελλοντική έρευνα.

4.3.11 Διαθεσιμότητα του καλούντα

Μία άλλη ιδιότητα που διακρίνει τους κανονικούς χρήστες από τους κακόβουλους είναι ότι δεν γίνεται να καλέσεις έναν κακόβουλο χρήστη γιατί δεν είναι διαθέσιμος. Λύση θα μπορούσε να είναι η εφαρμογή ενός πρωτοκόλλου χειραψίας στο ξεκίνημα κατά το οποίο καλείται και ο καλούντας. Σημειώνεται ότι ακόμα και αν ο κακόβουλος προσπαθήσει να γίνει διαθέσιμος ο πολύ μεγάλος αριθμός τον κλήσεων που θα γίνουν προς αυτόν κατά τη διάρκεια της επίθεσης ενοχλητικών κλήσεων που κάνει ο ίδιος θα λειτουργήσουν παρόμοια με μία επίθεση άρνησης της υπηρεσίας προς αυτόν.

4.3.12Greylists με χρήση Tokens

Όπως έχει αναφερθεί προηγουμένως οι Greylists προκαλούν από τη φύση τους μία καθυστέρηση καθώς ο καλούντας απαιτείται να ξανακάνει κλήση μετά από μία συγκεκριμένη χρονική περίοδο. Ωστόσο μπορούμε να καταλάβουμε ότι αυτό ισχύει μόνο για την πρώτη επαφή μεταξύ καλούντα και καλούμενου. Συγκεκριμένα μία λύση θα ήταν μετά από κάθε επιτυχημένη κλήση να συμφωνείται μεταξύ τους ένα κοινόχρηστο μυστικό. Στην επόμενη κλήση ο καλούντας γνωστοποιώντας αυτό το μυστικό στον καλούμενο μπορεί να παρακάμψει την Greylist και να επικοινωνήσει με τον καλούμενο άμεσα.

4.3.13 Ερώτηση για την ταυτότητα

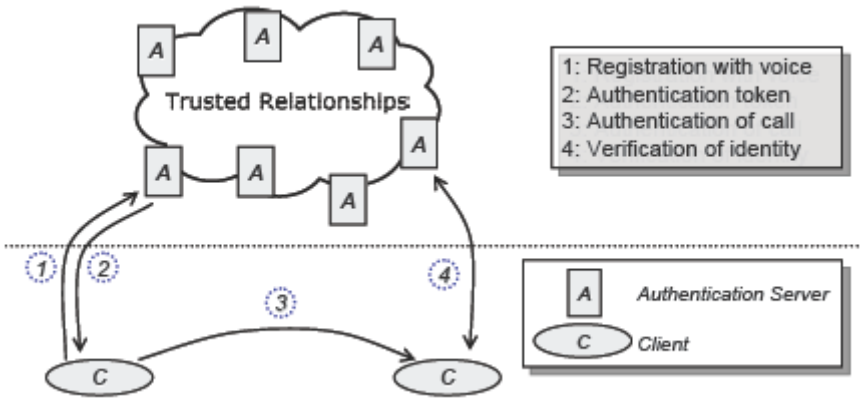
Ένα γενικό θέμα στην αναζήτηση φίλτρων ενοχλητικών κλήσεων είναι να απαιτείται κάποια συνεισφορά από τους κακόβουλους χρήστες, για παράδειγμα με σκοπό την υπολογιστική ισχύ, τους πόρους δικτύου κτλ. Αν και αυτές οι συνεισφορές είναι φτηνές για τους νόμιμους χρήστες, είναι πολύ ακριβές για τους κακόβουλους. Σημαντικό επίσης θα ήταν να ζητούνταν από τον καλούντα κάποιο είδος ταυτότητας. Μία ακραία περίπτωση που μπορεί να χρησιμοποιηθεί μόνο σαν παράδειγμα είναι να ζητείται μία έγκυρη χρεωστική κάρτα όταν προσπαθεί κάποιος να εγκαθιδρύσει μία κλήση.

4.3.14 Ένα βιομετρικό πλαίσιο για την πρόληψη των ενοχλητικών κλήσεων

Η μεγάλη δυσκολία στην πρόληψη των ενοχλητικών κλήσεων είναι ότι οι κακόβουλοι χρήστες αλλάζουν ταυτότητα πολύ συχνά. Μέθοδοι όπως οι μαύρες λίστες, δίνουν μία δύσκολη μάχη με τις συνεχείς αλλαγές ταυτότητας. Ως εκ τούτου είναι βασικό για τα φίλτρα ενοχλητικών κλήσεων να αναστείλουν αυτές τις επιθέσεις που αποκαλούνται Sybil επιθέσεις. Η αντιστοίχιση ταυτοτήτων σε ανθρώπους μπορεί να βοηθήσει στην πρόληψη αυτών των επιθέσεων. Παρακάτω παρουσιάζεται ένα γενικό πλαίσιο που αντιμετωπίζει το πρόβληματων ενοχλητικών κλήσεων. Σε αυτή τη λύση γενικοί εξυπηρετητές αντιστοιχούν τις ταυτότητες των χρηστών σε προσωπικά δεδομένα, στη συγκεκριμένη περίπτωση τα αντιστοιχούν σε βιομετρικά δεδομένα, όπως η φωνή. Επίσης σε αντίθεση με άλλες λύσεις οι κακόβουλοι χρήστες δε μπορούν να αποκτήσουν νέες ταυτότητες ακόμα και αν αλλάξουν πάροχο ίντερνετ.

Αρχιτεκτονική

Η Γενική αρχιτεκτονική φαίνεται στην εικόνα 11. Χρησιμοποιείται μία ομάδα από έμπιστους εξυπηρετητές αυθεντικοποίησης (A). Πριν ο πελάτης (C) χρησιμοποιήσει την Voip υπηρεσία για πρώτη φορά πρέπει να εγγραφεί σε έναν εξυπηρετητή αυθεντικοποίησης. Στόχος αυτής της διαδικασίας είναι να εγγραφεί η φωνή του χρήστη και να αντιστοιχηθεί με την Voip ταυτότητα του. Αρχικά ο πελάτης καλεί τον εξυπηρετητή. Ο εξυπηρετητής ζητάει από τον πελάτη να επαναλάβει μία πρόταση. Για την ασφάλεια της διαδικασίας η πρόταση πρέπει να είναι διαφορετική για κάθε εγγραφή. Μετά την ολοκλήρωση αυτής τη διαδικασίας ο εξυπηρετητής αποθηκεύει το αρχείο φωνής του πελάτη και του στέλνει πίσω τα συνθηματικά. Ο πελάτης τώρα μπορεί να κάνει όσες κλήσεις θέλει σε άλλους πελάτες αυθεντικοποιώντας τον εαυτό του με τη χρήση των συνθηματικών του. Οποιοσδήποτε λαμβάνει μία κλήση επιβεβαιώνει την ταυτότητα του καλούντα ελέγχοντας τα συνθηματικά του, σε αυτό μπορεί να εμπλέκεται και μία επικοινωνία με τον εξυπηρετητή αυθεντικοποίησης.



Εικόνα 11. Αρχιτεκτονική του συστήματος

Κεφάλαιο 5

Επίλογος

Η ραγδαία εξάπλωση του διαδικτύου και το χαμηλό κόστος του οδηγούν στη συνεχώς αυξανόμενη χρήση Voip επικοινωνιών. Το Sip πρωτόκολλο κληρονομεί όλα τα τρωτά σημεία του διαδικτύου και αυτό το κάνει ευάλωτο σε πολλών ειδών επιθέσεις, οι υφιστάμενοι μηχανισμοί ασφαλείας αντιμετωπίζουν αρκετά θέματα αλλά δημιουργούνται συνεχώς νέες προκλήσεις που πρέπει να αντιμετωπιστούν. Η ανάγκη για ασφάλεια, διαθεσιμότητα και αξιοπιστία σε αυτές τις επικοινωνίες είναι μεγάλη και για το λόγο αυτό οι μηχανισμοί ασφαλείας πρέπει να είναι αποτελεσματικοί. Τα προβλήματα ασφαλείας στις διαδικτυακές επικοινωνίες είναι πολλά και συνεχώς αυξάνονται, το πεδίο έρευνας είναι πολύ μεγάλο και υπάρχουν ακόμα πολλά θέματα τα οποία χρήζουν έρευνας και δεν έχουν αντιμετωπιστεί επαρκώς. Σε αυτή τη μεταπτυχιακή διατριβή καταγράψαμε τα τρωτά σημεία του πρωτοκόλλου και τις υφιστάμενες επιθέσεις που μπορούν να γίνουν καθώς και τους μηχανισμούς ασφαλείας που υπάρχουν.

Είναι γεγονός ότι είναι αδύνατο να καλυφθούν όλα τα θέματα που προκύπτουν, το σημαντικότερο και ταυτόχρονα δυσκολότερο πεδίο είναι το πεδίο της πρόληψης και σε αυτό υπάρχουν οι περισσότεροι μηχανισμοί που καταγράψαμε. Ένα κομμάτι το οποίο χρήζει περισσότερης έρευνας είναι η επίπτωση όλων αυτών των μηχανισμών στην ποιότητα και την ταχύτητα των επικοινωνιών. Οι περισσότερες επιθέσεις που καταγράφηκαν έχουν σκοπό την πρόκληση άρνησης της υπηρεσίας.

Λεξικό όρων

Accounting = παρακολούθηση της κίνησης

Authentication = Αυθεντικοποίηση

Authorization = Εξουσιοδότηση

Bye=τερματισμός

Callsetup = Ρύθμισηκλήσης

Client = πελάτης

Domain = τομέας

Dos = Άρνηση της υπηρεσίας

Endtoend = από άκρο σε άκρο

EndtoMiddle= απόάκροστομέσο

Endpoint = Τερματικό

Firewall= Ανάχωμα Ασφάλειας

Hijacked = μολυσμένος

Hopbyhop = Από ενδιάμεσο σε ενδιάμεσο

Host = τερματικό

Interface=διεπαφή

Invite=Προσκαλώ

Locationserver = Εξυπηρετητήςτοποθεσιών

Malicious = μολυσμένος

Maninthemiddle= κακόβουλοςενδιάμεσοςχρήστης

MediaGateway=Πύλη δεδομένων

Module=κομμάτι

Peerproxy= Ομότιμοςπληρεξούσιος

Proxy = διαμεσολαβητής - πληρεξούσιος

Re-directServer = εξυπηρετητήςΕπαναπροωθήσεων

Registrarserver = Εξυπηρετητήςεγγραφών

Router=δρομολογητής

Server = Εξυπηρετητής

Serviceabuse = Κατάχρηση υπηρεσίας

Session = Συνεδρία - Σύνοδος

SIPSignaling = ΣηματοδοσίαSIP

Spit=ενοχλητική κλήση

Stream = Ροή

Tunneling=διασωλήνωση

Βιβλιογραφία

[01] Dimitris Geneiatakis, TasosDagiuklas, GeorgiosKambourakis, Costas Lambrinoudakisand Stefanos Gritzalis, University Of The Aegean, KarlovassisvenEhlert And DorghamSisalem, FraunhoferFokus Institute ''Survey Of Security Vulnerabilities Insession Initiation Protocol'' 3rd Quarter 2006

[02] Angelos D. Keromytis, Senior Member, IEEE ''A Comprehensive Survey of Voice over IP Security Research ''

[03] D. Geneiatakis and C. Lambrinoudakis, "A Lightweight Protection Mechanism against Signaling Attacks in a SIP-based VoIP Environment," *Telecommunication Systems*, vol. 36, pp. 153–159, December 2007.

[04] X. Wang, R. Zhang, X. Yang, X. Jiang, and D. Wijesekera, "Voice Pharming Attack and the Trust of VoIP," in *Proceedings of the* 4th*International Conference on Security and Privacy in Communication Networks (SecureComm)*, pp. 1–11, September 2008.

[05] A. Bremler-Barr, R. Halachmi-Bekel, and K. Kangasharju, "Unregister Attacks in SIP," in *Proceedings of the* 2nd*IEEE Workshop on Secure Network Protocols*, pp. 32–37, November 2006.

[06] R. Dantu and P. Kolan, "Detecting Spam in VoIP Networks," in *Proceedings of the USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, pp. 31–37, July 2005.

[07] Y.-S. Wu, S. Bagchi, N. Singh, and R. Wita, "Spam Detection in Voice-Over-IP Calls through Semi-Supervised Clustering," in *Proceedings of the* 39th*Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 307–316, June 2009.

[08] C. Porschmann and H. Knospe, "Analysis of Spectral Parameters of Audio Signals for the Identification of Spam Over IP Telephony," in *Proceedings of the* 5th*Conference on Email and Anti-Spam (CEAS)*, August 2008.

[09] K. Ono and H. Schulzrinne, "Have I Met You Before? Using Cross-Media Relations to Reduce SPIT," in *Proceedings of the* 3rd*Inter-national Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pp. 1–7, June 2009.

[10] R. Dantu and P. Kolan, "Preventing Voice Spamming," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), Workshop on VoIP Security Challenges and Solutions*, December 2004.

[11] M. Bertrand, Q. Loudier, Y. Gourhant, F. Bougant, and M. Osty, "SPIT Mitigation by a Network-Level Anti-Spit Entity," in *Proceedings of the* 3rd*Workshop on Securing Voice over IP*, June 2006.

[12] N. Croft and M. Olivier, "A Model for Spam Prevention in Voice over IP Networks using Anonymous Verifying Authorities," in *Proceedings of the* 5th*Annual Information Security South Africa Conference (ISSA)*, July 2005.

[13] R. Baumann, S. Cavin, and S. Schmid, "Voice Over IP -Security and SPIT," KryptDet Report FU Br 41, Swiss Army, August/September 2006.

[14] R. Zhang, X. Wang, X. Yang, and X. Jiang, "Billing Attacks on SIP-based VoIP Systems," in *Proceedings of the* 1st*USENIX Workshop On Offensive Technologies (WOOT)*, pp. 1–8, August 2007.