ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΔΙΔΑΚΤΙΚΗΣ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τίτλος Διατριβής:

SPAM στη διαδικτυακή τηλεφωνία. Εντοπισμός και αντιμετώπιση.

Δημακόπουλος Νικόλαος

Επιβλέπων: Κος Κάτσικας Σωκράτης, Καθηγητής

Διατριβή που υποβάλλεται ως μερική συμπλήρωση των απαιτήσεων για την απόκτηση μεταπτυχιακού τίτλου

Πειραιάς, Νοέμβριος 2009

Περίληψη

Στην παρούσα διπλωματική εργασία μελετάται η εξέλιξη της διαδικτυακής τηλεφωνίας σήμερα, οι καινοτομίες τις οποίες η εξέλιξη αυτή μας έχει προσφέρει, καθώς όμως και τους κινδύνους τους οποίους αυτή η εξέλιξη επισύρει. Παρουσιάζονται μέθοδοι ανίχνευσης πιθανών επιθέσεων στη διαδικτυακή τηλεφωνία, καθώς και λύσεις αντιμετώπισής τους. Γίνεται ανάλυση δομής ενός σύγχρονου συστήματος ασφάλειας, και περιγράφονται αναλυτικά τα επίπεδά του και το πως συμβάλει το κάθε ένα στην αντιμετώπιση πιθανών επιθέσεων.

Στο Κεφάλαιο 1, γίνεται μία εισαγωγή στην τρέχουσα κατάσταση της διαδικτυακής τηλεφωνίας, στα οφέλη τα οποία αυτή μας παρέχει, καθώς όμως και τους πιθανούς κινδύνους και προβλήματά της. Στο δεύτερο Κεφάλαιο συναντάμε μία σύντομη σύγκριση της διαδικτυακής τηλεφωνίας και των κλασσικών τηλεφωνικών δικτύων. Φτάνοντας στο Κεφάλαιο 3, γίνεται μία περιγραφή του επικρατέστερου πρωτόκολλου στη διαδικτυακή τηλεφωνία, στο πρωτόκολλο SIP, και τις μεθόδους ασφάλισής του. Στο τέταρτο Κεφάλαιο, περιγράφουμε τους πιθανούς κινδύνους από πιθανές επιθέσεις στη διαδικτυακή τηλεφωνία, ενώ το Κεφάλαιο 5 γίνεται σύγκριση των επιθέσεων αυτών με επιθέσει σε ηλεκτρονικό ταχυδρομείο. Στο έκτο Κεφάλαιο γίνεται μία αναφορά στις ομοσπονδίες των Member Islands σε ένα δίκτυο διαδικτυακής τηλεφωνίας, έτσι ώστε να τονίσουμε την ομαδοποίηση στην ασφάλισή της. Φτάνοντας στο Κεφάλαιο 7, συναντάμε μία περιγραφή στα χαρακτηριστικά ασφάλειας ενός δικτύου διαδικτυακής τηλεφωνίας, ενώ στο Κεφάλαιο 8, περιγράφουμε στη γλώσσα με την οποία μπορούμε να δηλώσουμε και να παραμετροποιήσουμε τα χαρακτηριστικά αυτά. Στο Κεφάλαιο 9, 10, 11 και 12, γίνεται μία παρουσίαση των απειλών και των επιθέσεων στη διαδικτυακή τηλεφωνία, καθώς και πιθανά σενάρια αντιμετώπισής τους και μέθοδοι ασφάλειας. Στο 13^{ο} Κεφάλαιο περιγράφουμε αναλυτικά τα επίπεδα αρχιτεκτονικής ενός συστήματος αντιμετώπισης spam, και στο Κεφάλαιο 14, τις μεθόδους αντιμετώπισης επιθέσεων σήμερα. Τελειώνοντας, στο Κεφάλαιο 15 γίνεται μία περιγραφή των νομικών περιορισμών οι οποίοι ισχύουν σε

κράτη με ανεπτυγμένη τη διαδικτυακή τηλεφωνία, ενώ στο 15^{ο} και τελευταίο Κεφάλαιο, συναντάμε γενικά συμπεράσματα και διαπιστώσεις τις οποίες κάναμε μέσω της τρέχουσας μελέτης.

ΕΥΡΕΤΗΡΙΟ ΠΙΝΑΚΩΝ 7

ΕΥΡΕΤΗΡΙΟ ΣΧΗΜΑΤΩΝ 7

1. ΕΙΣΑΓΩΓΗ 9

2. ΔΙΑΦΟΡΕΣ ΜΕΤΑΞΥ VOICE OVER IP ΚΑΙ PSTN ΤΗΛΕΦΩΝΙΚΟΥ ΚΕΝΤΡΟΥ. 12

3. ΤΟ ΠΡΩΤΟΚΟΛΛΟ SIP 15

3.1 Σηματοδότηση με το πρωτόκολλο SIP 15

3.2 Πραγματοποίηση απλής φωνητικής κλήσης με το πρωτόκολλο SIP 17

3.3 Ασφάλεια πρωτοκόλλου SIP 19

3.3.1 S/MIME (Secure/Multipurpose Internet Mail Extensions) 19

3.3.2 Digest Authentication 20

3.3.3 TLS & IPSec (Transport Layer Security & Internet Protocol Security) 21

4. VOICE OVER IP ΚΑΙ SPAM 23

5. EMAIL SPAM ΚΑΙ SPIT. ΚΟΙΝΑ ΣΗΜΕΙΑ ΚΑΙ ΔΙΑΦΟΡΕΣ 25

6. ΟΙ ΟΜΟΣΠΟΝΔΙΕΣ ΤΩΝ MIS (MEMBER ISLANDS) 27

Ταυτοποίηση 28

7. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΣΦΑΛΕΙΑΣ VOIP ΔΙΚΤΥΩΝ 30

7.1 Ισχύς Ταυτότητας (IdentityStrength) 30

7.2 Κόστος κλήσης (CostOfCall) 31

7.3 Αυθεντικοποίηση χρήστη (AuthenticationOfUser) 32

7.4 Δήλωση ταυτότητας (IdentityAssertion) 32

7.5 Ασφάλεια Σύνδεσης (ConnectionSecurity) 33

7.6 Υποψία Κλήσης SPIT (SPITSuspect) 33

7.7 Τηλεφωνικά Κέντρα (CallCenter) 34

7.8 Ισχύς Δήλωσης (AssertionStrength) 35

8. ΔΗΛΩΣΗ-ΔΙΑΧΕΙΡΙΣΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ, ΜΕΣΩ ΓΛΩΣΣΑΣ SAML 36

8.1 Μελλοντικές μελέτες βασισμένες στον κώδικα SAML 43

9. ΑΠΕΙΛΕΣ ΣΤΗ ΔΙΑΔΙΚΤΥΑΚΗ ΤΗΛΕΦΩΝΙΑ 45

9.1 Ενόχληση και διακοπή υπηρεσίας 46
9.2 Ωτακουστική και ανάλυση κίνησης 47
9.3 Παραποίηση ταυτότητας και ψευδοπροσωποποίηση 47
9.4 Μη εξουσιοδοτημένη πρόσβαση 48
9.5 Εξαπάτηση 49
9.6 Υποκλοπή πακέτων (packet sniffing) 49

10. ΕΠΙΘΕΣΕΙΣ ΣΕ SIP ΣΥΣΤΗΜΑΤΑ ΔΙΑΔΙΚΤΥΑΚΗΣ ΤΗΛΕΦΩΝΙΑΣ. 53

11. ΠΙΘΑΝΑ ΣΕΝΑΡΙΑ SPIT ΚΑΙ ΑΝΤΙΜΕΤΡΑ 63

11.1 Τηλεφωνικά κέντρα 63
11.2 Τηλεφωνικά ρομπότ 64
11.3 Επίμονη κλήση 64
11.4 Καλών χρονικά συνειδητοποιημένος 64
11.5 Προ-ηχογραφημένο μήνυμα 65
11.6 Θυρίδα μηνύματος 65
11.7 Πραγματοποίηση κλήσης από τρίτους 65
11.8 SPIT κωδωνισμός 66
11.9 Ανωνυμία 67
11.10 Συνδυασμός των παραπάνω 68

12. ΑΣΦΑΛΕΙΑ ΣΤΗ ΔΙΑΔΙΚΤΥΑΚΗ ΤΗΛΕΦΩΝΙΑ (SPIT PREVENTION) 69

12.1 Γενικά μέτρα ασφάλειας, πριν την επίθεση. 69

13. ΓΕΝΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΜΗΧΑΝΙΣΜΩΝ ΠΡΟΛΗΨΗΣ SPAM ΣΤΗΝ ΔΙΑΔΙΚΤΥΑΚΗ ΤΗΛΕΦΩΝΙΑ 73

13.1 Χτίζοντας τα τμήματα ενός συστήματος πρόληψης spit κλήσεων ... 76
13.1.1 Επίπεδο 1. Καμία αλληλεπίδραση καλούντα και καλούμενου .. 77
13.1.2 Επίπεδο 2. Αλληλεπίδραση με τον καλούντα 78
13.1.3 Επίπεδο 3. Διακοπή καλούμενου από κλήση SPIT 80
13.1.4 Επίπεδο 4. Λήψη κλήσης από τον καλούμενο 80
13.1.5 Επίπεδο 5. Ανάδραση από τον καλούμενο μετά την κλήση 80
13.2 Το επόμενο επίπεδο ενός συστήματος πρόληψης spit κλήσεων 82

14. ΙΣΧΥΟΥΣΑ ΚΑΤΑΣΤΑΣΗ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΛΗΣΕΩΝ SPIT 91

15. ΚΑΝΟΝΙΣΜΟΙ ΚΑΙ ΝΟΜΙΚΟΙ ΠΕΡΙΟΡΙΣΜΟΙ 93

16. ΣΧΟΛΙΑ – ΔΙΑΠΙΣΤΩΣΕΙΣ - ΣΥΜΠΕΡΑΣΜΑΤΑ..... 95

ΒΙΒΛΙΟΓΡΑΦΙΑ 97

Ευρετήριο πινάκων

Πίνακας 1. Λίστα αιτημάτων SIP
Πίνακας 2. Κωδικοί SIP απαντήσεων
Πίνακας 3. Περίληψη σύγκρισης κόστους συστημάτων spam κλήσεων

Ευρετήριο σχημάτων

Σχήμα 1. Αύξηση πώλησης IP-PBX παγκοσμίως
Σχήμα 2. Απλό παράδειγμα λειτουργίας VoIP
Σχήμα 3. Παράδειγμα τηλεφωνίας μέσω PSTN δικτύου
Σχήμα 4. Πραγματοποίηση τηλεφωνικής κλήσης με πρωτόκολλο SIP
Σχήμα 5α. Παραδείγματα ροής πραγματοποίησης και ολοκλήρωσης κλήσης με πρωτόκολλο SIP
Σχήμα 5β. Παραδείγματα ροής πραγματοποίησης και ολοκλήρωσης κλήσης με πρωτόκολλο SIP.
Σχήμα 6. Απεικόνιση ασφάλισης μηνύματος μέσω του μηχανισμού S/MIME
Σχήμα 7. Απεικόνιση διαδικασίας ασφάλισης μηνύματος με digest authentication
Σχήμα 8. TLS αυθεντικοποίηση
Σχήμα 9. Ασφάλεια με πρωτόκολλο Ipsec
Σχήμα 10. Αυθεντικοποιημένοι χρήστες, οι οποίοι χρήζουν πλέον εμπιστοσύνης
Σχήμα 11. Σχηματική απεικόνιση αρχιτεκτονικής των MIs ενός οργανισμού, και διεκπεραίωσης κλήσης μεταξύ τους
Σχήμα 12. Παράδειγμα SIP δήλωσης στοιχείων χρήστη στο MI
Σχήμα 13. Παράδειγμα εφαρμογής η οποία ζητάει αυθεντικοποίηση για να κάνει χρήση υπηρεσίας
Σχήμα 14. Διασύνδεση δήλωσης SAML και μηνύματος SIP
Σχήμα 15. Πλατφόρμα της Sun Microsystems. Φόρμα επιλογής μηχανισμού ασφάλειας
Σχήμα 16. Φόρμα δήλωσης ανακατεύθυνσης χρηστών σε περίπτωση σφάλματος SAML

Σχήμα 17. Packet sniffing συσκευές
Σχήμα 18. Packet sniffing freeware λογισμικό
Σχήμα 19. Λογισμικό παρακολούθησης φόρτου δικτύου, με στοιχεία και ιστορικό για κάθε τελικό χρήστη
Σχήμα 20. InviteReplay επίθεση εναντίων ενός SIP συνδρομητή της εταιρίας AT&T
Σχήμα 21. Απεικόνιση ροής μηνύματος InviteReplay επίθεσης κατά SIP τηλεφώνου
Σχήμα 22. Σχηματική απεικόνιση δικτύου, κατά την FakeBusy, ByeDelay, και ByeDrop επίθεση
Σχήμα 23. Σχηματική απεικόνιση ροής FakeBusy επίθεσης
Σχήμα 24. Ροή μηνυμάτων ByeDelay χρεώσιμης επίθεσης
Σχήμα 25. Σχηματική ροή μηνυμάτων ByeDrop billing Attack
Σχήμα 26. Πραγματοποίηση κλήσης SPIT μέσω της μεθόδου REFER
Σχήμα 27. Σενάριο SPIT κλήσης, μέσω ανωνυμίας στο SIP
Σχήμα 28. Γενική αρχιτεκτονική συστήματος αντιμετώπισης κλήσεων spit
Σχήμα 29. Φιλτράρισμα κλήσης κατά το δεύτερο επίπεδο ενός συστήματος πρόληψης SPIT (Turing Tests)
Σχήμα 30. Σχέδιο παλμών φωνής καλούντα και καλούμενου κατά την εκκίνηση μίας κλήσης
Σχήμα 31. Αντιμετώπιση SPIT κλήσεων ένα επίπεδο πριν το domain

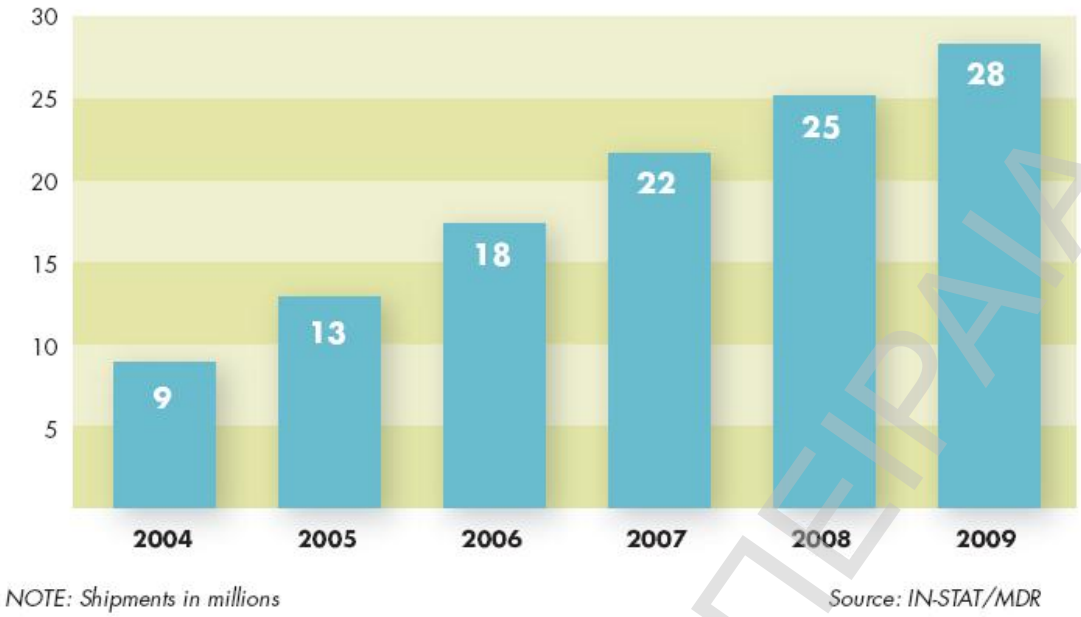
1. Εισαγωγή

Έχοντας πλέον αγγίξει τα όρια των δυνατοτήτων της γνωστής σε όλους μας δισύρματης συνδρομητικής τηλεφωνίας, καθίσταται επιτακτική η ανάγκη μετεξέλιξης της τηλεφωνίας σε ενός ανώτερου επιπέδου υπηρεσία.

Η νέας μορφής τηλεφωνία θα πρέπει να ανοίγει δυνατότητες οι οποίες ήδη έχουν τυπωθεί σαν ιδέες, και έχουν πλέον γίνει απαραίτητες ώστε να καλύψουν τις νέες επιχειρήσεις, αλλά και απλούς χρήστες καθώς και να ακολουθήσουν τους φρενήρεις ρυθμούς εξέλιξης των υπόλοιπων μέσων επικοινωνίας.

Το κενό αυτό, στον τομέα της τηλεφωνίας, ήρθε να καλύψει η διαδικτυακή τηλεφωνία (**V**oice **o**ver **IP**). Εκμεταλλευόμενη τις δωρεάν και τάχιστες πλέον υπηρεσίες που μας παρέχει το διαδίκτυο, η διαδικτυακή τηλεφωνία έχει αναπτυχθεί σε τέτοιο βαθμό, ώστε να είναι πλέον ικανή να καλύψει ανάγκες επαγγελματιών, καθώς και απλών χρηστών, χωρίς ιδιαίτερες τεχνικές γνώσεις.

Εύλογα πιστεύεται ότι η διαδικτυακή τηλεφωνία θα επηρεάσει τόσο την τηλεφωνία, όσο επηρέασε το ηλεκτρονικό ταχυδρομείο (email) την έγγραφη επικοινωνία. Η ανάπτυξή της είναι ραγδαία τα τελευταία έτη, με τις υπηρεσίες τις οποίες παρέχει, να γίνονται όλο και περισσότερες, καθώς και όλο πιο φιλικές προς τον τελικό χρήστη.



Σχήμα 1. Αύξηση πώλησης IP-PBX παγκοσμίως.

Τα νούμερα αναφέρονται σε εκατομμύρια πωλήσεις. Είναι φανερή η σθεναρή αύξηση της IP τηλεφωνίας.

Καθώς όμως η διαδικτυακή τηλεφωνία γίνεται όλο και πιο διαδεδομένη, είναι αναμενόμενο να δημιουργηθούν ταυτοχρόνως προβλήματα ασφάλειας, τα οποία αποτελούν και υψίστης σημασίας ζητήματα στην ευρεία εξάπλωσή της. Τα προβλήματα αυτά παρουσιάζονται κυρίως σε σενάρια επικοινωνίας εντός ενός IP δικτύου, και λιγότερο σε επικοινωνία ενός συνδρομητή διαδικτυακής τηλεφωνίας, και ενός ο οποίος είναι μέλος ενός συμβατικού τηλεφωνικού κέντρου.

Οι απειλές ασφάλειας στη διαδικτυακή τηλεφωνία (**SP**am over **I**nternet **T**elephony) πληθαίνουν διαρκώς. Από μία απλή κλήση η οποία θα χρεώσει κάποιον συνδρομητή χωρίς αυτός να το επιθυμεί, έως ένα συντονισμένο καταιγισμό ανεπιθύμητων κλήσεων, ο οποίος είναι ικανός να μειώσει την απόδοση ενός τηλεφωνικού κέντρου στο ελάχιστο.

Οι απειλές αυτές μπορεί να προέρχονται από ένα φυσικό χρήστη (κακοπροαίρετο), καθώς και από αυτοματοποιημένες συσκευές οι οποίες είναι κατασκευασμένες γι' αυτόν ακριβώς το σκοπό. Δυστυχώς, οι νομικοί

περιορισμοί οι οποίοι εφαρμόζονται σε διάφορα κράτη, δεν είναι πάντα αποτελεσματικοί στην πάταξη του φαινομένου αυτού. Γι' αυτό το λόγο είναι επιτακτική η ανάγκη εύρεσης τρόπων αντιμετώπισης του φαινομένου.

Σκοπός του εγγράφου αυτού, είναι η παρουσίαση των απειλών κατά τις ορθής λειτουργίας της διαδικτυακής τηλεφωνίας, οι ιδιαιτερότητες των απειλών αυτών καθώς και οι συνεχείς προκλήσεις όσων αφορά τον τομέα της ασφάλειας. Θα δοθεί μία γενική άποψη λειτουργίας της διαδικτυακής τηλεφωνίας, των δημοφιλέστερων πρωτοκόλλων τα οποία εφαρμόζονται, και θα εξετασθούν διάφορες προσεγγίσεις όσον αφορά το θέμα ασφάλειας επί VoIP.

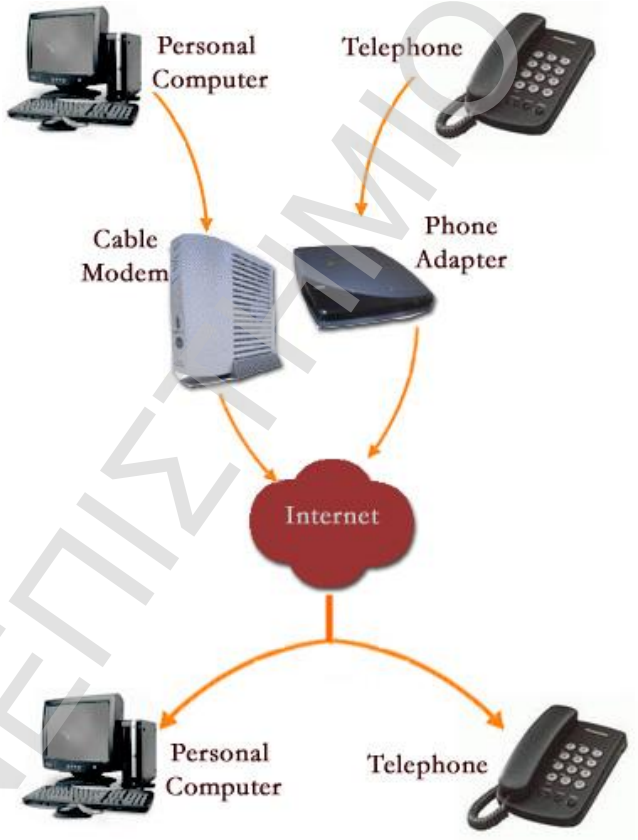
2. Διαφορές μεταξύ Voice over IP και PSTN τηλεφωνικού κέντρου.

Η διαδικτυακή τηλεφωνία, όπως τη γνωρίζουμε σήμερα, έχει θεμελιώδεις διαφορές σε σχέση με τα συμβατικά PSTN δίκτυα (**P**ublic **S**witched **T**elephone **N**etwork):

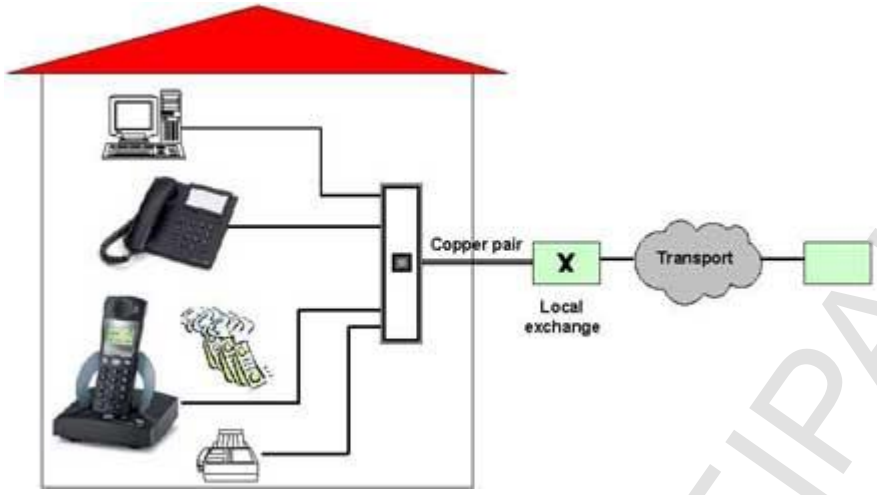
- Σε ένα συμβατικό δίκτυο, η σηματοδότηση γίνεται σε ένα διακριτό, αυτόνομο και κλειστό δίκτυο. Η διαδικασία όμως αυτή σε ένα VoIP δίκτυο γίνεται σε ένα εκτεθειμένο, ανοιχτό, και πλήρως αναξιόπιστο δίκτυο (π.χ. στο internet), όπου οι επιθέσεις και τα προβλήματα ασφάλειας είναι σαφώς εντονότερα.
- Οι παραδοσιακές τηλεφωνικές συσκευές, που χρησιμοποιούνται εδώ και χρόνια, είναι απλές συσκευές με περιορισμούς στις δυνατότητες και τη χρηστικότητά τους. Οι τερματικές συσκευές όμως ενός VoIP δικτύου, από την άλλη πλευρά, αποτελούν σύνθετες συσκευές με δικές τους, ξεχωριστές ρυθμίσεις πρωτοκόλλου TCP/IP. Οι δυνατότητές τους είναι πολύ μεγαλύτερες από τις κλασσικές τηλεφωνικές συσκευές, και οι επιλογές που προσφέρουν σε ένα χρήστη, είναι εντυπωσιακές.
- Ένα VoIP δίκτυο προσφέρει φορητότητα. Ένας χρήστης VoIP δικτύου, μπορεί να αλλάξει την τοποθεσία από όπου καλεί, να μεταφέρει σε άλλο σημείο του δικτύου την τερματική του συσκευή, χωρίς καμία επίδραση στη λειτουργία της, καθώς εξακολουθεί να διατηρεί την ταυτότητά του στο δίκτυο. Το μόνο που χρειάζεται ένας VoIP συνδρομητής, είναι απλά πρόσβαση στο διαδίκτυο. Αυτό δεν συμβαίνει όμως με ένα συνδρομητή PSTN δικτύου, καθώς τέτοιου τύπου δίκτυα δεν παρέχουν καμίας μορφής φορητότητα.
- Λόγω του ότι δεν παρέχεται το προνόμιο της φορητότητας σε ένα PSTN δίκτυο, δεν απαιτείται και αυθεντικοποίηση του χρήστη από το δίκτυο. Με αυτό τον τρόπο οποιοσδήποτε έχει φυσική πρόσβαση σε μία απλή πρίζα του δικτύου, είναι και σε θέση να κάνει χρήση της γραμμής αυτής. Καθώς όμως σε ένα VoIP δίκτυο ένας χρήστης έχει τη δυνατότητα να συνδεθεί από οπουδήποτε μέσω διαδυκτίου, απαιτείται επιπλέον αυθεντικοποίησή του προτού εισαχθεί στο δίκτυο.

Η πλειοψηφία των προβλημάτων ασφαλείας, τα οποία συναντάμε στα VoIP δίκτυα, προκύπτει από τις προαναφερθείσες διαφορές τους με τα PSTN δίκτυα. Αυτό επαληθεύεται διαρκώς, με το ολοένα και αυξανόμενο πλήθος κλήσεων, οι οποίες προέρχονται από το διαδίκτυο.

Από μία άλλη οπτική γωνία, λαμβάνοντας υπ' όψη τις ιδιαιτερότητες της φορητότητας και της αυθεντικοποίησης, θα μπορούσε κάποιος να παρομοιάσει τη VoIP τηλεφωνία, με τηλεφωνικό δίκτυο κινητής τηλεφωνίας τύπου GSM. Παρ' όλα αυτά, τα GSM δίκτυα διαφέρουν από τα VoIP, καθώς τα πρώτα χρησιμοποιούν έξυπνες κάρτες (smartcards) στις τερματικές τους συσκευές και αποτελούνται από έναν γνωστό και περιορισμένο αριθμό πάροχων μεταξύ των οποίων υπάρχει εμπιστοσύνη.



Σχήμα 2. Απλό παράδειγμα λειτουργίας VoIP.



Σχήμα 3. Παράδειγμα τηλεφωνίας μέσω PSTN δικτύου.

3. Το πρωτόκολλο SIP

Η υπάρχουσα διαδικτυακή τηλεφωνία, και η διαδικασία χρέωσης σε αυτή, βασίζεται στη μέθοδο της σηματοδοσίας. Το SIP (**S**ession **I**nitiation **P**rotocol) αποτελεί το επικρατέστερο πρωτόκολλο σηματοδοσίας στη διαδικτυακή τηλεφωνία, και χρησιμοποιείται ευρέως σε επιχειρησιακά και μη δίκτυα. Ως εκ τούτου, η οποιαδήποτε ευπάθεια του πρωτοκόλλου αυτού, συνεπάγεται ταυτόχρονα ένα ευπρόσβλητο VoIP τηλεφωνικό δίκτυο.

Θα εξετασθούν στη συνέχεια, ο τρόπος λειτουργίας του SIP πρωτοκόλλου, και πως οι όποιες ευπάθειες του πρωτοκόλλου SIP μπορούν να καταπολεμηθούν, ώστε να εξασφαλίσουμε τη σταθερότητα και την αξιοπιστία των VoIP δικτύων, όταν αυτά βασίζονται στο πρωτόκολλο αυτό. Συγκεκριμένα, θα εστιάσουμε στις χρεώσιμες επιθέσεις, οι οποίες δημιουργούν ασυνέπεια στο λόγο του τι αιτήθηκε κάποιος συνδρομητής, προς το τι, εν τέλει, του προσεφέρθει από τον πάροχο.

3.1 Σηματοδότηση με το πρωτόκολλο SIP

Το πρωτόκολλο SIP, έχει καθοριστεί από τον οργανισμό IETF (**I**nternet **E**ngineering **T**ask **F**orce) ως το πρότυπο πρωτόκολλο σηματοδοσίας και ελέγχου πολυμέσων και επικοινωνιών μέσω IP. Δεν είναι βέβαια το μόνο πρωτόκολλο το οποίο χρησιμοποιείται στις IP επικοινωνίες. Το SDP (**S**ession **D**escription **P**rotocol**)**, χρησιμοποιείται για την επιλογή παραμέτρων, όπως οι αποκωδικοποιητές (codecs) και ο τύπος πολυμέσου (media type), με σκοπό την εκπομπή.

Εφόσον έχει πραγματοποιηθεί μία κλήση μέσω SIP, η εκπομπή γίνεται ουσιαστικά μέσω του πρωτοκόλλου *RTP* (**R**eal-time **T**ransfer **P**rotocol). Καθώς το πρωτόκολλο SIP χρησιμοποιείται για την εκκίνηση μίας συνεδρίας, και λόγω του ότι τις αρκετά συχνά απαιτούνται ασφαλείς συνεδρίες, οι οποίες ενδέχεται να περιέχουν εμπιστευτικές πληροφορίες, η ασφάλεια του SIP πρωτοκόλλου καθίσταται υψίστης σημασίας αντικείμενο στην ασφάλεια της VoIP τηλεφωνίας.

Το SIP αποτελεί ένα client-server πρωτόκολλο, το οποίο παρουσιάζει ομοιότητες με το HTTP πρωτόκολλο. Η σηματοδοσία βασίζεται σε μηνύματα κειμένου. Ένα μήνυμα αποτελείται από τον προπομπό (header), και το κυρίως τμήμα. Τα μηνύματα αποτελούν αιτήματα ή αποκρίσεις αιτημάτων. Στην περίπτωση που μία SIP οντότητα, δεχτεί ένα αίτημα, πραγματοποιείται η αντίστοιχη ενέργεια, και επιστρέφεται μία απάντηση στον ιδιοκτήτη του αιτήματος. Οι απαντήσει αυτές είναι στην ουσία τριψήφιοι κωδικοί, οι οποίοι δηλώνουν κάποια κατάσταση.

Παρακάτω εμφανίζονται δύο πίνακες, οι οποίοι περιέχουν αιτήματα SIP (πίνακας 1), και λίστα κωδικών απαντήσεων του SIP πρωτοκόλλου στα διάφορα αιτήματα (πίνακας 2).

SIP Request	Description
INVITE	*Initiates a call signalling sequence*
BYE	*Terminates a session*
ACK	*Acknowledge*
OPTIONS	*Queries a server about its capabilities*
CANCEL	*Used to cancel a request in progress*
REGISTER	*Used to register location information at a registrar*

Πίνακας 1. Λίστα αιτημάτων SIP

SIP Response Codes
1xx - informational
2xx - ok
3xx - redirection
4xx - client error
5xx - server error
6xx - global failure

Πίνακας 2. Κωδικοί SIP απαντήσεων

Η διευθυνσιοδότηση στο πρωτόκολλο SIP πραγματοποιείται μέσω σταθερών αναγνωριστών (URIs[1]). Ένας τέτοιος αναγνωριστής (SIP-URI) θα μπορούσε να παρομοιασθεί με μία διεύθυνση ηλεκτρονικού ταχυδρομείου, του τύπου : ΄΄sip:user@domain΄΄. Στο SIP υπάρχουν καθορισμένες (λογικές) οντότητες όπως user agent, proxy, registrar, redirect server και location server. Ένας user agent αποτελεί ένα τερματικό, το οποίο λαμβάνει μέρος στην όλη διαδικασία της SIP επικοινωνίας (αυτό μπορεί να είναι software ή hardware). Ο proxy δέχεται μηνύματα, και τα προωθεί σε κάποια άλλη SIP οντότητα. Ο redirect server έχει ως καθήκον να ανακατευθύνει τον αποστολέα του μηνύματος σε κάποια άλλη SIP οντότητα, αντί να κάνει ανακατεύθυνση του μηνύματος.

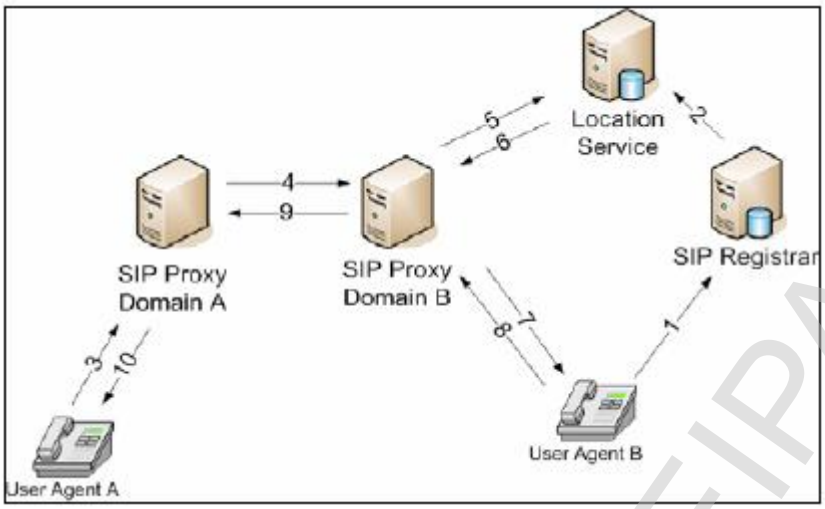
[1] Uniform resource Identifiers

Οι users μπορούν να δηλώσουν την τρέχουσα τοποθεσία τους (π.χ. IP διεύθυνση) μέσω του registrar του domain τους. Ένας location server χρησιμοποιείται από έναν registrar ώστε να αποθηκεύει την τοποθεσία των χρηστών, τη σύνδεση δηλαδή ενός SIP-URI με την τρέχουσα IP διεύθυνση. Ο location server παρέχει έναν κατάλογο όπου οι SIP οντότητες μπορούν να ανατρέχουν για εύρεση της τρέχουσας τοποθεσίας ενός συγκεκριμένου SIP-URI. Προφανώς κάτι τέτοιο προσφέρει φορητότητα.

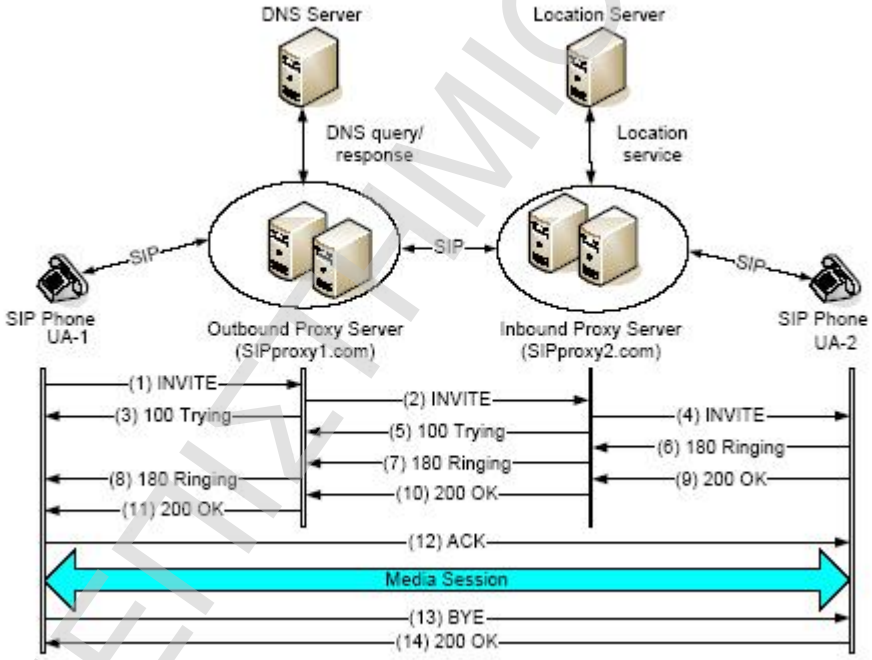
3.2 Πραγματοποίηση απλής φωνητικής κλήσης με το πρωτόκολλο SIP

Η πραγματοποίηση μίας φωνητικής κλήσης μεταξύ δύο συνδρομητών φαίνεται στο σχήμα 4. Στο συγκεκριμένο παράδειγμα, οι χρήστες (user agents) A και B βρίσκονται σε διαφορετικά domains και διαθέτουν ξεχωριστούς proxies.

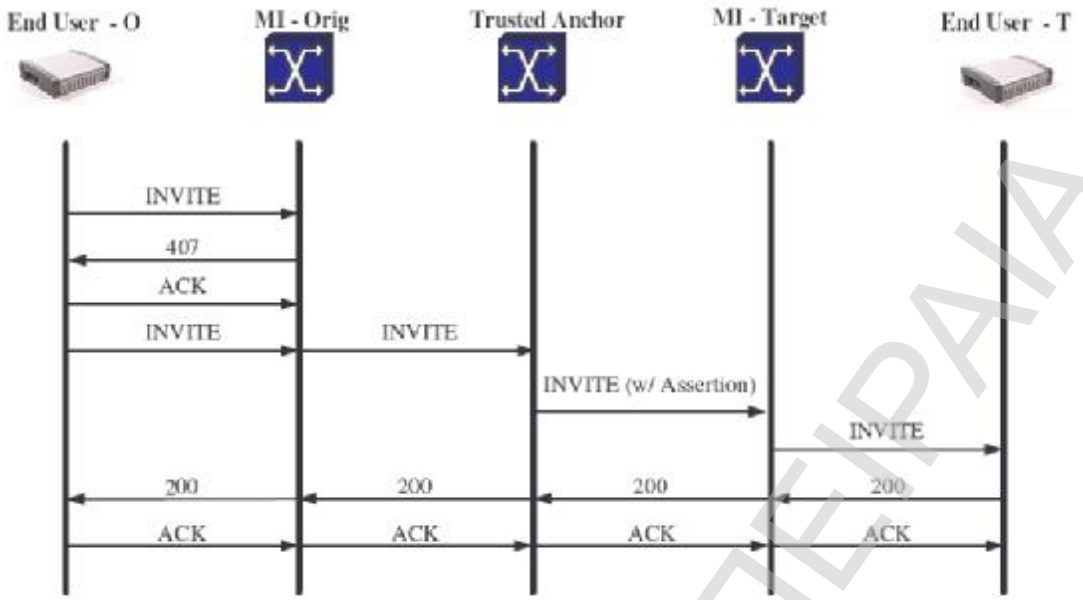
Αρχικά, ο αιτών την κλήση, χρήστης B, πρέπει να εγγραφεί μέσω του τοπικού του registrar (1), ώστε να είναι σε θέση να λαμβάνει κλήσεις. Ο registrar αποθηκεύει τις πληροφορίες της τοποθεσίας του στον location server (2). Όταν ο χρήστης A αποφασίσει να καλέσει τον B, στέλνει ένα INVITE αίτημα στον τοπικό SIP-proxy (3), ο οποίος προωθεί το αίτημα (ίσως κατόπιν ενός ελέγχου DNS) στον proxy του domain του χρήστη B (4). Ο proxy του domain B θα πρέπει εν συνεχεία να ελέγξει την IP διεύθυνση του χρήστη B, στον location server (5, 6), προτού στείλει το αίτημα στον user agent B (7). Το απαντητικό μήνυμα του χρήστη A, θα διατρέξει την ίδια διαδρομή προς την αντίθετη κατεύθυνση (8, 9, 10).



Σχήμα 4. Πραγματοποίηση τηλεφωνικής κλήσης με πρωτόκολλο SIP.



Σχήμα 5α. Παραδείγματα ροής πραγματοποίησης και ολοκλήρωσης κλήσης με πρωτόκολλο SIP.



Σχήμα 5β. Παραδείγματα ροής πραγματοποίησης και ολοκλήρωσης κλήσης με πρωτόκολλο SIP.

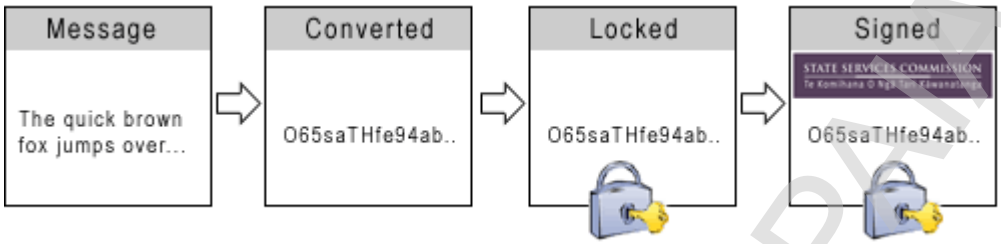
3.3 Ασφάλεια πρωτοκόλλου SIP

Η ασφάλεια του πρωτοκόλλου SIP, βασίζεται κατά ένα πολύ μεγάλο μέρος στους ήδη υπάρχοντες μηχανισμούς ασφαλείας HTTP και SMTP. Οι καθιερωμένοι μηχανισμοί ασφάλειας, οι οποίοι χρησιμοποιούνται από το SIP αναλύονται παρακάτω.

3.3.1 S/MIME (Secure/Multipurpose Internet Mail Extensions)

Ανεπτύχθη από τον αμερικάνικο οργανισμό RSA Data Security Inc., ο οποίος εδρεύει στη Μασαχουσέτη, και παρέχει ασφάλεια μέσω συστήματος κρυπτογράφησης, σε εφαρμογές ανταλλαγής γραπτών μηνυμάτων. Προσφέρει ασφάλεια στην αυθεντικοποίηση, στην ακεραιότητα του μηνύματος, και την προέλευσή του, μέσω της κρυπτογράφησής του.

Στο παρακάτω σχήμα απεικονίζεται η μέθοδος ασφάλισης ενός μηνύματος μέσω του μηχανισμού ασφάλειας S/MIME.



Σχήμα 6. Απεικόνιση ασφάλισης μηνύματος μέσω του μηχανισμού S/MIME.

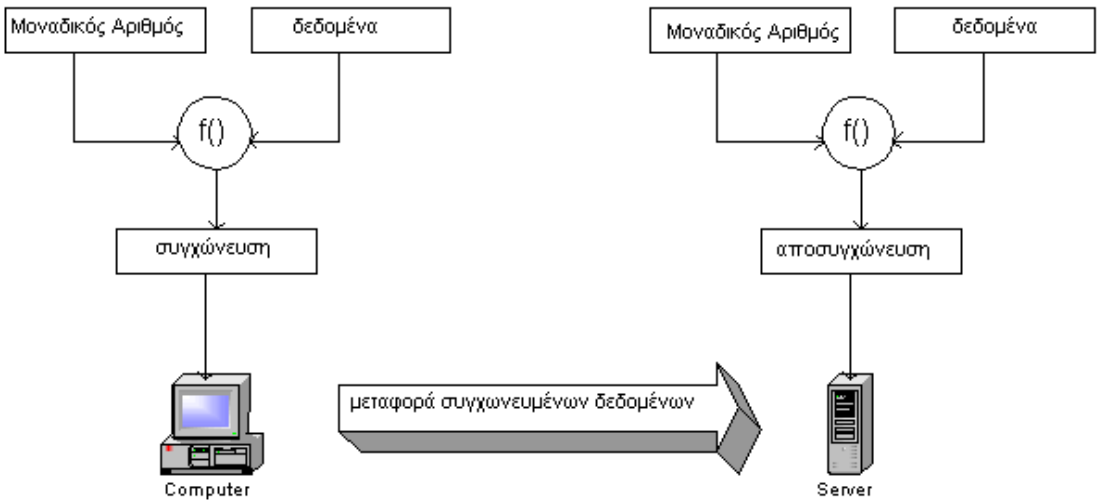
Αρχικά γίνεται η μετατροπή του ανοιχτού κειμένου, σε κώδικα το οποίο μόνο ο παραλήπτης είναι ικανός να μεταφράσει. Στη συνέχεια, το μήνυμα ασφαλίζεται ώστε να αποφευχθεί η οποιαδήποτε κακόβουλη επέμβαση. Εν τέλει, το μήνυμα σηματοδοτείται ώστε να μπορεί να αποδειχθεί η προέλευσή του.

3.3.2 Digest Authentication

Οι SIP οντότητες οι οποίες μοιράζονται από κοινού κάποια εμπιστευτική πληροφορία, όπως για παράδειγμα ένα password, μπορούν να επιτυγχάνουν αυθεντικοποίηση μεταξύ τους μέσω ενός μηχανισμού ο οποίος απαντά σε αιτήματα που του δηλώνονται. Για να αποφευχθούν επιθέσεις οι οποίες επαναλαμβάνουν το αμέσως προηγούμενο αίτημα, ώστε να αυθεντικοποιηθούν, ο μηχανισμός αυτός χρησιμοποιεί ένα μοναδικό αριθμό σε κάθε αίτημα, ο οποίος καθιστά κάθε διαδικασία αυθεντικοποίησης μοναδική.

Στο σχήμα που ακολουθεί, φαίνεται σχηματικά η διαδικασία εισαγωγής του μοναδικού αριθμού στο μήνυμα, η μεταφορά του, και στη συνέχεια

ο διαχωρισμός του μηνύματος από τον μοναδικό αριθμό που είχε εισαχθεί.

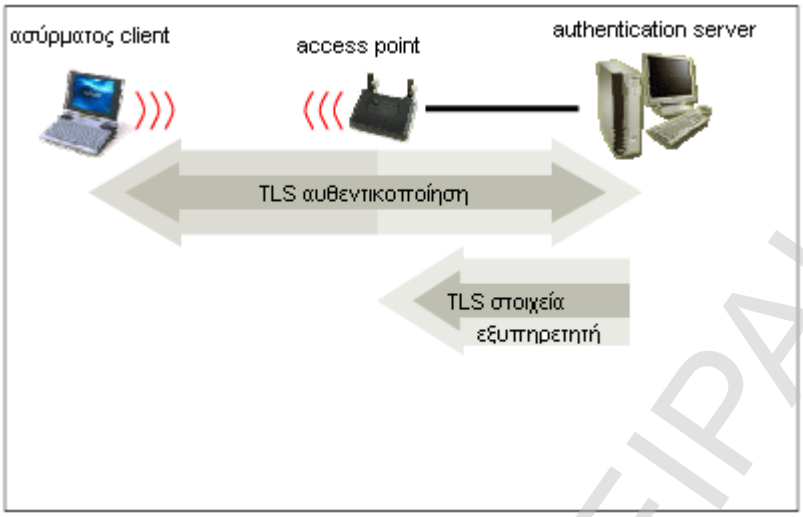


Σχήμα 7. Απεικόνιση διαδικασίας ασφάλισης μηνύματος με digest authentication.

3.3.3 TLS & IPSec (Transport Layer Security & Internet Protocol Security)

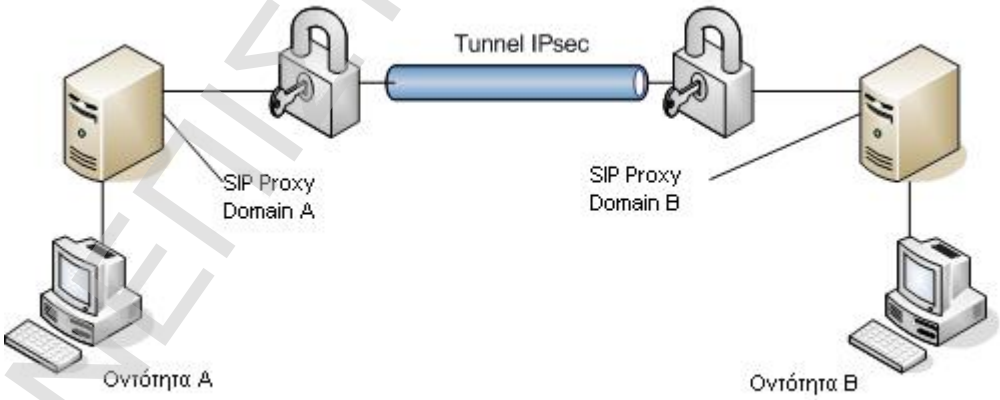
Η βήμα προς βήμα ασφάλεια για τη διαδικασία της σηματοδοσίας μέσω SIP, μπορεί να επιτευχθεί είτε στο επίπεδο μεταφοράς (transport layer), ή στο επίπεδο δικτύου (network layer).

Το πρωτόκολλο TLS παρέχει ασφάλεια στα δύο άκρα ενός επικοινωνιακού δίαυλου στο ευρύ διαδίκτυο επιτυγχάνοντας κρυπτογράφηση. Συγκεκριμένα, γίνεται αυθεντικοποίηση μόνο του εξυπηρετητή, ενώ ο πελάτης παραμένει μη αυθεντικοποιημένος. Κάτι τέτοιο σημαίνει ότι ο τελικός χρήστης, ο οποίος μπορεί να είναι ένα φυσικό πρόσωπο, μία εφαρμογή, ή ένας browser, μπορεί να είναι βέβαιος για το ότι επικοινωνεί με αυτόν το οποίο επιθυμεί και όχι με κάποιον κακόβουλο εισβολέα.



Σχήμα 8. TLS αυθεντικοποίηση.

Το IPSec πρωτόκολλο δρα σε επίπεδο δικτύου (OSI Model επίπεδο 3), πράγμα το οποίο το καθιστά εξαιρετικά ευέλικτο και εύχρηστο, καθώς μία εφαρμογή δεν απαιτεί την εξ αρχής σχεδίασή της βάση αυτού του πρωτοκόλλου. Αυτό το κάνει να διαφέρει από πρωτόκολλα όπως το SSL (Secure Shell Protocol), το οποίο απαιτεί την ενσωμάτωσή του στον αρχικό σχεδιασμό μίας εφαρμογής, καθώς δρα σε υψηλότερο επίπεδο OSI.



Σχήμα 9. Ασφάλεια με πρωτόκολλο Ipsec.

4. Voice over IP και SPAM

Το **SPAM** γενικότερα συναντάται σε μορφή μεγάλου μεγέθους αυτόκλητα emails, τα οποία αποστέλλονται με μοναδικό σκοπό τη σύγχυση, ή πρόκληση βλάβης ενός συστήματος. Θεωρείται ως ένα από τα σημαντικότερα προβλήματα του διαδικτύου αυτή τη στιγμή, παράλληλα με την ευρεία αύξηση των διαφόρων ιών που κατακλύζουν τη διαδικτυακή κοινότητα. Παράλληλα με την άφιξη, και ευρεία εφαρμογή της διαδικτυακής τηλεφωνίας, ήταν αναμενόμενο να κάνει και σε αυτό το χώρο την εμφάνισή της μία αντίστοιχη μορφή spam.

Η απειλή αυτή, η οποία είναι γνωστή ως **SPIT** (SPam over Internet Telephony), ορίζεται ως τη μεταβίβαση αυτόκλητων κλήσεων μέσω του δικτύου διαδικτυακής τηλεφωνίας. Το spam στη διαδικτυακή τηλεφωνία αναμένεται να αποτελέσει ένα ακόμη εντονότερο πρόβλημα στο προσεχές μέλλον. Δυστυχώς, υπάρχουν οι προοπτικές να εξελιχθεί το spam over internet telephony σε ένα πολύ μεγαλύτερο πρόβλημα από ότι το email spam, καθώς ο συνδρομητής ενοχλείται, και διαταράσσεται η επικοινωνία του από κάθε ληφθείσα spit κλήση. Η πιθανότητα μείωσης της απόδοσης, συστήματος και χρήστη, είναι πολύ μεγαλύτερη στην περίπτωση του spit, εν συγκρίσει με το spam, καθώς στην πρώτη περίπτωση η διαταραχή γίνεται άμεσα στον συνδρομητή μέσω τηλεφωνικής κλήσης. Η αμεσότητα αυτή της ενόχλησης, είναι που καθιστά και το spit, ως μία σύγχρονη απειλή στον τομέα των ενσύρματων επικοινωνιών, ιδίως σε περιπτώσεις όπου οι ασφαλής και απρόσκοπτη επικοινωνία, είναι ζωτικής σημασίας.
Μία εκδοχή μετάδοσης αυτόκλητων κλήσεων, υφίσταται ήδη στα συμβατικά PSTN δίκτυα. Τέτοιου είδους κλήσεις συναντάμε συνήθως σε περιπτώσεις τηλεπωλήσεων, όπου αδιακρίτως δρομολογούνται κλήσεις, πολλές φορές αυτοματοποιημένα, με μόνο σκοπό την προώθηση προϊόντων.

Άξια αναφοράς είναι η υπ αριθμόν 2002/58/EC οδηγία του Ευρωπαϊκού κοινοβουλίου[2], οποία αφορά την τηλεφωνική προώθηση προϊόντων.

[2] Οδηγία περί προσωπικών δεδομένων και ηλεκτρονικών Επικοινωνιών 2002/58/EC του Ευρωπαϊκού κοινοβουλίου και συμβουλίου, της 12 Ιουλίου 2002.

Σύμφωνα με την προαναφερθείσα οδηγία, δεν επιτρέπεται η χρήση αυτόματων τηλεφωνικών μηχανών και μηχανών αποστολής fax, χωρίς προηγούμενη συγκατάθεση του συνδρομητή-καταναλωτή. Οι προτεινόμενες επιλογές είναι, είτε η προεπιλεγμένη απόρριψη παρόμοιων κλήσεων, εκτός και αν ο συνδρομητής επιλέξει την αποδοχή τους, ή η αποδοχή τέτοιων κλήσεων έως ότου ο συνδρομητής εκφράσει την επιθυμία του να πάψει να τις δέχεται. Το Ηνωμένο Βασίλειο , παραδείγματος χάριν, έχει επιλέξει τη δεύτερη εκδοχή[3].

Το αυξημένο κόστος των PSTN κλήσεων, εν συγκρίσει με το μηδαμινό κόστος των VoIP δικτύων, αποτελεί επίσης αποτρεπτικό παράγοντα στην εξάπλωση του spam στα συμβατικά τηλεφωνικά δίκτυα. Αυτό είναι και ένα σημαντικό αίτιο εξάπλωσης του spam στη διαδικτυακή τηλεφωνία. Μία πρόσφατη μελέτη[4] έδειξε ότι το spam σε PSTN δίκτυο είναι συνολικά τρεις φορές πιο δαπανηρό από ότι το SPIT.

Δυστυχώς η φύση του SPIT είναι πολύ διαφορετική σε σχέση με του mail spam, γεγονός που καθιστά τις όποιες μεθόδους πρόληψης mail spam, ανεφάρμοστες στην περίπτωση του SPIT. Ιδιαζόντως, το περιεχόμενο μίας SPIT κλήσης, δεν μπορεί να ελεγχθεί προτού ο συνδρομητής διαταραχθεί από μία SPIT κλήση.

[3] Θεσμοθετημένη πράξη 2003, υπ αριθμόν 2426, υπουργείου επικοινωνιών Ηνωμένου Βασιλείου.
[4] J.Rosenberg. “The Session Initiation Protocol (SIP) and Spam”. Ιούλιος 2005

5. Email SPAM και SPIT. Κοινά σημεία και διαφορές

Κάνοντας μία σύγκριση email spam και SPIT, διαπιστώνουμε διαφορές οι οποίες οι οποίες βοηθούν να αντιληφθούμε την έκταση της απειλής του spam στη διαδικτυακή τηλεφωνία, καθώς και το πόσο επιτακτική είναι η ανάγκη ανάπτυξη νέων μεθόδων αντιμετώπισής της.

Η περίπτωση του SPIT, αποτελεί μία πολύ μεγαλύτερη απειλή σε σχέση με το email spam, καθώς κατά το SPIT υπάρχει άμεση επίδραση στον χρήστη. Μία κλήση SPIT προκαλεί ενεργοποίηση της προσωπικής τηλεφωνικής συσκευής του συνδρομητή με συνέπεια ενόχληση και φόρτο δικτύου. Αντίθετα, στην περίπτωση του email spam, ένα τέτοιο email τοποθετείται σε ένα σωρό, όπου και θα παραμείνει, έως ότου ο χρήστης ανατρέξει στον σωρό αυτό και ελέγξει για νέα email. Ακόμη όμως και στην περίπτωση αυτή, ο χρήστης έχει τη δυνατότητα να διακρίνει απευθείας, εμπειρικά από κάποιο σημείο κι έπειτα, τα spam emails και να τα διαγράψει ομαδικώς. Κάτι τέτοιο δεν επηρεάζει ούτε τον ίδιο, αλλά ούτε και το σύστημά του, καθώς τα νέα emails καταχωρούνται πιθανώς σε κάποιον αυτόνομο mail server.

Ένα επιπρόσθετο πρόβλημα, όσων αφορά το SPIT, αποτελεί το γεγονός ότι ελάχιστες από τις υπάρχουσες τεχνικές αντιμετώπισης email spam μπορούν να εφαρμοσθούν και στην αντιμετώπιση του SPIT.
Αυτό συμβαίνει καθώς:

- Η χρονική κλίμακα είναι εντελώς διαφορετική στις δύο περιπτώσεις. Ενώ κατά το SPIT έχουμε να κάνουμε με μία απειλή πραγματικού χρόνου, δεν συμβαίνει κάτι τέτοιο και στο email spam.
- Μία από τις αποτελεσματικότερες μεθόδους αντιμετώπισης email spam, αυτή κατά την οποία γίνεται έλεγχος περιεχομένου του spam mail, είναι ανεφάρμοστη στην περίπτωση του SPIT, καθώς το περιεχόμενο μίας spam κλήσης δεν δύναται να ανιχνευθεί προτού απαντηθεί η κλήση.
- Δεν είναι εφικτό να γίνει ανάλυση του περιεχομένου μιας κλήσεως προτού αυτή εξυπηρετηθεί, κάτι το οποίο οποίο συμβαίνει κατά τη

διαδικασία του email filtering. Η απόφαση αποδοχής ή απόρριψης της κλήσης, πρέπει να γίνει σε πραγματικό χρόνο. Ακόμη όμως και αν κάτι τέτοιο ήταν εφικτό, υπάρχουν νομικοί φραγμοί οι οποίοι δρουν αποτρεπτικά στο να εφαρμοσθεί αυτή η λύση.

Ένας επικουρικός παράγοντας, ο οποίος μας δίνει μία γενική εποπτεία του πόσο θα εξαπλωθεί το spam στη διαδικτυακή τηλεφωνία, είναι το κατά πολύ μικρότερο κόστος του SPIT, εν συγκρίσει με το spam σε PSTN δίκτυο. Μία απλή ανάλυση κόστους, είναι ικανή να μας δείξει πόση είναι η διαφορά μεταξύ spam σε PSTN δίκτυο, και στο ανοιχτό διαδίκτυο. Υπάρχουν τρία διακριτά επίπεδα, στα οποία είναι αναμενόμενη η διαφορά κόστους:

- Το κόστος ενός συστήματος όσων αφορά το λογισμικό.
- Το κόστος συστήματος από τη σκοπιά του hardware.
- Το κόστος ανά κλήση spam.

Παρά το ότι το συγκριτικό κόστος στο επίπεδο του λογισμικού είναι σε γενικές γραμμές ίδιο, δεν συμβαίνει κάτι τέτοιο στο επίπεδο του hardware. Σε αυτή την περίπτωση, η ζυγαριά γέρνει αισθητά προς την πλευρά του PSTN δικτύου, καθώς οι PSTN κάρτες είναι πολύ πιο δαπανηρές από μία απλή κάρτα δικτύου όπου απαιτείται στην περίπτωση του SPIT.

Εξετάζοντας το τρίτο επίπεδο, και πάλι το SPIT υπερτερεί οικονομικά, καθώς το κόστος διασυνδέσεων σε PSTN δίκτυο είναι πολλαπλάσιο αυτών σε ένα VoIP.
Συμπερασματικά, κάνοντας αυτή την ανάλυση κόστους, διαπιστώνουμε ποια μορφή spam θα διάλεγε ο οποιοσδήποτε κακόβουλος spammer.

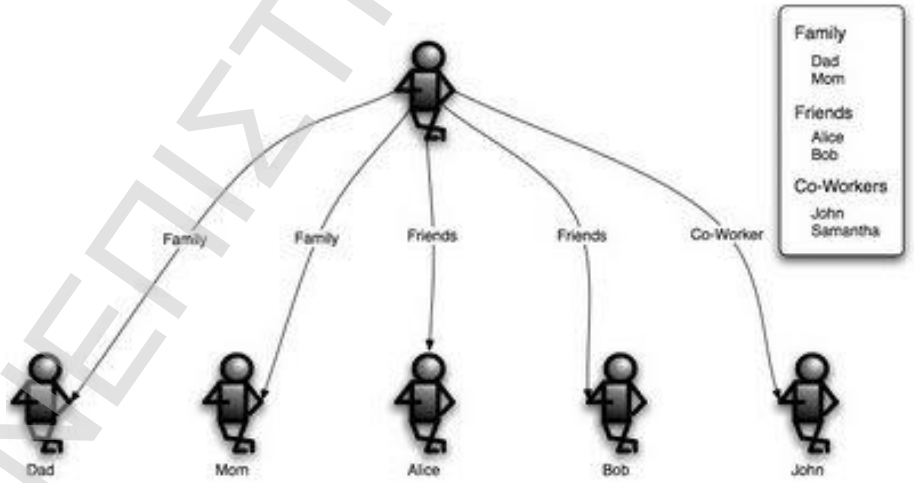
Costs	SPAM over PSTN	SPIT	Additional considerations
Software costs	X	X	X is depending on the signaling protocol
Hardware costs	10 Y - 100 Y	Y	Y is independent of the signaling protocol
Costs per spam call	about 1000 Z	Z	Z is independent of the signaling protocol

Πίνακας 3. Περίληψη σύγκρισης κόστους συστημάτων spam κλήσεων.

6. Οι ομοσπονδίες των MIs (Member Islands)

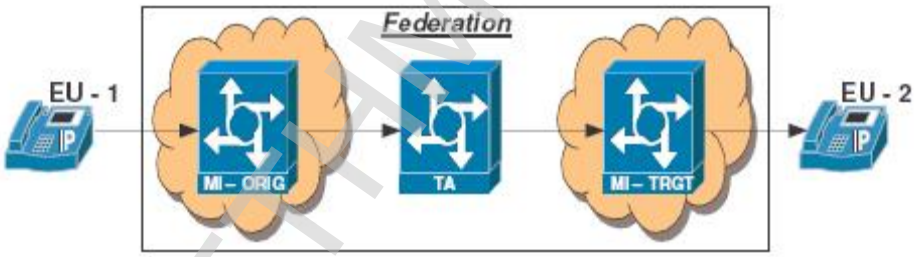
Το MI (Member Island) αποτελεί έναν συνονθυλευτικό οργανισμό, ο οποίος είναι υπεύθυνος για μία ομάδα (group) τελικών χρηστών (end users). Ένα MI θα μπορούμε κάλλιστα να είναι ένας Internet Telephony Service Provider (ITSP) ή μία επιχείρηση με εγκατεστημένο VoIP τηλεφωνικό κέντρο. Τα τυπικά VoIP σύνορα ενός MI περιορίζονται σε έναν SIP Proxy, ένα IP-PBX, ή έναν Session Border Controller ο οποίος ρυθμίζει τις δυνατότητες επέκτασης κάθε συνδρομητή.

Οι σχέσεις εμπιστοσύνης κάθε MI είναι συγκεκριμένης φύσεως και δέχονται τους περιορισμούς του εκάστοτε οργανισμού στον οποίο ανήκουν. Έναν τέτοιο περιορισμό μπορεί να αποτελεί η απαγόρευση επικοινωνίας ενός MI με άλλο. Οι πολιτικές ασφάλειας ορίζονται από μία κεντρική αρχή, γνωστή ως TA (Trust Anchor), η οποία και είναι υπεύθυνη για την εγκαθίδρυση δεδομένων ασφάλειας και εμπιστοσύνης στον εκάστοτε οργανισμό. Η ανάγκη για την οροθέτηση αυτή, προέκυψε από την αναγκαιότητα των MIs να μεταφέρουν ανώνυμα και με ασφάλεια δεδομένα, σηματοδοσίες, και άλλα πιστοποιητικά, δίχως αυτά να “υποκλέπτονται”.



Σχήμα 10. Αυθεντικοποιημένοι χρήστες, οι οποίοι χρήζουν πλέον εμπιστοσύνης.

Οι σχέσεις εμπιστοσύνης διατηρούνται από την TA, την κεντρική αρχή ενός οργανισμού, καθώς αυτή είναι παράλληλα υπεύθυνη για την πιστοποίηση πληροφοριών ασφάλειας σχετικά με την ταυτότητα του καλούντος, και την κανονικοποίησή[5] τους έτσι ώστε αυτές να φθάσουν στο επιθυμητό MI, και κατά συνέπεια στον τελικό χρήστη, μέσω μίας και μόνο κλήσης. Η κεντρική αρχή TA είναι υπεύθυνη για την ενημέρωσή της σχετικά με την εκάστοτε πολιτική των MIs, και είναι αυτή η οποία θα πρέπει να διαθέτει εγκατεστημένους μηχανισμούς, οι οποίοι θα παρέχουν βήμα προς βήμα προστασία των δεδομένων. Οι μηχανισμοί αυτοί, γνωστοί ως hop-by-hop data integrity mechanisms, θα πρέπει να διασφαλίζουν ασφαλείς κλήσεις μεταξύ των μελών ενός οργανισμού, και σχέσεις εμπιστοσύνης μεταξύ MI και TA, και αντιστρόφως. Αναφέροντας τέτοιου είδους μηχανισμούς, περιλαμβάνουμε συνήθως TLS ή VPN/IPSEC.



Σχήμα 11. Σχηματική απεικόνιση αρχιτεκτονικής των MIs ενός οργανισμού, και διεκπεραίωσης κλήσης μεταξύ τους.

Ταυτοποίηση

Όπως διακρίνεται από το σχήμα 11 κατά τη διάρκεια μιας κλήσης το MI από το οποίο επιχειρείται η κλήση, θα πρέπει να κάνει αυθεντικοποίηση του καλών χρήστη. Στη συνέχεια θα πρέπει να γίνει περαιτέρω έλεγχος για το εάν η ταυτότητα του χρήστη (caller ID), όπως αυτή εμφανίζεται κατά τη

[5] Με τον όρο κανονικοποίηση, εννοούμε τη δημιουργία ομογενών κατηγοριών εμπιστοσύνης και παρουσίασης των πληροφοριών με έναν σταθερό και ενιαίο τρόπο.

σηματοδοσία της κλήσης, συμφωνεί με την τιμή αυτής η οποία διατηρείται στη βάση δεδομένων του MI, με μόνη εξαίρεση την περίπτωση κατά την οποία η ταυτότητα του καλών έχει ρυθμιστεί να διατηρείται ανώνυμη.

Στη συνέχεια, οι πληροφορίες ταυτότητας του συνδρομητή προωθούνται από το MI, στην αρχή ασφαλείας TA. Κατά την προώθηση αυτή των στοιχείων, το MI από το οποίο προέρχεται η κλήση, εισάγει έναν SIP header ο οποίος και περιέχει την αυθεντικοποιημένη ταυτότητα του χρήστη. Κατά την ανταλλαγή αυτή πληροφοριών χρησιμοποιείται πρωτόκολλο TLS ή IPSEC και υπάρχει σχέση εμπιστοσύνης μεταξύ MI και αρχής TA.

```
INVITE sip:+14085551212@MIO.com SIP/2.0
Via: SIP/2.0/TLS euo.MIO.com;branch=z9hG4bK-123
To: <sip:+14085551212@MIO.com>
From: "Anonymous"
<sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 70
Privacy: id
Proxy-Authorization: ... realm="sip.originatingMI.com"
username="alice"
```

Σχήμα 12. Παράδειγμα SIP δήλωσης στοιχείων χρήστη στο MI.
Ο συγκεκριμένος χρήστης διατηρούσε μέχρι πρότινος ανωνυμία.

7. Χαρακτηριστικά ασφάλειας VoIP δικτύων

Παράλληλα με την πιστοποίηση ταυτότητας, είναι εξίσου σημαντική η διαδικασία τυποποίησής της (formatting) με μία σταθερή και κοινή διαδικασία, καθώς και η παραγωγή μοναδικής ταυτότητας εντός του ομίλου (Federation Unique IDentity). Γι' αυτά, καθώς και για την προσθήκη άλλων σχετικών πληροφοριών ασφαλείας σχετικών με την κλήση, τον καλών, και το MI του καλών, είναι υπεύθυνη η αρχή TA. Οι πληροφορίες αυτές είναι προσβάσιμες και ελεγχόμενες ακόμη και offline, μέσω των πολιτικών ασφάλειας του MI. Για την ορθή επιλογή πολιτικών ασφάλειας, και ρύθμισή τους ώστε να αποφευχθεί όσο το δυνατό περισσότερο το spam, οι ιοί και τα worms, θα πρέπει να λαμβάνονται υπ' όψη όλα τα χαρακτηριστικά ασφάλειας τα οποία θα πρέπει να ρυθμίζονται διαρκώς.

Η λίστα των χαρακτηριστικών ασφάλειας ενός VoIP δικτύου μεταβάλλεται δυναμικά, και με βάση τις τάσεις του SPIT και των μεθόδων ανίχνευσης κακόβουλων επιθέσεων. Θα πρέπει να ανανεώνεται διαρκώς καθώς επίσης και οι μέθοδοι μεταφοράς πληροφοριών, λαμβάνοντας πάντα υπ' όψη νέες παραμέτρους ή τυχόν τροποποιήσεις των υπάρχων.

Παρακάτω, παραθέτονται χαρακτηριστικά ασφάλειας, με τη μορφή την οποία περιέχονται στο προφίλ ενός MI, καθώς και οι πιθανές τιμές τους.

7.1 Ισχύς Ταυτότητας (IdentityStrength)

Η παράμετρος αυτή αναφέρεται στη σχετική δυσκολία την οποία συναντούν χρήστες στον να έρθουν σε επαφή ή να επέμβουν σε λογαριασμούς ενός MI. Με άλλα λόγια, το επίπεδο εμπιστοσύνης το οποίο μπορεί να διαθέτει η ταυτότητα ενός χρήστη.

Για παράδειγμα, στην περίπτωση ενός Internet Telephony Service Provider, μία δωρεάν υπηρεσία, βασισμένη σε email, όπου οι χρήστες θα μπορούν να κάνουν download λογισμικό, θα έχει πολύ χαμηλότερο τιμή επίπεδου

εμπιστοσύνης από ένα προϊόν με προκαθορισμένη ταυτότητα, το οποίο αποστέλλεται σε συγκεκριμένη φυσική διεύθυνση.

Επιπρόσθετα, κλήσεις οι οποίες προέρχονται από PSTN δίκτυο θα διαθέτουν μεγαλύτερο επίπεδο εμπιστοσύνης καθώς η αναγνώριση κλήσης η οποία σχετίζεται με μία κλήση από PSTN δίκτυο έχει μεγάλο βαθμό εμπιστοσύνης.

Θεωρείται ότι συνδρομητές με υψηλότερο επίπεδο εμπιστοσύνης, είναι λιγότερο πιθανό να παράγουν SPIT κλήσεις.
Οι τιμές για την παράμετρο αυτή είναι:

0 - Άγνωστο

1 - Δωρεάν υπηρεσία

2 – Υπηρεσία πληρωμής (για παράδειγμα επιβεβαίωση μεθόδου πληρωμής)

3 – Επιβεβαίωση φυσικών προϋποθέσεων / εντός ομίλου / PSTN based

4 – Ισχυρή (κρυπτογραφική) αυθεντικοποίηση ταυτότητας χρήστη

7.2 Κόστος κλήσης (CostOfCall)

Η παράμετρος αυτή ανιχνεύει τις όποιες χρεώσεις κατά τη διάρκεια μίας κλήσης. Θεωρείται ότι οι χρεώσιμες κλήσεις είναι λιγότερο πιθανό να αποτελούν κλήσεις SPIT.
Οι τιμές της παραμέτρου είναι:

0 – Άγνωστο

1 – Δωρεάν

2 – Ενιαίας αξίας (μετά από εγγραφή σε υπηρεσία χρέωσης ανεξαρτήτου διάρκειας)

3 – Ανά λεπτό (ή ανά πεπερασμένου πλήθος λεπτών)

7.3 Αυθεντικοποίηση χρήστη (AuthenticationOfUser)

Η παράμετρος αυτή περιγράφει τη μέθοδο, σύμφωνα με την οποία γίνεται η αυθεντικοποίηση των χρηστών από την υπηρεσία αυθεντικοποίησης.
Οι τιμές της παραμέτρου είναι:

0 – Άγνωστο ή μηδενικό

1 – Βασικό

2 – Συγχώνευση με μοναδικό αριθμό (digest)

3 – Άλλη μορφή ισχυρής κρυπτογράφησης (για παράδειγμα smart card)

7.4 Δήλωση ταυτότητας (IdentityAssertion)

Η παράμετρος αυτή χρησιμοποιείται για δήλωση ταυτότητας ενός χρήστη. Η δήλωση ταυτότητας, διαφέρει από την αυθεντικοποίηση χρήστη. Συχνά μάλιστα, συναντάται το φαινόμενο όπου ένας αυθεντικοποιημένος χρήστης υποκλέπτει την ταυτότητα κάποιου άλλου, επίσης αυθεντικοποιημένου.

Σε περιπτώσεις όπου η αρχή ΤΑ είναι επίσης υπεύθυνη για τη δρομολόγηση κλήσεων μεταξύ των MIs, είναι πολύ πιθανό να διαθέτει και πληροφορίες οι οποίες επιτρέπουν την εξακρίβωση ότι ο συγκεκριμένος καλών χρήστης, όντως ανήκει στο MI από όπου προέρχεται η κλήση.

Η αρχή ασφάλειας ΤΑ εν τέλει, είναι σε θέση να καθορίσει επαληθεύσει εάν μία κλήση από κάποιο MI, ανήκει ή όχι σε ένα γκρουπ χρηστών οι οποίοι βρίσκονται στο πεδίο αυτού του MI.

Θεωρείται ότι κλήσεις με υψηλότερη αξία της παραμέτρου δήλωσης ταυτότητας, είναι λιγότερο πιθανό να αποτελούν κλήσεις SPIT.
Οι τιμές της παραμέτρου είναι:

0 – Ανίχνευση παραβίασης ταυτότητας χρήστη

1 – Άγνωστο (στην περίπτωση όπου μία κλήση εμφανίζεται άνευ πληροφορίες ταυτότητας, όπως για παράδειγμα μία ανώνυμη κλήση από PSTN δίκτυο)

2 – Δήλωση ταυτότητας από την αρχή ασφάλειας TA, βασιζόμενη στο MI, στο οποίο ανήκει ο χρήστης.

3 – Δήλωση ταυτότητας βάση του MI από το οποίο προέρχεται η κλήση, και το οποίο συνδέεται μοναδικά με το χρήστη.

7.5 Ασφάλεια Σύνδεσης (ConnectionSecurity)

Η παράμετρος αυτή ανιχνεύει το επίπεδο ασφάλειας μεταξύ του MI από το οποίο προέρχεται η κλήση και την αρχή ασφάλειας TA.

Οι τιμές της παραμέτρου αυτής είναι:

0 – Μηδενική

1 – Access List

2 – Proxy Αυθεντικοποίηση

3 – VPN/IPsec

4 – TLS

7.6 Υποψία Κλήσης SPIT (SPITSuspect)

Η παράμετρος αυτή, αποτελεί ουσιαστικά έναν ενδείκτη ο οποίος τοποθετείται από την αρχή ασφάλειας TA στην κλήση, μετά από εξέταση του αρχείου κλήσεων του συγκεκριμένου χρήστη. Κάνοντας έναν έλεγχο στο αρχείο αυτό, υπάρχουν μεγάλες πιθανότητες να ανιχνευθεί εάν η κλήση αυτή είναι κλήση spit ή όχι.

Υπάρχει πλήθος ελέγχων οι οποίοι μπορούν να γίνουν σε κλήσεις ή σε τελικούς χρήστες, και στη συνέχεια να βάλουν έναν δείκτη ο οποίος θα αφορά τις κλήσεις ενός συγκεκριμένου χρήστη.

Κάποιοι από αυτούς τους ελέγχους, είναι:

- Έλεγχος υπέρβασης ενός συνηθισμένου μέσου όρου κλήσεων από ένα χρήστη ανά λεπτό.

- Μικρό ποσοστό επί τοις εκατό κληθέντων/απαντηθέντων κλήσεων από ένα χρήστη.
- Μικρό ποσοστό επαναλαμβανόμενων/ξεχωριστών κλήσεων από ένα χρήστη.
- Πλήθος κλήσεων ίδιας διάρκειας.
- Πολλαπλές κλήσεις προς διαδοχικούς αριθμούς.

Οι έλεγχοι αυτοί είθισται να γίνονται συνδυαστικά και δειγματοληπτικά προς τους χρήστες προτού σχηματιστεί το αρχείο κάθε ενός. Οι τιμές των παραμέτρων αυτών κυμαίνονται από 0 έως 9, όπου 9 είναι και οι υψηλότερης πιθανότητας SPIT κλήσεις.

7.7 Τηλεφωνικά Κέντρα (CallCenter)

Είναι αρκετές οι περιπτώσεις όπου η τιμή της παραμέτρου Υποψίας Κλήσης SPIT (SPITSuspect) είναι υψηλή (για παράδειγμα ίσως λόγω μεγάλου πλήθους εξερχόμενων κλήσεων), παρ' όλα αυτά όμως ο χρήστης να αποτελεί έναν ασφαλή και εγγυημένο συνδρομητή. Το MI είναι σε αυτή την περίπτωση υπεύθυνο να πιστοποιήσει ότι ο εκάστοτε χρήστης στην ουσία ίσως ανήκει σε ένα εξωτερικό τηλεφωνικό κέντρο, το οποίο είναι εγγυημένο, παρά την αυξημένη παράμετρο υποψίας κλήσης SPIT. Από το συγκεκριμένο τηλεφωνικό κέντρο, ενδέχεται να λαμβάνονται αρκετές κλήσεις έτσι ώστε και ένας από τους ελέγχους της παραμέτρου SPITSuspect να το κατηγοριοποιήσει ως μη ασφαλές. Γι' αυτό το MI του εξωτερικού τηλεφωνικού κέντρου, από το οποίο προέρχεται η κλήση, θα πρέπει αρχικά να δίνει ταυτότητα στο χρήστη προτού η κλήση εξέλθει του κέντρου, έτσι ώστε να επιτευχθεί στη συνέχεια η αναγνώρισή του από το δίκτυο στο οποίο καταλήγει η κλήση.

Οι τιμές της παραμέτρου αυτής είναι:

0 – Άγνωστο

1 – Γνωστό, αλλά άνευ εμπιστοσύνης, τηλεφωνικό κέντρο. (για παράδειγμα, το συγκεκριμένο κέντρο ίσως πραγματοποιεί αυτόκλητες κλήσεις, δίχως να λαμβάνει υπ' όψη τις βάσεις δεδομένων του με τους απαγορευμένους προς κλήσεις αριθμούς)

2 – Γνωστό και εμπιστεύσιμο τηλεφωνικό κέντρο.

7.8 Ισχύς Δήλωσης (AssertionStrength)

Η παράμετρος αυτή αποτελεί μία ολική και συνονθυλευμένη τιμή, την οποία και αναθέτει η αρχή ασφάλειας ΤΑ σε μία κλήση, έχοντας λάβει υπ' όψη της τις προαναφερθείσες παραμέτρους ασφάλειας. Με αυτόν τον τρόπο, λιγότερο εξεζητημένες αποφάσεις είναι δυνατό να παρθούν βασιζόμενες μεμονωμένα στην τιμή αυτής της παραμέτρου, ενώ παράλληλα είναι διαθέσιμες πιο λεπτομερείς πληροφορίες.

Οι τιμές της παραμέτρου αυτής, είναι:

0 – Χαμηλού επιπέδου ασφάλεια

1 – Μεσαίου επιπέδου ασφάλεια

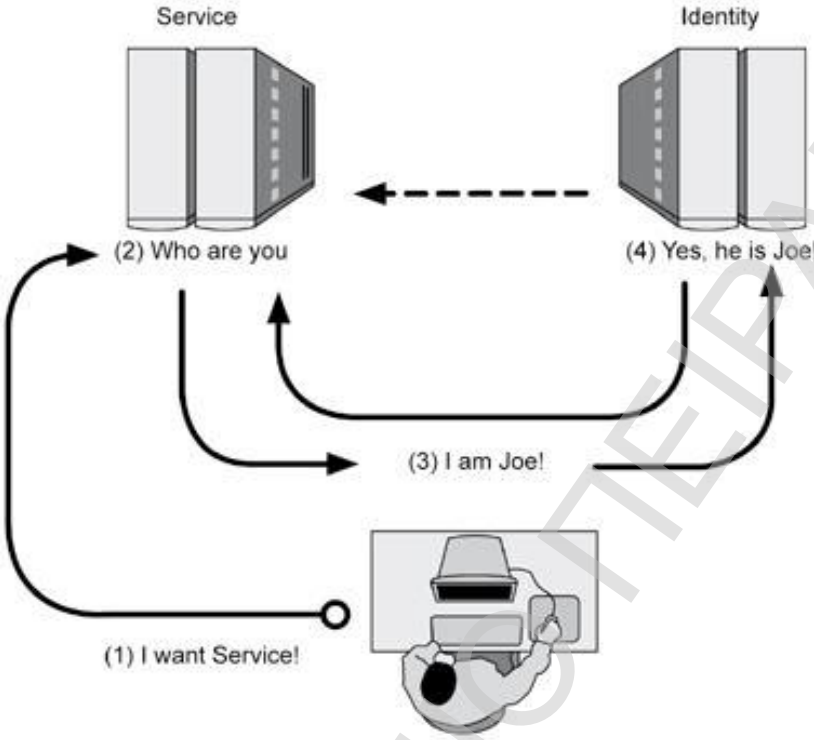
2 – Υψηλού επιπέδου ασφάλεια

Καθώς η παράμετρος αυτή αποτελεί μία ολική εκτίμηση της κλήσης, είναι πιθανό να αποτελεί το χρησιμότερο κριτήριο για δρομολόγηση μίας κλήσης ή φραγή αυτής. Ο καθορισμός αυτός είναι δυνατό να γίνει μέσω ενός τερματικού IP-PBX, Proxy ή ακόμη και από έναν απλό agent.

8. Δήλωση-Διαχείριση χαρακτηριστικών ασφάλειας, μέσω γλώσσας SAML

Η γλώσσα SAML αποτελεί μία γλώσσα, μέσω της οποίας γίνεται ουσιαστικά η δήλωση των παραπάνω χαρακτηριστικών ασφάλειας, καθώς και του βαθμού τους.

Αποτελεί ένα πλαίσιο εργασίας βασισμένο στην XML και ουσιαστικά εξυπηρετεί στη μεταφορά και διαμοιρασμό πληροφοριών ασφάλειας. Τη στιγμή που άλλες προσεγγίσεις χρησιμοποιούν μία κεντρική αρχή, μέσω της οποίας διανέμονται πιστοποιητικά ασφάλειας από ένα σημείο του δικτύου σε άλλο, η γλώσσα SAML δίνει τη δυνατότητα σε κάθε σημείο του δικτύου να δηλώσει ότι γνωρίζει την ταυτότητα ενός χρήστη ή δεδομένων. Αυτό προφανώς μπορεί να γίνει όχι μόνο με την ταυτότητα, αλλά και με οποιαδήποτε άλλη πληροφορία ασφάλειας. Στην συνέχεια, είναι στην κρίση της οιασδήποτε εφαρμογής να εμπιστευτεί ή όχι την δήλωση ασφάλειας κάποιας οντότητας. Κάθε εφαρμογή η οποία είναι SAML-συμβατή είναι σε θέση να δηλώσει την εμπιστοσύνη της όσων αφορά την αυθεντικοποίηση ενός χρήστη ή δεδομένων.



Σχήμα 13. Παράδειγμα εφαρμογής η οποία ζητάει αυθεντικοποίηση για να κάνει χρήση υπηρεσίας.

Όπως έχει προαναφερθεί, οι πληροφορίες σχετικά με την ταυτότητα και ασφάλεια χρήστη, προωθούνται μέσω του εκάστοτε MI, με την προσθήκη κάποιων SIP Headers. Όταν αφορά πληροφορία ταυτότητας, αυτή εισάγεται στο μηχανισμό απόδοσης identity-info header.

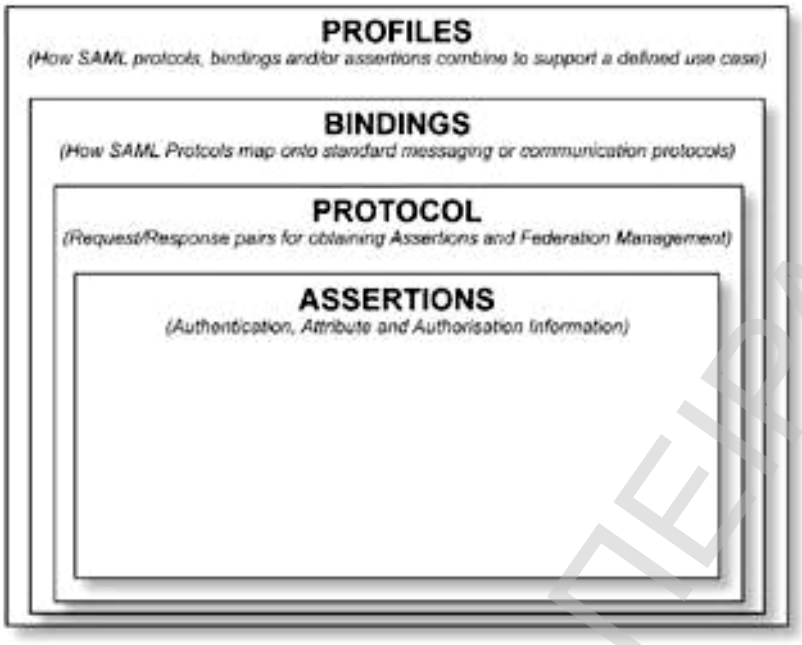
Οι πληροφορίες ασφάλειας διαμορφώνονται σε ζεύγη descriptor=value και προωθούνται στο τελικό MI με χρήση της γλώσσας SAML (Security Assertion Markup Language). Τα ζεύγη αυτά descriptor=value είναι αρκετά ευέλικτα, και μπορούν να προσαρμοστούν ανάλογα με την εξέλιξη των απαιτήσεων και τις μεταβολές καταστάσεων.

Θεωρείται αυτονόητο, ότι είναι απαραίτητη η ενσωμάτωση της γλώσσας SAML με το πρωτόκολλο SIP. Οπότε, για να γίνει η μεταφορά των δηλώσεων SAML και των διαφόρων οντοτήτων, χρησιμοποιούνται οι εξής δύο μηχανισμοί.

- Ο SIP header δύναται να μεταφέρει είτε μία οντότητα, ή έναν δείκτη ο οποίος δείχνει σε μία δήλωση ασφάλειας στο SIP. Ο header αυτός του SIP, ονομάζεται SAML-Payload.
  Μία οντότητα SAML αποτελείται από ένα TypeCode, ένα SourceID και έναν AssertionHandle. Θα πρέπει οπωσδήποτε να διατηρείται πάντα ένα πίνακας με ταξινομημένες τις SourceIDs καθώς και URLs, έτσι ώστε να επικοινωνούν τα προς δήλωση στοιχεία.
- Ο κορμός του SIP μπορεί να μεταφέρει ο ίδιος μία ή περισσότερες δηλώσεις SAML.

Ένας SIP user agent είναι σε θέση να προσθέσει νέες δηλώσεις στον κορμό ενός SIP μηνύματος, ή ακόμη και να προσθέσει μία αναφορά δήλωσης στον SIP header. Σε καμία περίπτωση όμως δεν θα πρέπει ένας SIP proxy να προσθέσει δηλώσεις ασφάλειας στον κορμό του SIP. Αντ' αυτού, θα πρέπει να χρησιμοποιείται ο SIP header όταν πρέπει να προστεθεί μία νέα δήλωση ασφάλειας.
Όπως περιγράφηκε, τα χαρακτηριστικά ασφάλειας, ενσωματώνονται στη δομή της γλώσσας SAML, και μεταφέρονται είτε μέσω ενός SAML header, ή μέσω μίας οντότητας SAML. Σε ορισμένες περιπτώσεις υπάρχουν περιορισμοί, όσων αφορά την αρχιτεκτονική, από την κεντρική αρχή ασφάλειας TA, όπου δεν επιτρέπεται η χρήση proxies και προτιμάται η λύση της SAML οντότητας.

Για τη διασύνδεση μίας δήλωσης SAML και ενός μηνύματος SIP, χρησιμοποιούνται μόνο λίγα πεδία του μηνύματος SIP ως είσοδος σε μία αρκετά μπερδεμένη συνάρτηση. Ο μοναδικός αριθμός, ο οποίος θα συγχωνευθεί, θα πρέπει να λαμβάνεται υπ όψη στις παραμέτρους της SAML δήλωσης.



Σχήμα 14. Διασύνδεση δήλωσης SAML και μηνύματος SIP.

Ένα παράδειγμα ακριβούς διατύπωσης αυτού του προς συγχώνευση μοναδικού αριθμού, είναι:

> digest-string = addr-spec ":" addr-spec ":" callid ":" 1*DIGIT SP method ":" SIP-Date ":" [addr-spec] ":" message-body

Το string αυτό αποτελείται από το πρώτο addr-spec, το οποίο είναι η τιμή του πεδίου του header “από”, το δεύτερο addr-spec, το οποίο είναι η τιμή του header “προς”, και το τρίτο addr-spec, το οποίο είναι η τιμή του πεδίου Contact header.

Σε ένα ολοκληρωμένο σύστημα, θα πρέπει να δημιουργηθεί ένα σημείο όπου θα παίρνονται αποφάσεις σχετικά με πολιτικές ασφάλειας κατά τη λήψη SAML δηλώσεων, και ένα σημείο το οποίο θα προωθεί το αποτέλεσμα της κάθε απόφασης.

Ακολουθεί ένα λεπτομερές παράδειγμα, ενσωμάτωσης πληροφοριών ασφάλειας SAML, σε ένα SIP μήνυμα. Το παράδειγμα είναι αποσπασμένο από τμήμα δομής SAML μεγάλου οργανισμού.

```
<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
    xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    AssertionID="_e2baaae679 f1663ac342ed7f08e42fb4"
    IssueInstant="2005-05-22T20:18:28.830Z"
    Issuer="http://www.opensaml.org"
    MajorVersion="1"
    MinorVersion="1">
    <Conditions
        NotBefore="2005-05-22T20:18:28.826Z"
        NotOnOrAfter="2005-05-22T20:19:28.826Z">
        <AudienceRestrictionCondition>
            <Audience>http://www.opensaml.org</Audience>
        </AudienceRestrictionCondition>
    </Conditions>
    <AttributeStatement>
        <Subject>
            <NameIdentifier>foo</NameIdentifier>
            <SubjectConfirmation>
                <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:bearer
                </ConfirmationMethod>
            </SubjectConfirmation>
        </Subject>
        <Attribute
        AttributeName="IdentityStrength"
        AttributeNamespace="http://ta.com">
            <AttributeValue>2</AttributeValue>
      </Attribute>
      <Attribute
      AttributeName="CostOfCall"
      AttributeNamespace="http://ta.com">
      <AttributeValue>2</AttributeValue>
      </Attribute>
      <Attribute
      AttributeName="ConnectionSecurity"
      AttributeNamespace="http://ta.com">
      <AttributeValue>2</AttributeValue>

      </Attribute>
    <Attribute
        AttributeName="CallCenter"
        AttributeNamespace="http://ta.com">
        <AttributeValue>2</AttributeValue>
    </Attribute>
    <Attribute
        AttributeName="SPITSuspect" AttributeNamespace="http://ta.com">
        <AttributeValue>0</AttributeValue>
    </Attribute>
    <Attribute
        AttributeName="IdentityAssertion"
        AttributeNamespace="http://ta.com">
        <AttributeValue>1</AttributeValue>
    </Attribute>
    <Attribute
        AttributeName="AssertionStrength"
        AttributeNamespace="http://ta.com">
        <AttributeValue>0</AttributeValue>
    </Attribute>
    <Attribute
        AttributeName="AuthenticationOfUser"
```

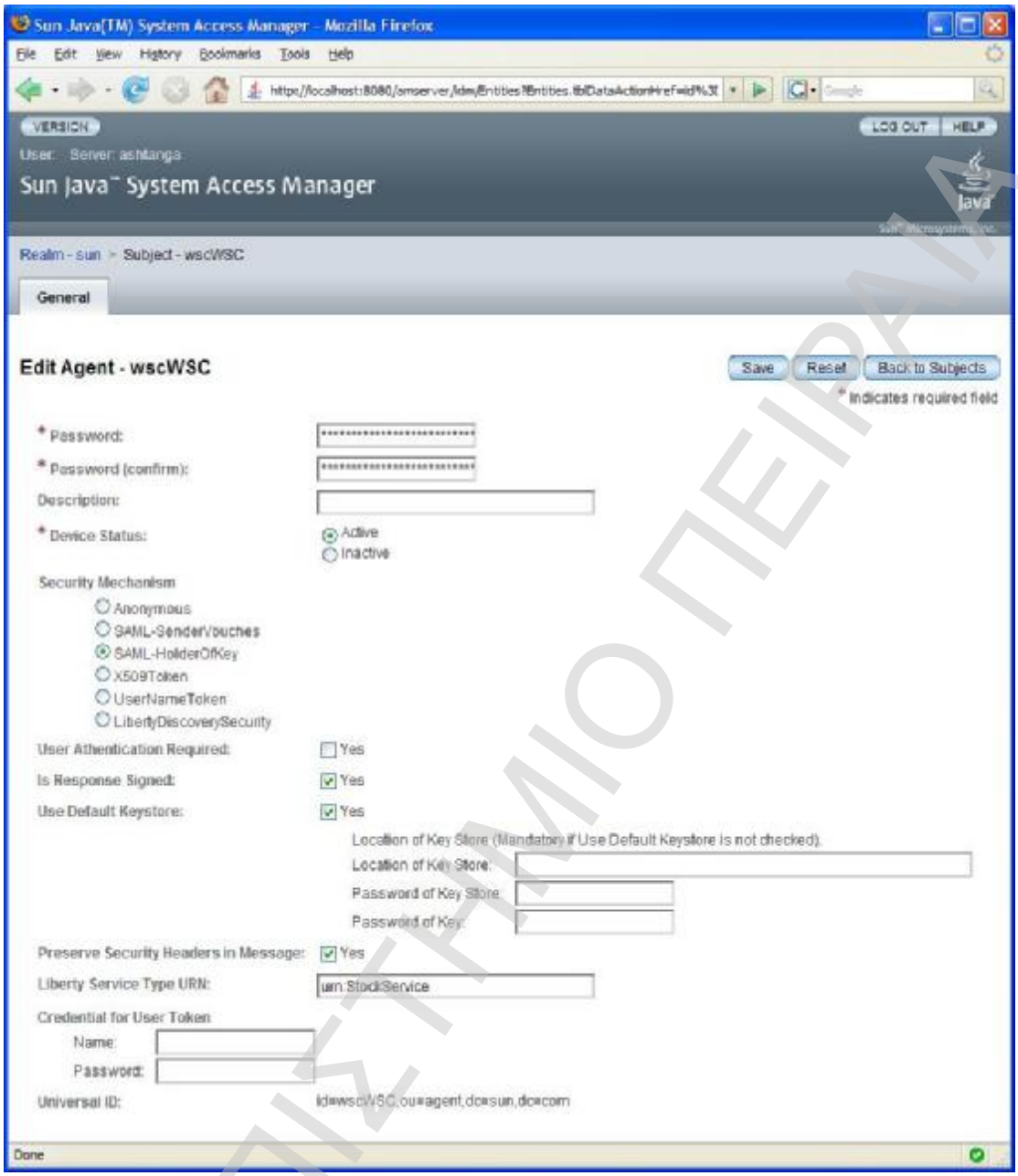
```
        AttributeNamespace="http://ta.com">
        <AttributeValue>0</AttributeValue>
</Attribute>
</AttributeStatement>
</Assertion>
```

Στο παραπάνω παράδειγμα μπορούμε να δούμε τη δήλωση χαρακτηριστικών ασφάλειας ενός χρήστη, με το αναγνωριστικό "**foo"**.
Γίνεται δήλωση των εξής χαρακτηριστικών με την παρακάτω σειρά:

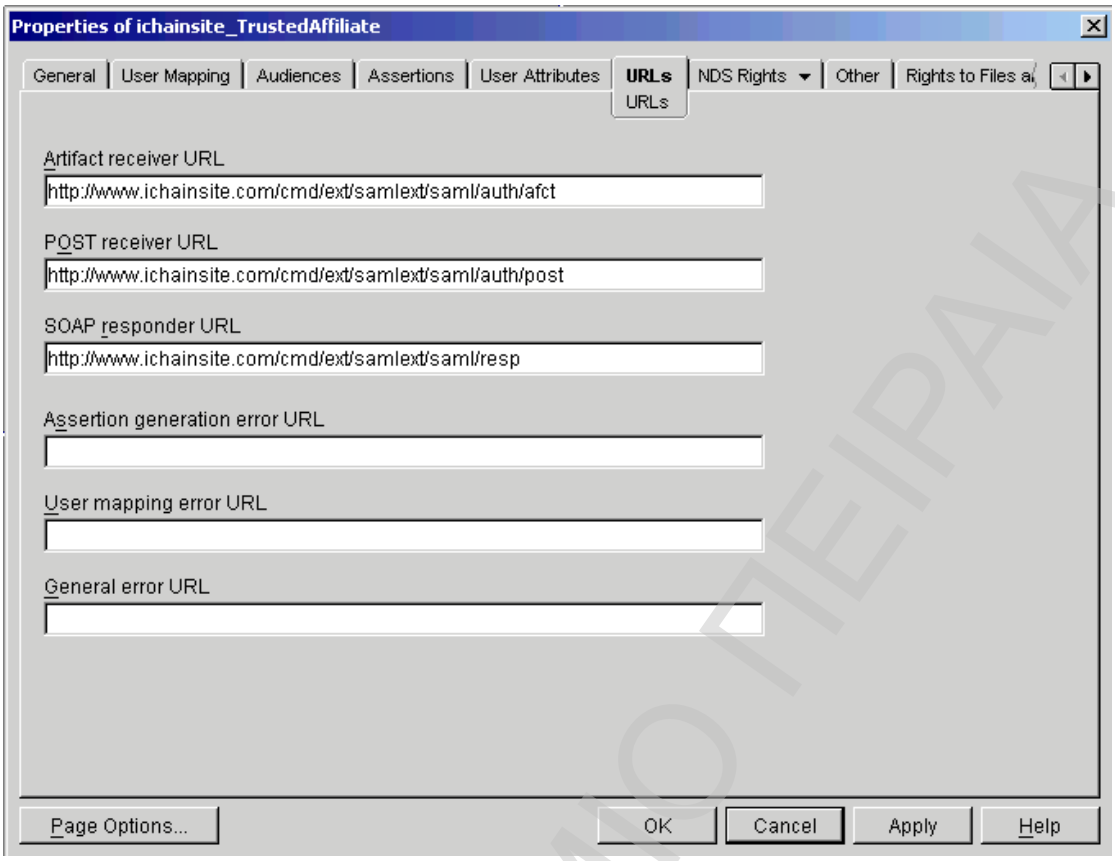
- **Ισχύς Ταυτότητας (IdentityStrength)**
- **Κόστος κλήσης (CostOfCall)**
- **Ασφάλεια Σύνδεσης (ConnectionSecurity)**
- **Τηλεφωνικά Κέντρα (CallCenter)**
- **Υποψία Κλήσης SPIT (SPITSuspect)**
- **Δήλωση ταυτότητας (IdentityAssertion)**
- **Ισχύς Δήλωσης (AssertionStrength)**
- **Αυθεντικοποίηση χρήστη (AuthenticationOfUser)**

Σε κάθε περίπτωση, δηλώνεται και η τιμή του κάθε χαρακτηριστικού.
Η δήλωση αυτή των χαρακτηριστικών ασφάλειας, έχει ένα μοναδικό αριθμό-κωδικό αναφοράς, ο οποίος δηλώνεται ως AssertionID.

Σε μεγάλους οργανισμούς, με πλήθος χρηστών τέτοιο ώστε να κάνει αποτρεπτική την παραπάνω μέθοδο δήλωσης χαρακτηριστικών ασφάλειας, χρησιμοποιούνται customized πλατφόρμες με έτοιμες παραστατικές επιλογές για το κάθε χαρακτηριστικό χρήστη. Έτσι είναι ευκολότερες οι ρυθμίσεις ασφάλειας χρηστών, καθώς είναι δυνατό να γίνουν και ομαδικά, σε πολύ μικρότερο χρόνο.



Σχήμα 15. Πλατφόρμα της Sun Microsystems. Φόρμα επιλογής μηχανισμού ασφάλειας.



Σχήμα 16. Φόρμα δήλωσης ανακατεύθυνσης χρηστών σε περίπτωση σφάλματος SAML.

8.1 Μελλοντικές μελέτες βασισμένες στον κώδικα SAML

Πολλές μελέτες σχετικά με τη μελλοντική VoIP ασφάλεια περιλαμβάνουν ως προϋπόθεση την ύπαρξη κεντρικών αρχών ασφάλειας εντός του δικτύου. Έτσι, οποιαδήποτε πληροφορία σχετική με το επίπεδο ασφάλειας, και την πιστοποίηση ταυτότητας, είναι διαθέσιμο στην αρχή αυτή. Με τη συνεχόμενη ανάπτυξη της από IP σε IP επικοινωνίας, και με την απουσία της ανάγκης για ανωνυμία εντός του δικτύου, οι οποιεσδήποτε πληροφορίες σχετικά με τον καλούντα, μπορούν να εισαχθούν στην τελική συσκευή του χρήστη, ή στον διακομιστή του Member Island. Εάν δεν υπάρχει επιπλέον πληροφορία για να προστεθεί στην βάση πληροφοριών της αρχής ασφαλείας, τότε μπορεί να

παραχθεί κώδικας SAML στον τελικό χρήστη ή στο Member Island. Στην περίπτωση αυτή, το τελικό Member Island, το οποίο και θα περιέχει τον κώδικα με τους περιορισμούς, θα είναι σε θέση μέσω του κώδικα να φιλτράρει καταλλήλως τις κλήσεις.

Παρ' όλα αυτά, ίσως υπάρξουν περιπτώσεις όπου η κεντρική ασχή ασφάλειας θα συνεχίσει να διατηρεί σημαντικές πληροφορίες ασφάλειας, ακόμη και αν ο τελικός χρήστης ή το Member Island κάνουν τις δικές τους δηλώσεις ασφάλειας. Στην περίπτωση αυτή, προτιμάται ένα υβριδικό μοντέλο καθαρού end to end SAML κώδικα, το οποίο μαζί με τις προσθήκες της κεντρικής αρχής ασφάλειας, θεωρείται ως η καλύτερη λύση.

Ο κώδικας SAML καθορίζει μεθόδους αίτησης πληροφοριών ασφάλειας από και προς την αρχή ασφάλειας, οι οποίες επιτρέπουν τη μεταφορά αυτών των πληροφοριών με τρόπο ενσωματωμένο και ασφαλή, έτσι ώστε να διατηρούνται μυστικές και ασφαλείς ακόμη και από τον χρήστη από τον οποίο έχουν προέλθει, ή από το Member Island. Οι μέθοδοι αυτοί μπορούν να ενσωματωθούν σε αρχιτεκτονικές όπου η κλήση δεν χρειάζεται να διατρέχει κεντρικά κομβικά σημεία στο δίκτυο, ή σε δίκτυα όπου οι πληροφορίες ασφάλειας είναι τοποθετημένες εκτός οργανισμού.

9. Απειλές στη διαδικτυακή τηλεφωνία

Τον Αύγουστο του 2006, κατατέθηκε στον IETF, τον βασικό οργανισμό των "standards" για το Internet (Internet Engineering Task Force), ένα προσχέδιο στο οποίο ταξινομούνταν και κατατάσσονταν οι απειλές στη διαδικτυακή τηλεφωνία. Το προσχέδιο αυτό κατατέθηκε από τον Dr. Saverio Niccolini, μέλος ομάδας ερευνών της NEC Europe Ltd, ο οποίος ειδικεύεται στη διαδικτυακή τηλεφωνία, και περιείχε μία τεράστια λίστα απειλών και πιθανών επιθέσεων στη διαδικτυακή τηλεφωνία. Δυστυχώς η λίστα αυτή είχε υπερβολικά πολυάριθμες καταχωρήσεις, γεγονός το οποίο καθιστούσε την πρακτική ανάλυση VoIP ασφάλειας, ακατόρθωτη. Παρά το γεγονός ότι οποιοδήποτε στοιχείο, συμπεριλαμβανομένων των υποστηριζόμενων στοιχείων ή πρωτοκόλλων VoIP, είναι ικανό να αποτελέσει απειλή, είναι πραγματικά δύσκολο να προβλεφθούν όλες οι πιθανές μελλοντικές VoIP επιθέσεις, και να προστατευθούν όλες οι πτυχές της διαδικτυακής τηλεφωνίας.

Γι’αυτό το λόγο, η εστίαση στην ανάλυση του application layer της διαδικτυακής τηλεφωνίας, αποτελεί μία λογική συνέχεια της υπάρχουσας θεμελίωσης πρακτικών και αρχών ασφάλειας ενός δικτύου. Από την άλλη, οι απειλές οι οποίες αναφέρονται στο προσχέδιο της IETF “VoIP Security Threats”, αποτελούν απειλές οι οποίες θα έπρεπε να ληφθούν υπ’όψη κατά το στάδιο σχεδίασης του πρωτοκόλλου.

Η πρώτη έκδοση του προσχέδιου το οποίο κατατέθηκε στην IETF, περιείχε τις εξής κατηγορίες απειλών:

- Ανάσχεση και τροποποίηση απειλών.
- Απειλή διακοπής υπηρεσίας.
- Απειλή κατάχρησης υπηρεσίας.
- Τυπικές απειλές.

Υπάρχουν πολλών ειδών κατηγοριοποιήσεις και ταξινομήσεις, καθώς κάθε ταξινόμηση έχει και άλλου είδους σκοπό. Η επιτροπή ασφάλειας διαδικτυακής τηλεφωνίας (VOIPSA), παρακολουθεί στενά όλα τα είδη απειλών, καθώς αυτά

αυξάνονται και τροποποιούνται διαρκώς, έτσι ώστε να είναι σε θέση να δώσει όσο το δυνατό περισσότερες πληροφορίες σχετικά με αυτά, οι οποίες όμως πληροφορίες μπορούν να χαρακτηριστούν ως υπερβολικές από πολλούς οργανισμούς. Παρ'όλα ταύτα, η μελέτη αυτή δεν παύει να αποτελεί μία σημαντική συνεισφορά η οποία βοηθά στη κατανόηση και αντιμετώπιση σχετικών απειλών.

Η ταξινόμηση απειλών από την IETF, κατηγοριοποιεί απειλές οι οποίες βασίζονται στο πως τα χαρακτηριστικά του πρωτοκόλλου μπορούν να βελτιωθούν έτσι ώστε να ελαχιστοποιηθεί ο αντίκτυπος μίας απειλής, και συνεπώς δεν ασχολείται με θέματα τα οποία σχετίζονται με την υποδομή υποστήριξης, όπως μία πλατφόρμα στο λειτουργικό σύστημα και μία διαμόρφωση του δικτύου.

Παρακάτω παρατίθεται και αναλύεται η ταξινόμηση VoIP απειλών, έτσι ώστε να γίνει διάκριση κάποιων απειλών, οι οποίες μπορούν να επικαλύπτουν, αλλά και να περιέχουν επιθέσεις, οι οποίες δεν έχουν ληφθεί υπ' όψην κατά τη σχεδίαση του πρωτοκόλλου. Οι απειλές αυτές περιορίζονται στις ακόλουθες κατηγορίες:

9.1 Ενόχληση και διακοπή υπηρεσίας

Η προσπάθεια διακοπής της VoIP υπηρεσίας, συμπεριλαμβανομένου του ελέγχου, της πρόβλεψης, της πρόσβασης, και των λειτουργιών. Επιθέσεις αυτής της κατηγορίας μπορούν να επηρεάσουν οποιοδήποτε στοιχείο δικτύου το οποίο υποστηρίζει τη VoIP υπηρεσία, συμπεριλαμβανομένων των routers, DNS servers, SIP Proxies, session border controllers, και λοιπά στοιχεία.

Τέτοιου είδους επιθέσεις μπορούν να επιτευχθούν είτε εξ αποστάσεως, δίχως να υπάρχει άμεση πρόσβαση στο επιτιθέμενο στοιχείο δικτύου, αλλά χειραγωγώντας τα πρωτόκολλα VoIP, ή τοπικά δίνοντας εντολές διατάραξης. Ένας εισβολέας μπορεί να βάλει ως στόχο μία τελική συσκευή, παραδείγματος χάριν μία VoIP τηλεφωνική συσκευή, ένα βασικό στοιχείο του δικτύου, ή ένα σύνολο στοιχείων, όπως SIP proxies, τα οποία μπορούν να

έχουν αντίκτυπο σε ένα μεγάλο πλήθος χρηστών. Η συγκεκριμένη κατηγορία, περιλαμβάνει επίσης επιθέσεις τύπου SPIT.

9.2 Ωτακουστική και ανάλυση κίνησης

Η προσπάθεια συλλογής ευαίσθητων πληροφοριών για επικείμενη επίθεση, ή προς απόκτηση εμπειρίας για μελλοντική επίθεση. Γενικότερα στις εφαρμογές Internet multimedia, αλλά ιδίως στη διαδικτυακή τηλεφωνία, κάτι τέτοιο ερμηνεύεται με την ικανότητα του εισβολέα να παρακολουθεί απροστάτευτη σηματοδοσία ή ροή δεδομένων η οποία εναλλάσσεται μεταξύ των χρηστών του δικτύου.

Η κατηγορία αυτή η οποία περιλαμβάνει ανάλυση κίνησης, μπορεί να είναι ενεργητική ή παθητική. Αυτό μεταφράζεται ως συλλογή, αποθήκευση, ανάλυση, ή μετάφραση/αποκωδικοποίηση πακέτων σε πραγματικό χρόνο. Συνήθως τέτοιου είδους επιθέσεις στοχεύουν στην υποκλοπή λεκτικών ή κειμένου από το περιεχόμενο μίας συνδιάλεξης, όπως ένας αριθμός πιστωτικής κάρτας, ή ένας κωδικός pin. Παράλληλα, γίνεται συλλογή και ανάλυση στοιχείων της επικοινωνίας μεταξύ των άκρων, έτσι ώστε να γίνει αντιληπτό το σχέδιο και ο τύπος της επικοινωνίας, για μελλοντική επίθεση.

9.3 Παραποίηση ταυτότητας και ψευδοπροσωποποίηση

Η ικανότητα μίμησης ενός χρήστη, ενός στοιχείου δικτύου, ή μίας υπηρεσίας, με σκοπό την απόκτηση πρόσβασης σε ένα δίκτυο, υπηρεσία, στοιχείο του δικτύου, ή πληροφορίες.

Αυτή αποτελεί μία ιδιαίτερη κατηγορία, καθώς οι επιθέσεις αυτές εξαπάτησης μπορούν να χρησιμοποιηθούν για την επίτευξη δόλιας, μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες, καθώς και διαταραχή υπηρεσιών. Μία ιδιαίτερη περίπτωση απειλής παραποίησης ταυτότητας αποτελεί η ψευδοπροσωποποίηση, όπου ο επιτεθείς μπορεί να προσποιηθεί ή να πάρει

προσωρινά την ταυτότητα κάποιας άλλης οντότητας. Στόχοι αυτής της κατηγορίας μπορούν να είναι χρήστες, τερματικές συσκευές, στοιχεία δικτύου, και μπορεί να πραγματοποιηθεί η χειραγώγηση μέσω απομακρυσμένης αποστολής δεδομένων και εντολών, ή μέσω μη εξουσιοδοτημένης πρόσβασης σε VoIP στοιχεία, όπως signaling gateways, του SIP registrar, ή DNS servers. Για παράδειγμα, εάν ένας τηλεπικοινωνιακός πάροχος χρησιμοποιεί μόνο πληροφορίες αναγνώρισης κλήσεως για να αυθεντικοποιήσει τους συνδρομητές του στα voice mailboxes του, είναι πολύ πιθανό ένας εισβολέας να ισχυριστεί ταυτότητα ίδια με ενός χρήστη, και να κερδίσει πρόσβαση στο voice mailbox του χρήστη αυτού.
Αυτού του είδους οι επιθέσεις στα VoIP δίκτυα μπορούν επίσης να πραγματοποιηθούν μέσω χειραγώγησης υποκείμενων πρωτοκόλλων τα οποία υποστηρίζουν τη VoIP τηλεφωνία, όπως το ARP, IP, και DNS.

9.4 Μη εξουσιοδοτημένη πρόσβαση

Η επίτευξη πρόσβασης σε μία υπηρεσία, λειτουργία, ή ένα στοιχείο δικτύου δίχως εξουσιοδότηση. Τέτοιου είδους επιθέσεις μπορούν να χρησιμοποιηθούν προς υποστήριξη άλλων επιθέσεων, συμπεριλαμβανομένων των προαναφερθέντων, καθώς ο επιτεθείς αποκτά τον έλεγχο μίας συσκευής, διάφορων πόρων, ή πρόσβαση σε κάποιο δίκτυο. Η διαφορά μεταξύ παραποίησης ταυτότητας και μη εξουσιοδοτημένης πρόσβασης έγκειται στο ότι κατά τη δεύτερη, ο επιτεθείς δεν χρειάζεται να προσποιηθεί άλλο χρήστη ή στοιχείο δικτύου, καθώς έχει τη δυνατότητα να αποκτήσει άμεση πρόσβαση εκμεταλλευόμενος μία αδυναμία, όπως μία υπερχείλιση buffer, μία ρύθμιση η οποία έχει διατηρήσει τις προεπιλεγμένες τιμές, ένα φτωχό σύστημα σηματοδοσίας, ή ανεπαρκείς ελέγχους πρόσβασης. Για παράδειγμα, ένας εισβολέας, ο οποίος καταφέρνει να επιτύχει πρόσβαση με δικαιώματα διαχειριστή σε έναν SIP proxy, είναι σε θέση να διαταράξει την VoIP σηματοδοσία σβήνοντας κρίσιμα αρχεία συστήματος του λειτουργικού, και συνεπώς να φέρει μεγάλη σύγχυση σε host και service. Ένα άλλο αντιπροσωπευτικό παράδειγμα αποτελεί η περίπτωση όπου ο επιτεθείς αποκτά πρόσβαση σε ένα media gateway και εγκαθιστά κακόβουλο

λογισμικό, το οποίο είναι ικανό να συλλέξει πακέτα δεδομένων και τελικά να καταφέρει παθητική υποκλοπή επικοινωνιών ενός συνδρομητή.

Η μη εξουσιοδοτημένη πρόσβαση μπορεί να συνδέεται άμεσα με απειλές όπως υποκλοπή, παραποίηση ταυτότητας και παραποίηση στοιχείων.

9.5 Εξαπάτηση

Η ικανότητα εκμετάλλευσης των VoIP υπηρεσιών για προσωπικό, συχνά οικονομικό, κέρδος. Η κατηγορία αυτών των επιθέσεων, αποτελεί ένα από τα κρισιμότερα ζητήματα στους τηλεπικοινωνιακούς φορείς και παρόχους, μαζί με την ευθύνη για διαθεσιμότητα και συνέχεια των υπηρεσιών τους. Η εξαπάτηση μπορεί να επιτευχθεί μέσω της επιδέξιας διαχείρισης των μηνυμάτων σηματοδοσίας ή των ρυθμίσεων κάποιων VoIP στοιχείων, από έναν εισβολέα, καθώς και με την απόκτηση ελέγχου των συστημάτων χρέωσης.

Κάποια πιθανά σενάρια εξαπάτησης στη διαδικτυακή τηλεφωνία, μπορούν να εξετασθούν μέσω της διαχείρισης της ροής σηματοδοσίας σε μία κλήση.
Περισσότερο εξεζητημένες τεχνικές εξαπάτησης αναμένονται να αναπτυχθούν στο μέλλον, καθώς η διαδικτυακή τηλεφωνία γίνεται όλο και πιο δεσπόζουσα τάση στους μεγάλους οργανισμούς, αλλά και στις προσωπικές, οικιακές επικοινωνίες.

9.6 Υποκλοπή πακέτων (packet sniffing)

Η παρεμβολή software ή hardware ανάμεσα σε στοιχεία δικτύου, και αντιγραφή των προς δρομολόγηση πακέτων.

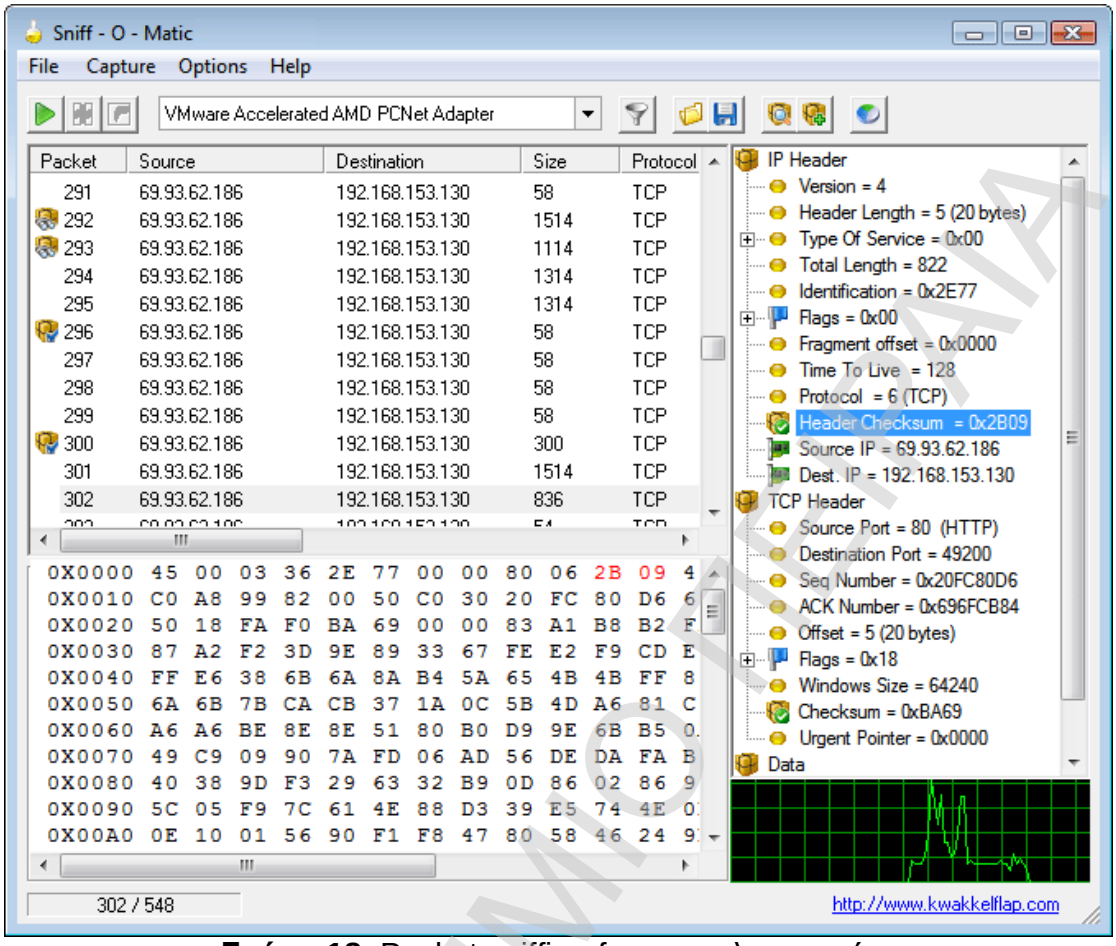
Υπάρχει πληθώρα συσκευών ,οι οποίες τοποθετούμενες σε ένα τυχλό σημείο του δικτύου, θα μπορούσαν με μεγάλη ευκολία να υποκλέψουν voice ή data πακέτα, και να τα αποστείλουν σε κάποιο άλλο σημείο του δικτύου προς αποθήκευση ή ακρόαση. Κάτι τέτοιο θα μπορούσε να γίνει εσωτερικά σε έναν οργανισμό, με άμεση φυσική παρέμβαση στο hardware του δικτύου. Για

παράδειγμα ένας υπάλληλος, με προθέσεις δολιοφθοράς ή οικονομικά οφέλη, θα μπορούσε να τοποθετήσει μία συσκευή sniffer σε ένα σημείο του δικτύου, από όπου υπάρχει ροή δεδομένων. Ένα τέτοιο σημείο θα μπορούσε να είναι ένα switch ή ένα patch panel.

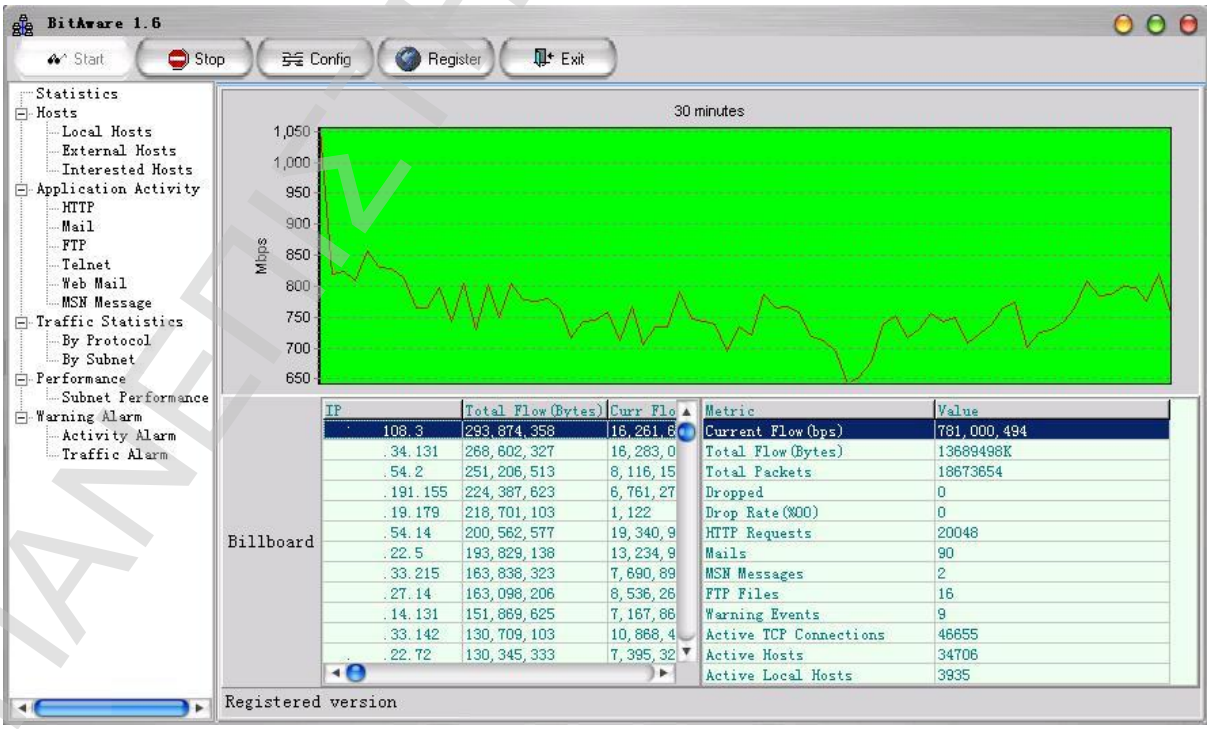
Πέραν των συσκευών sniffing όμως, μεγαλύτερη απειλή αποτελούν τα sniffing softwares, καθώς η οποιαδήποτε υποκλοπή μέσω υπολογιστή είναι πολύ δυσκολότερο να εντοπισθεί. Το λογισμικό αυτό αρκεί να τρέχει στο παρασκήνιο ενός υπολογιστή ο οποίος έχει πρόσβαση στον call manager ενός οργανισμού, έτσι ώστε να υποκλέψει πακέτα από οποιονδήποτε χρήστη του δικτύου. Κάτι τέτοιο είναι πιο δύσκολο στον εντοπισμό, καθώς στην προκειμένη περίπτωση δεν υπάρχει φυσική συσκευή η οποία να μπορεί να γίνει αντιληπτή. Η μέθοδος αντιμετώπισης είναι ένας διαρκής έλεγχος και παρακολούθηση του φόρτου του δικτύου, καθώς πιθανές αυξήσεις ροής δεδομένων και κατάληψη εύρους ζώνης δικτύου σε μη φυσιολογικές ώρες, και από χρήστες οι οποίοι δεν συνηθίζουν να κάνουν τόσο εκτεταμένη χρήση πόρων, αποτελεί μία πιθανή ένδειξη μη επιθυμητής ροής δεδομένων προς κάποια κατεύθυνση.

Η υποκλοπή πακέτων, μπορεί να αποτελέσει μία πολύ σοβαρή απειλή όταν μιλάμε για οργανισμούς όπου απαιτείται υψηλό επίπεδο ασφάλειας, οι χρήστες του διαχειρίζονται πληροφορίες υψηλής διαβάθμισης, και η εξόρυξη πληροφοριών από το τηλεφωνικό δίκτυό τους, θα μπορούσε να έχει σοβαρά επιπτώσεις ακόμη και σε εθνικό επίπεδο. Τέτοιοι οργανισμοί θα μπορούσαν για παράδειγμα να είναι το Γενικό Επιτελείο Στρατού, ή η Γενική διεύθυνση της Αστυνομίας.

Σχήμα 17. Packet sniffing συσκευές.



Σχήμα 18. Packet sniffing freeware λογισμικό.



Σχήμα 19. Λογισμικό παρακολούθησης φόρτου δικτύου, με στοιχεία και ιστορικό για κάθε τελικό χρήστη.

Η παραπάνω λίστα, αποτελεί μία περιλιπτική δομή όπου μπορούν να κατηγοριοποιηθούν τρέχουσες και νέες απειλές στη διαδικτυακή τηλεφωνία. Για παράδειγμα, μία επίθεση εναντίων ενός μηχανισμού αυθεντικοποίησης, ο οποίος χρησιμοποιείται από ένα πρωτόκολλο σηματοδοσίας, δύναται να κατηγοριοποιηθεί στις επιθέσεις μη εξουσιοδοτημένης πρόσβασης, στην περίπτωση όπου η επίθεση αυτή δίνει πρόσβαση σε πληροφορίες, αλλά δεν έχει οικονομικό αντίκτυπο σε έναν οργανισμό. Στην περίπτωση όπου θα υπήρχαν οικονομικά οφέλη μέσω της επίθεσης αυτής, θα άνηκε στην κατηγορία των εξαπατήσεων. Δεν αποκλείεται φυσικά μία επίθεση να ανήκει σε περισσότερες από μία κατηγορίες.

10. Επιθέσεις σε SIP συστήματα διαδικτυακής τηλεφωνίας.

Σε αυτό το σημείο, θα εξετάσουμε πως οι όποιες ευπάθειες και τρωτά σημεία του πρωτόκολλου SIP μπορούν να τύχουν εκμετάλλευσης έτσι ώστε να πραγματοποιηθούν επιθέσεις σε SIP συστήματα διαδικτυακής τηλεφωνίας.
Πιο συγκεκριμένα, θα εστιάσουμε κυρίως στις χρεώσιμες επιθέσεις οι οποίες ως στόχο έχουν συνδρομητές SIP based συστημάτων τηλεφωνίας. Χρεώσιμες χαρακτηρίζουμε τις επιθέσεις, οι οποίες ως κύριο στόχο τους έχουν όχι τόσο την απλή υποκλοπή κλήσεων, ή απόρριψή τους, αλλά την κατά πολύ μεγαλύτερη χρέωση του συνδρομητή, από το αναμενόμενο. Τέτοιου είδους επιθέσεις, εκτός από την οικονομική επιβάρυνση των συνδρομητών, ευθύνονται επίσης σε αύξηση του φόρτου δικτύου, μη απόκριση υπηρεσιών (denial of service), και γενικότερη σύγχυση μεταξύ συνδρομητή και πάροχου.

Οι υπάρχουσες εμπορικές VoIP υπηρεσίες μπορούν να παρέχουν απεριόριστες ή συγκεκριμένο πλήθος κλήσεων, ή προκαθορισμένων κλήσεων (όπως για παράδειγμα τοπικές κλήσεις, ή κλήσεις προς συγκεκριμένες χώρες). Σε περίπτωση όπου ο συνδρομητής καλέσει ένα νούμερο το οποίο δεν ανήκει στη λίστα των προκαθορισμένων απεριόριστων αριθμών (όπως μία διεθνής κλήση, ή κλήση προς δίκτυο κινητής τηλεφωνίας) τότε θα γίνει εκκίνηση χρέωσης της κλήσης ανά λεπτό.
Επιπρόσθετα, ένας συνδρομητής VoIP ενός περιορισμένου προγράμματος κλήσεων (για παράδειγμα 500 λεπτά ανά μήνα) θα πρέπει να χρεωθεί επιπρόσθετα τις όποιες κλήσεις πέραν των 500 λεπτών πραγματοποιήσει.

Σε τέτοιες περιπτώσεις, εάν ο κακόβουλος επιτιθέμενος κατάφερνε να πραγματοποιήσει κλήσεις, οι οποίες δεν ανήκουν στο πλάνο κλήσεων στο οποίο είναι εγγεγραμμένος ο συνδρομητής, ή κατάφερνε να παρατείνει τη διάρκεια των κλήσεων του συνδρομητή, τότε θα ήταν σε θέση να χρεώσει τον συνδρομητή πολύ περισσότερο από όσο προέβλεπε το πλάνο κλήσεών του, και ο προκαθορισμένες χρεώσεις του.

Ένα συστατικό κλειδί σε όλες σχεδόν τις επιθέσεις, αποτελεί το MITM (Man In The Middle). Όταν αναφερόμαστε σε MITM επιθέσεις, εννοούμε επιθέσεις όπου ο επιτιθέμενος πραγματοποιεί ταυτόχρονα ξεχωριστές συνδέσεις με κάθε ένα από τα θύματά του, μεταδίδει μηνύματα σε αυτά, κάνοντάς τα να πιστεύουν ότι τη συγκεκριμένη στιγμή επικοινωνούν μεταξύ τους μέσω μίας ιδιωτικής σύνδεσης, ενώ στην πραγματικότητα η όλη επικοινωνία ελέγχεται από τον κακόβουλο επιτιθέμενο.
Ο επιτιθέμενος συνήθως σε τέτοιου είδους επιθέσεις, υποκλέπτει τα όποια μηνύματα ανταλλάσουν οι συνδρομητές, και στη θέση τους εισάγει νέα, τα οποία ο ίδιος έχει συνθέσει.

Δεδομένου ότι οι πάροχοι VoIP υπηρεσιών συνήθως εξυπηρετούν έναν ή λίγους SIP servers για την πραγματοποίηση μίας κλήσης, το πλήθος των SIP τηλεφώνων θα βρίσκονται εκατοντάδες ή ακόμη και χιλιάδες μίλια μακριά από τον εξυπηρετητή SIP σηματοδοσίας. Κάτι τέτοιο θα ευνοούσε τον επιτιθέμενο στο να πραγματοποιήσει μία MITM επίθεση μέσω του διαδικτύου.

Μεγάλοι πάροχοι διαδικτυακής τηλεφωνίας της Αμερικής[6] πραγματοποίησαν προσομοίωση κακόβουλων VoIP επιθέσεων τις οποίες και ανέλυσαν. Τις επιθέσεις αυτές εφάρμοσαν οι ίδιοι οι πάροχοι στους εαυτούς τους, και όχι σε συνδρομητές, έτσι ώστε να μη γίνει κατάχρηση εύρους ζώνης τηλεφωνίας, να μην επηρεαστεί με κανένα τρόπο η VoIP υποδομή, και να μην καταπατηθούν συμφωνίες υπηρεσιών μεταξύ των πάροχων και των συνδρομητών.

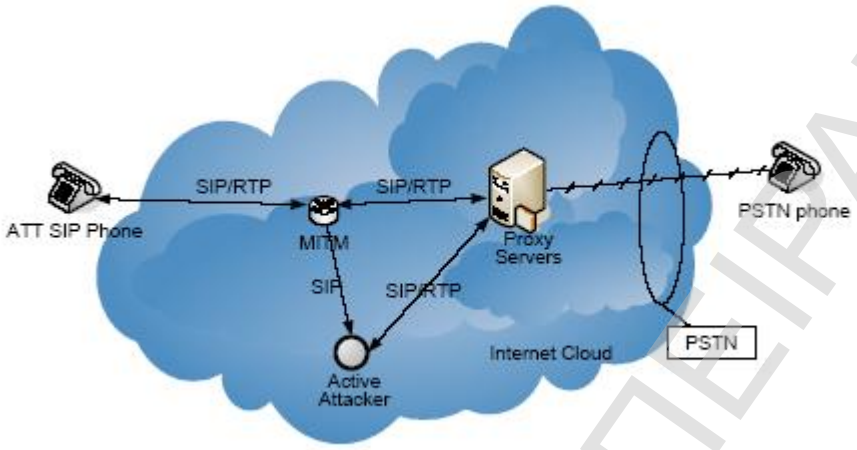
Οι επιθέσεις αυτές, αναλύονται στη συνέχεια:

- **InviteReplay Billing Atack**

Η χρεώσιμη αυτή επίθεση στοχεύει στο να πραγματοποιήσει μη επιτρεπτές κλήσεις, επαναλαμβάνοντας υποκλεμμένα INVITE μηνύματα SIP. Μία τέτοιου είδους επίθεση εκμεταλλεύεται τις αδυναμίες του μηχανισμού anti-replay του πρωτοκόλλου SIP, και αποτελεί κίνδυνο ακόμη και όταν τα INVITE μηνύματα προστατεύονται από SIP αυθεντικοποίηση.

[6] Vonage, AT&T, icallglobe

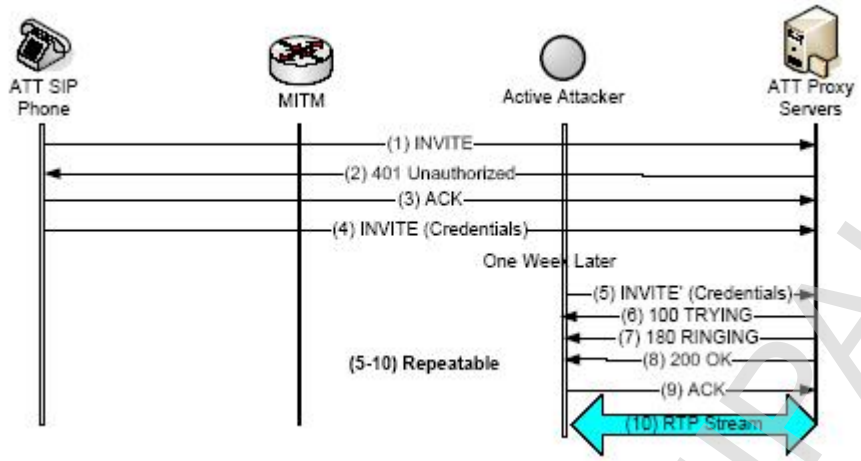
Στο παρακάτω σχήμα απεικονίζεται μία χρεώσιμη επίθεση κατά SIP VoIP συνδρομητών της AT&T.



Σχήμα 20. InviteReplay επίθεση εναντίων ενός SIP συνδρομητή της εταιρίας AT&T.

Ο μηχανισμός MITM, ο οποίος βρίσκεται μεταξύ του SIP τερματικού της AT&T και του AT&T SIP εξυπηρετητή, είναι σε θέση να παρατηρεί και να υποκλέπτει όλα τα SIP μηνύματα, τα οποία στέλνονται από το SIP τηλέφωνο. Ο μηχανισμός αυτός μπορεί στη συνέχεια να αποστέλλει τα υποκλεμμένα INVITE μηνύματα σε άλλον επιτιθέμενο ο οποίος με τη σειρά του μπορεί να πραγματοποιήσει μη εξουσιοδοτημένες κλήσεις, αναπαράγοντας ξανά, το τροποποιημένο πλέον INVITE μήνυμα.

Στο παρακάτω σχήμα διακρίνεται η ροή του μηνύματος κατά τη διάρκεια μίας InviteReplay επίθεσης.



Σχήμα 21. Απεικόνιση ροής μηνύματος InviteReplay επίθεσης κατά SIP τηλεφώνου.

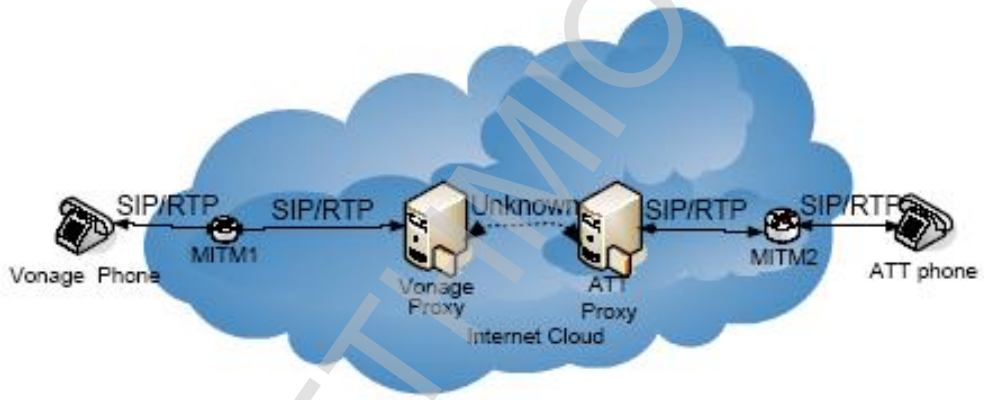
Όπως φαίνεται και στο παραπάνω σχήμα, όταν ο συνδρομητής καλεί έναν PSTN αριθμό, το SIP τηλέφωνο χρειάζεται να αυθεντικοποιήσει το INVITE μήνυμα στον SIP proxy, κατόπιν σχετικού αιτήματος. Ο μηχανισμός MITM είναι σε θέση να υποκλέψει τα πιστοποιητικά αυθεντικοποίησης και να τα αποστείλει στον απομακρυσμένο εν ενεργεία επιτιθέμενο. Ο επιτιθέμενος στη συνέχεια μπορεί εύκολα να τροποποιήσει τις παραμέτρους του RPT session (για παράδειγμα IP διεύθυνση και αριθμό πόρτας), καθώς αυτές δεν προστατεύονται από SIP αυθεντικοποίηση. Κατόπιν, ο επιτιθέμενος είναι σε θέση να ενεργοποιήσει επαναλαμβανόμενες InviteReplay επιθέσεις, επαναλαμβάνοντας το τροποποιημένο INVITE μήνυμα. Έτσι πραγματοποιείται η κλήση μεταξύ του επιτιθέμενου και του SIP server, και ο επιτιθέμενος είναι πλέον σε θέση να είτε να συνομιλήσει με τον καλούμενο, ή να αναπαράγει ηχογραφημένο μήνυμα.

Μετά από μελέτη και πειραματισμούς της εταιρίας AT&T, κατέληξαν στο συμπέρασμα ότι το υποκλεμμένο INVITE μήνυμα μπορεί να χρησιμοποιηθεί από έναν επιτιθέμενο με επιτυχία, ακόμη και μετά από μία εβδομάδα, αφού έχει υποκλαπεί. Αυτό σημαίνει ότι ένας επιτιθέμενος θα μπορεί να εξαπολύει επαναλαμβανόμενες επιθέσεις Invite Replay εναντίων ενός VoIP συνδρομητή.

- **FakeBusy Billing Attack**

Αυτού του είδους η χρεώσιμη επίθεση, στην ουσία υφαρπάζει κλήσεις οι οποίες προορίζονται για έναν VoIP συνδρομητή, και ελέγχει τη διάρκειά τους. Ως αποτέλεσμα, η κλήση αυτή αποτυγχάνει, παρ' όλα αυτά όμως, ο συνδρομητής ο οποίος έχει πραγματοποιήσει την κλήση, χρεώνεται ανάλογα με τη διάρκεια την οποία όρισε ο εισβολέας.

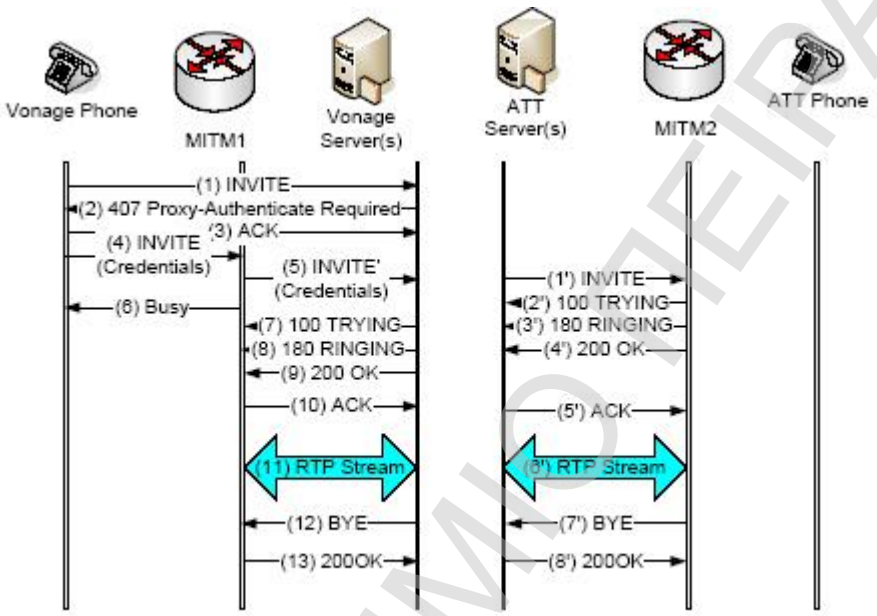
Το παρακάτω σχήμα απεικονίζει την όλη διαδικασία της FakeBusy επίθεσης, της ByeDelay, και της ByeDrop επίθεσης.



Σχήμα 22. Σχηματική απεικόνιση δικτύου, κατά την FakeBusy, ByeDelay, και ByeDrop επίθεση.

Είναι εμφανής η ύπαρξη δύο MITM οντοτήτων. Του MITM1, ο οποίος βρίσκεται μεταξύ του SIP τηλεφώνου, και του SIP server από το ένα άκρο, και του MITM2 στο άλλο άκρο, ο οποίος βρίσκεται και πάλι μεταξύ SIP τηλεφώνου, και του SIP server.

Στο παρακάτω σχήμα απεικονίζεται η ροή μίας FakeBusy χρεώσιμης επίθεσης.



Σχήμα 23. Σχηματική απεικόνιση ροής FakeBusy επίθεσης.

Το αριστερό και δεξί άκρο του σχήματος, απεικονίζει τη ροή των μηνυμάτων του καλούντος, και του καλούμενου αντίστοιχα. Στο σχήμα εμφανίζεται SIP server για να δηλώσουμε τον server ο οποίος χειρίζεται τη σηματοδοσία των μηνυμάτων, και *RTP* server για να δηλώσουμε τον server ο οποίος αναλαμβάνει την ροή *RTP* μηνυμάτων. Σε πείραμα το οποίο πραγματοποιήθηκε από τις εταιρίες διαδικτυακής τηλεφωνίας, Vonage και AT&T, αφέθηκαν οι MITM1 και MITM2 να ανταλλάσουν *RTP* μηνύματα για περίπου 34 λεπτά, προτού ο MITM2 τερματίσει την κλήση. Για τον τερματισμό της κλήσης, ο MITM2 παράγει ένα *BYE* μήνυμα το οποίο και στέλνει στον AT&Tα SIP server. Εφόσον ο AT&T server δεν απαιτεί αυθεντικοποίηση του *BYE* μηνύματος, το δέχεται, στο οποίο και απαντά με ένα *200 OK* μήνυμα, και ζητά από τον Vonage server να τερματίσει την κλήση.

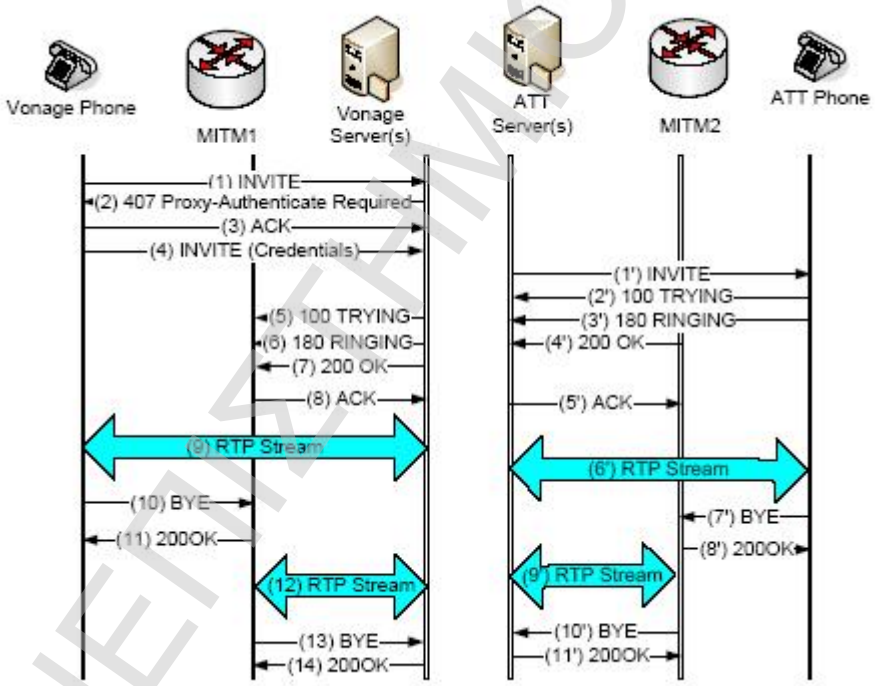
Έτσι, το σύστημα ενεργής δραστηριότητας κλήσεων της Vonage δείχνει ότι έχει πραγματοποιηθεί μία κλήση διάρκειας 34 λεπτών προς δίκτυο της AT&T, ενώ στην πραγματικότητα, ο συνδρομητής έχει την εντύπωση ότι η κλήση την οποία επιχείρησε να πραγματοποιήσει, απέτυχε.

Έτσι ο συνδρομητής έχει χρεωθεί μία κλήση την οποία δεν πραγματοποίησε ποτέ, και ο καλούμενος δεν ειδοποιήθηκε καν για το ότι δέχθηκε κλήση.

- **ByeDelay Billing attack**

Οι ByeDelay χρεώσιμες επιθέσεις επιδιώκουν, πάντα παρασκηνιακά, να παρατείνουν τη διάρκεια των επιτυχημένων κλήσεων μεταξύ καλούντος και καλούμενου VoIP συνδρομητή, καθυστερώντας τα *BYE* μηνύματα.

Στο παρακάτω σχήμα διακρίνεται η ροή των σημάτων κατά την επίθεση.



Σχήμα 24. Ροή μηνυμάτων ByeDelay χρεώσιμης επίθεσης.

Στο σχήμα, τα βήματα 1 έως 9, και 1’ έως 6’ είναι όμοια με αυτά μίας φυσιολογικής, επιτυχημένης κλήσης.

Όταν ο καλούμενος ή ο καλών κλείνει το τηλέφωνό του, και στέλνει ένα *BYE* μήνυμα στον SIP server του, οι MITMs υποκλέπτουν το μήνυμα αυτό και στέλνουν πίσω ένα *200 OK* μήνυμα.

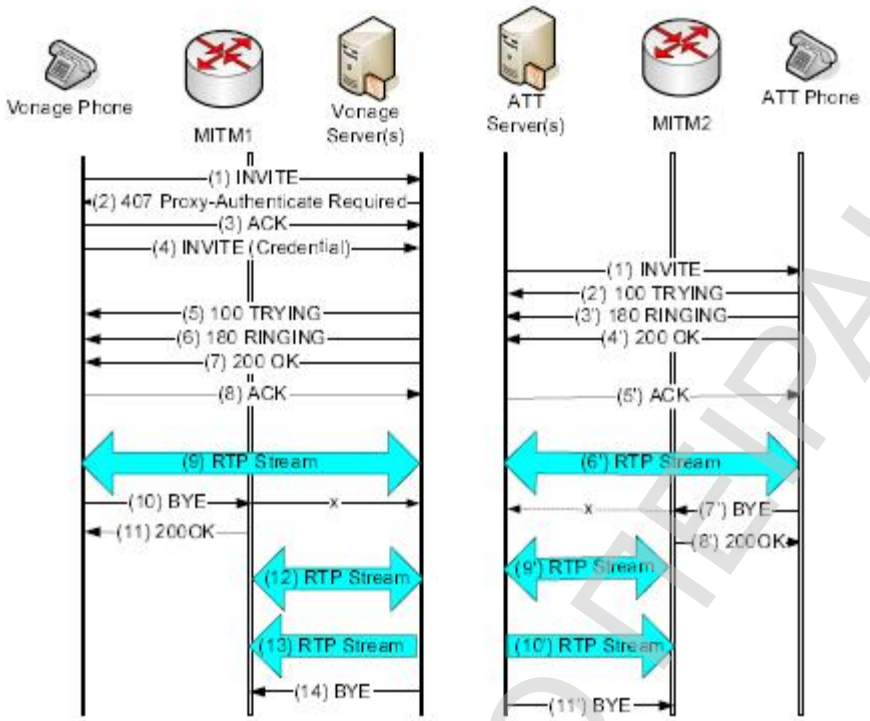
Κάτι τέτοιο θα έδινε στον καλών ή στον καλούμενο την εντύπωση ότι η κλήση τερματίστηκε με επιτυχία, ενώ στην ουσία τα MITMs έχουν αναλάβει την κλήση.
Στα βήματα 12 και 9', ο MITM1 και MITM2 παράγουν εικονικά *RTP* μηνύματα, τα οποία και στέλνουν στους δύο servers αντιστοίχως. Κάτι τέτοιο δίνει στους service providers την εντύπωση ότι ο καλών και ο κληθέν συντηρούν ακόμη μία ενεργή μεταξύ τους κλήση, και συνεπώς συνεχίζουν τη χρέωση ως έχει.

Μία τέτοιου είδους επίθεση είναι ικανή να χρεώσει υπέρογκα ποσά σε κάποιον συνδρομητή, ο οποίος θα έχει πλήρη άγνοια του τι συνέβη.

- **ByeDrop Billing Attack**

Μία τέτοιου είδους επίθεση παρατείνει τη διάρκεια των κλήσεων μεταξύ των VoIP συνδρομητών, απλά απορρίπτοντας τα *BYE* μηνύματα.

Στο παρακάτω σχήμα απεικονίζεται η ροή μηνυμάτων κατά τη διάρκεια μιας ByeDrop χρεώσιμης επίθεσης, η οποία πραγματοποιήθηκε μεταξύ συνδρομητή της AT&T και της εταιρίας Vonage.



Σχήμα 25. Σχηματική ροή μηνυμάτων ByeDrop billing Attack.

Παρομοίως με την ByeDelay επίθεση, οι MITMs υποκλέπτουν τα *BYE* μηνύματα, και απαντούν σε αυτά με *200 OK* μηνύματα, τα οποία δημιουργούν στον καλούντα και στον καλούμενο την εντύπωση ότι η κλήση έχει τερματιστεί επιτυχώς.

Η διαφορά της συγκεκριμένης επίθεσης σε σχέση με την ByeDelay, έγκειται στον τρόπο με τον οποίο αντιμετωπίζονται τα *BYE* μηνύματα. Το αποτέλεσμά τους για τον συνδρομητή είναι ακριβώς το ίδιο. Δείξαμε ότι κακόβουλοι εισβολείς, οι οποίοι βρίσκονται μεταξύ ενός SIP τηλεφώνου και SIP server, είναι σε θέση να εξαπολύσουν επιθέσεις σε συνδρομητές SIP υπηρεσιών, χωρίς να απαιτείται η γνώση μυστικών κωδικών.

Καθώς ο SIP μηχανισμός αυθεντικοποίησης διαθέτει ενσωματωμένη τη δυνατότητα μη επανάληψης μηνυμάτων, οποιαδήποτε ορθή ενσωμάτωσή του σε VoIP επικοινωνιακά συστήματα, θα τα καταστήσει δυσπρόσβλητα σε InviteReplay χρεώσιμες επιθέσεις. Γι’ αυτό το λόγο, η ευπάθεια της εταιρίας τηλεπικοινωνιών AT&Τα στις InviteReplay επιθέσεις, η οποία οφείλεται σε

κενά ενσωμάτωσης, τα οποία όμως είναι εύκολο να διορθωθούν. Παρ'όλα ταύτα, οι FakeBusy, ByeDelay, και ByeDrop επιθέσεις, εκμεταλλεύονται τις δομικές ευπάθειες του SIP πρωτοκόλλου και γι' αυτό το λόγο είναι δυσκολότερο να αντιμετωπισθούν. Για παράδειγμα, η συσχέτιση μεταξύ των *RTP* και *SIP* μηνυμάτων μπορεί να ανιχνεύσει κάποιες VoIP επιθέσεις. Παρ' όλα αυτά, απλά κάνοντας συσχέτιση των *RTP* και *SIP* μηνυμάτων, δεν θα ανιχνευθούν οι FakeBusy, οι ByeDelay, και ByeDrop επιθέσεις, οι οποίες παράγουν εικονικά *RTP* μηνύματα, χρησιμοποιώντας υπάρχουσες IP διευθύνσεις και αριθμούς πόρτας. Αυτό οφείλεται στην έλλειψη ενσωματωμένης προστασίας των *SIP* και *RTP* μηνυμάτων. Εάν τα SIP μηνύματα είναι πλήρως προστατευμένα, και τα *RTP* μηνύματα είναι ορθώς κρυπτογραφημένα μέσω μηχανισμού anti-replay προστασίας, είναι δυνατόν να ανιχνευθούν και να αντιμετωπισθούν οι FakeBusy και ByeDelay επιθέσεις.

Οι ByDrop επιθέσεις, παρ' όλα αυτά είναι επικίνδυνες, παρά την πλήρη προστασία των SIP μηνυμάτων, και την κρυπτογράφηση των *RTP* μηνυμάτων. Καθώς η απόρριψη πακέτων είναι ένα σύνηθες φαινόμενο στο ευρύ διαδίκτυο, είναι δύσκολο να γίνει διαφοροποίηση της ByeDrop επίθεσης από μία απλή απώλεια πακέτων. Το πώς θα γίνει μετριασμός τέτοιου είδους επιθέσεων, παραμένει ένα ανοιχτό θέμα έρευνας από τις εταιρίες και τους πάροχους διαδικτυακής τηλεφωνίας.

Η διαδικασία της χρέωσης είναι θεμελιώδης σε κάθε είδους παροχής VoIP υπηρεσιών, και έχει άμεση επίπτωση στους εκάστοτε συνδρομητές. Η χρήση του ευρύ διαδικτύου για σηματοδοσία, καθιστά την τηλεφωνία περισσότερο ευπαθή σε χρεώσιμες επιθέσεις οι οποίες επικεντρώνονται στο να χτυπήσουν τη διαδικασία σηματοδοσίας. Κάτι τέτοιο δεν συμβαίνει στην PSTN τηλεφωνία. Επιπρόσθετα, η μετάπτωση από την PSTN αρχιτεκτονική στη διαδικτυακή τηλεφωνία, όπου η πολυπλοκότητα και και η ευφυΐα μεταφέρεται πλέον στα περιφερειακά στοιχεία του δικτύου και όχι στον πυρήνα του, καθιστά τη διαδικασία της VoIP χρέωσης περισσότερο ενδιαφέρουσα για τους πάροχους VoIP τηλεφωνίας.

11. Πιθανά σενάρια SPIT και αντίμετρα

Παρακάτω ακολουθεί παράθεση πιθανών σεναρίων SPIT, τα οποία δεν περιορίζονται μόνο στο πλαίσιο της διαδικτυακής τηλεφωνίας, αλλά είναι πολύ πιθανό να εφαρμοστούν σε ευρύτερο φάσμα των επικοινωνιών.

Τα τηλεφωνικά πρωτόκολλα των σύγχρονων τηλεφωνικών πλατφόρμων περιλαμβάνουν συχνά μηχανισμούς οι οποίοι απαιτούν πληροφορίες σχετικές με το γενικότερο τηλεπικοινωνιακό πλαίσιο. Για παράδειγμα, είναι πιθανό να αιτηθεί η κατάσταση προσβασιμότητας του καλούμενου, ή να μεταδοθεί ένα μικρό μήνυμα, το οποίο θα μπορούσε επίσης να χρησιμοποιηθεί για γνωστοποίηση κατάστασης.

Παράλληλα, είναι πιθανή η έκδοση στιγμιαίων μηνυμάτων τα οποία θα μπορούσαν κάλλιστα να χρησιμοποιηθούν ως επικοινωνιακό κανάλι για αυθαίρετες εκπομπές. Είναι αρκετά πιθανό να γίνει εκμετάλλευση της χρηστικότητας της διαδικτυακής τηλεφωνίας για παράνομη μετάδοση διαφημιστικών ηχητικών μηνυμάτων, καθώς και απλών διαφημιστικών κλήσεων.

11.1 Τηλεφωνικά κέντρα

Σε σύγχρονα τηλεφωνικά κέντρα, λειτουργούν διαρκώς τηλεφωνικοί μηχανισμοί (agents) οι οποίοι πραγματοποιούν διαφημιστικές κλήσεις. Ένας υπολογιστής επιχειρεί συστηματικά ή τυχαία μέσω αλγορίθμων, κλήσεις προς διάφορους συνδρομητές. Σε περίπτωση όπου κάποιος καλούμενος απαντήσει την κλήση, αυτός συνδέεται άμεσα με ένα διαθέσιμο υπάλληλο ο οποίος αναλαμβάνει να διεκπεραιώσει την κλήση και τη μετάδοση του διαφημιστικού μηνύματος.

Ο ιδιοκτήτης ενός τέτοιου τηλεφωνικού κέντρου, θα πρέπει να επωμιστεί το κόστος των υπαλλήλων, του απαραίτητου εξοπλισμού και υπολογιστών, καθώς και το κόστος των κλήσεων που πραγματοποιήθηκαν. Το κόστος των τελευταίων είναι μηδαμινό, στα πλαίσια πάντα της διαδικτυακής τηλεφωνίας.

Στο συγκεκριμένο παράδειγμα, το πλήθος των πιθανών ταυτόχρονων κλήσεων, και συνεπώς η επιπτώσεις του φαινομένου spam, εξαρτάται κυρίως από το πλήθος των υπαλλήλων.

11.2 Τηλεφωνικά ρομπότ

Η διαδικτυακή τηλεφωνία αποτελεί μία πλατφόρμα η οποία βασίζεται κυρίως σε ηλεκτρονικούς υπολογιστές. Είναι συνεπώς πιθανό οι υπολογιστές αυτοί να χρησιμοποιούνται έτσι ώστε, συστηματικά ή τυχαία, να επιλέγουν συνδρομητές στους οποίους θα μεταδίδουν, όταν αυτοί δεχτούν την κλήση, ένα ηχογραφημένο διαφημιστικό μήνυμα.

11.3 Επίμονη κλήση

Αφορά την περίπτωση όπου ο υπάλληλος μίας εταιρίας δεν είναι διατεθειμένος να λήξη μία κλήση αν δεν το αποφασίσει ο κληθέντας. Ο υπάλληλος, ενδέχεται να προωθεί κάποιο προϊόν, και να επιμένει με την προσφορά του, ή να μην του επιτρέπεται λόγω κάποιου επαγγελματικού κώδικα να τερματίσει ο ίδιος την κλήση.
Έτσι, η ροή των *call set-up* αιτημάτων είναι από τον καλούντα προς τον καλούμενο, ενώ τα *termination* αιτήματα έχουν την αντίθετη ροή.

11.4 Καλών χρονικά συνειδητοποιημένος

Αφορά την περίπτωση, όπου ο υπάλληλος της εταιρίας προώθησης προϊόντων προσπαθεί να καλύψει όσους περισσότερους συνδρομητές μπορεί, και για να πετύχει κάτι τέτοιο τερματίζει ο ίδιος απροειδοποίητα την κλήση σε περίπτωση όπου αντιληφθεί ότι η προσφορά του δεν πρόκειται να γίνει αποδεκτή. Γι' αυτό το λόγο, τα *call set-up* και *termination* αιτήματα έχουν ροή από τον καλούντα προς τον καλούμενο. Στην ίδια κατηγορία επίσης κατατάσσονται και οι ομαδικές αποστολές fax.

11.5 Προ-ηχογραφημένο μήνυμα

Εδώ το SPIT μεταδίδεται με τη μορφή ηχογραφημένου μηνύματος. Ο ακροατής του μηνύματος, ο οποίος είναι και αυτός που τερματίζει την κλήση, εκτός από σπάνιες περιπτώσει όπου ακολουθεί κάποιες οδηγίες, οι οποίες εμπεριέχονται στο μήνυμα, και εν τέλει συνδέεται με κάποιον υπάλληλο. Συνήθως, τα *call set-up* και *termination* αιτήματα έχουν αντίστοιχη ροή με αυτή της περίπτωσης ”επίμονης κλήσης”.

11.6 Θυρίδα μηνύματος

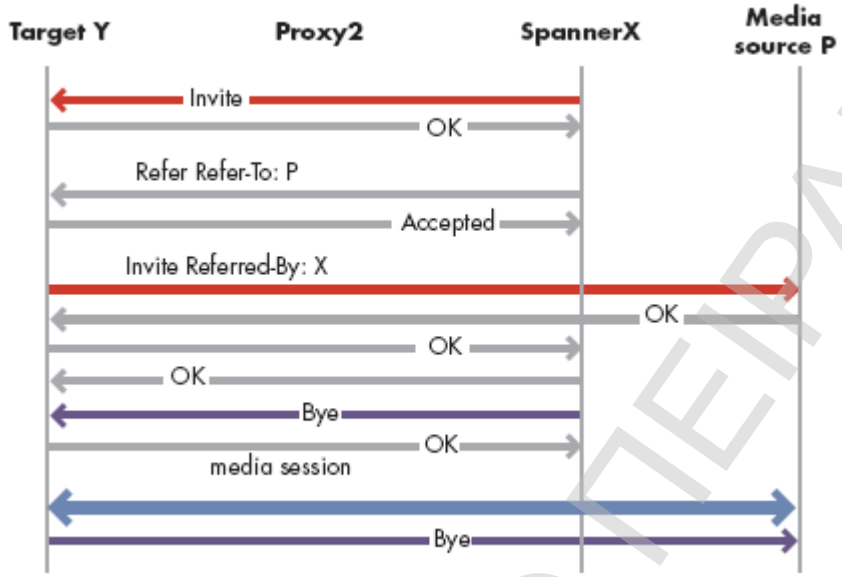
Ο καλών είναι σε θέση να ανιχνεύσει μία θυρίδα ηχητικού μηνύματος από την πλευρά του καλούμενου, και στη συνέχεια είτε να αφήσει κάποιο μήνυμα, ή να τερματίσει την κλήση, ανάλογα με τη μέθοδο δράσης του. Σε κάθε περίπτωση, τα *call set-up* και *termination* αιτήματα φεύγουν από την πλευρά του spammer.

Τα περιστατικά απλών κλήσεων, και εισβολής στα θυρίδα μηνυμάτων είναι δυνατό να διαχωρίζονται στον call server και να καταμετρώνται ξεχωριστά. Έτσι, υπάρχει η δυνατότητα διατήρησης αρχείου για στατιστικούς λόγους, ή για μελλοντική εξάλειψη του φαινομένου.

11.7 Πραγματοποίηση κλήσης από τρίτους

Σύμφωνα με αυτό το σενάριο, υπάρχει το ενδεχόμενο μία κλήση μεταξύ των συνδρομητών P και Y, να πραγματοποιηθεί από το συνδρομητή X. Ο συνδρομητής X μπορεί να είναι ένα spam εικονικό δίκτυο (zombie network), και ο P είτε ένας υπάλληλος εταιρίας τηλεπωλήσεων, ή ένας media server ο οποίος αναπαράγει ένα ηχογραφημένο μήνυμα.

Στο SIP, κάτι τέτοιο θα μπορούσε να επιτευχθεί είτε μέσω 3pcc[7], ή μέσω της μεθόδου REFER, όπως και απεικονίζεται στο σχήμα 26.



Σχήμα 26. Πραγματοποίηση κλήσης SPIT μέσω της μεθόδου REFER

11.8 SPIT κωδωνισμός

Ορισμένες VoIP τηλεφωνικές συσκευές, διαθέτουν προεπιλεγμένη ρύθμιση, έτσι ώστε να δέχονται μία συγκεκριμένη SIP header πληροφορία, η οποία ονομάζεται “Alert Info” και μπορεί να περιέχει ένα URL, το οποίο δείχνει σε ένα προηχογραφημένο ηχητικό μήνυμα κάπου στο διαδίκτυο.
Προφανώς, κάτι τέτοιο μπορεί να χρησιμοποιηθεί με τρόπο τέτοιο, ώστε να αναπαράγονται διαφημιστικά μηνύματα προτού καν η κλήση γίνει δεκτή από τον καλούμενο, αλλά απλώς μόλις ηχήσει η τηλεφωνική συσκευή.

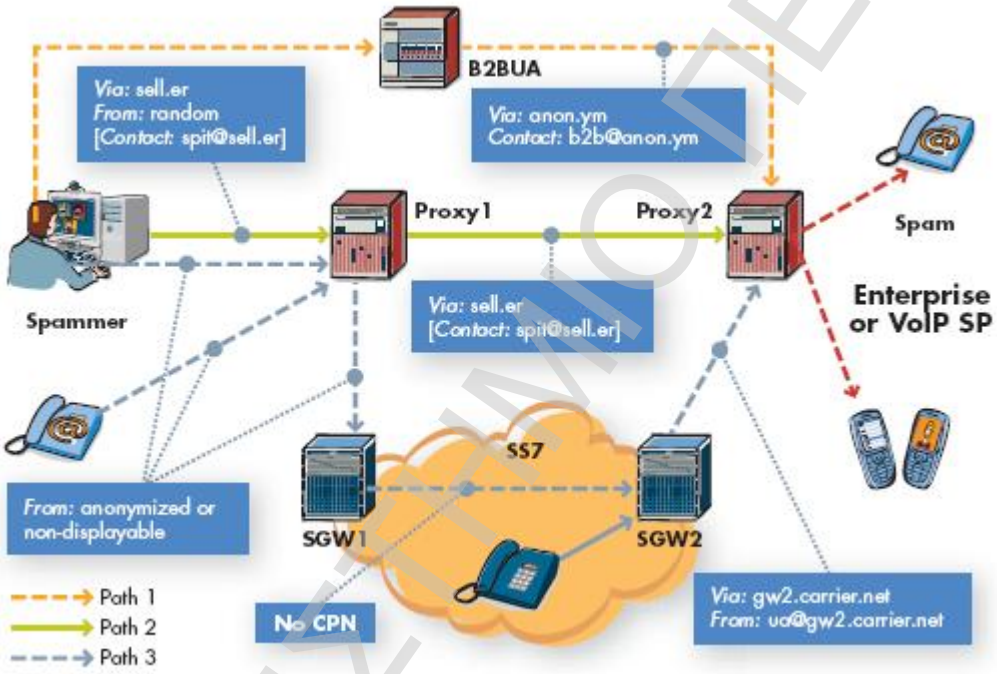
Η λύση σε μία τέτοια περίπτωση θα ήταν η σωστή ρύθμιση της τηλεφωνικής συσκευής, έτσι ώστε να μην επιτρέπεται η αποδοχή ηχητικών δεδομένων από το διαδίκτυο.

[7] Third Party Call Control

11.9 Ανωνυμία

Ανάμεσα στα στοιχεία μίας κλήσης, μπορεί να απαιτούνται και η ταυτότητα του καλούντος, καθώς και η ταυτοποίηση αυτής. Παρ' όλα αυτά, η πραγματική ταυτότητα του συνδρομητή ο οποίος πραγματοποιεί την κλήση, μπορεί να παραμένει άγνωστη.

Εντός των πλαισίων του πρωτοκόλλου SIP για παράδειγμα, ο κακόβουλος εισβολέας (spammer) αρκεί να χρησιμοποιήσει την υπηρεσία SIP B2BUA[8], ως μία δικτυακή υπηρεσία διατήρησης απορρήτου.



Σχήμα 27. Σενάριο SPIT κλήσης, μέσω ανωνυμίας στο SIP.

Σε αυτή την περίπτωση, όπως φαίνεται και στο σχήμα 27 η σηματοδοσία ακολουθεί τη διαδρομή 1. Εναλλακτικά, ο εισβολέας μπορεί να διατηρήσει την ανωνυμία του μέσω του *From* header του SIP *INVITE* signal, αλλά οι πραγματικές τιμές του πρώτου *via* και *Contact* header, διατηρούνται από τον Proxy1. Αυτή είναι η διαδρομή 2 του σχήματος 27. Η τρίτη περίπτωση, η οποία συνθέτει τη διαδρομή 3 του παραπάνω σχήματος, αποτελεί τη

[8] Ο Back-to-Back User Agent (B2BUA) αποτελεί έναν SIP agent, ο οποίος είναι υπεύθυνος για τη διαχείριση της σηματοδοσίας στο SIP μεταξύ δύο άκρων, από την εκκίνηση μίας κλήσης, έως και την ολοκλήρωσή της.

δρομολόγηση της σηματοδοσίας μέσω ενός SS7 δικτύου και του SGW1[9], και στη συνέχεια μέσω του SGW2. Καθώς η CPN[10] παράμετρος δεν περιλαμβάνεται στο SGW1, εάν η τιμή του *From* header είναι μη χρησιμοποιήσιμη (διαστρεβλωμένη, ή περιέχει μη αποδεκτούς χαρακτήρες). Σε αυτή την περίπτωση, ο *From* header θα πάρει θα λάβει πληροφορίες από τον SGW2.

11.10 Συνδυασμός των παραπάνω

Συνδυασμός των προαναφερθέντων σεναρίων είναι θεωρητικά, και όχι μόνο, αρκετά πιθανό να συμβεί. Το κόστος για έναν συνδρομητή είναι επίσης ένας συνδυασμός όλων των σεναρίων, συνεπώς είναι και αρκετά δυσκολότερο να αντιμετωπιστεί μία τέτοιου είδους επίθεση.

[9] Οι Sgw1 και Sgw2 αντιπροσωπεύουν IPsec Security Gateways.
[10] Αριθμός καλούντος (Called Party's Number)

12. Ασφάλεια στη διαδικτυακή τηλεφωνία (SPIT Prevention)

12.1 Γενικά μέτρα ασφάλειας, πριν την επίθεση.

- **Φιλτράρισμα, και Call Blocking**

Η ευθύνη για το φιλτράρισμα ή ακόμη και την απαγόρευση κλήσεων, μπορεί να ανήκει σε διαφορετικά στοιχεία εντός μίας ροής κλήσης. Αυτά καθορίζονται από πολλούς παράγοντες.

Μία περίπτωση ασφάλειας αποτελεί η χρήση μηχανισμού στο ένα άκρο, ο οποίος, με τις ανάλογες ρυθμίσεις, αποφασίζει αν θα απορρίψει μία κλήση, αν θα την προωθήσει τη θυρίδα φωνητικών μηνυμάτων, και θα επιτρέπει τη δρομολόγηση μόνο των ασφαλών, σύμφωνα με τα κριτήριά του, κλήσεων.

Κατά μία άλλη περίπτωση, τη λήψη αποφάσεων σχετικά με την ασφάλεια και εγκυρότητα μίας κλήσης αναλαμβάνει ένας κεντρικός service provider, ο οποίος μπορεί να φιλοξενείται στο τηλεφωνικό κέντρο, ή ακόμη και η ίδια η αρχή ΤΑ, η οποία θα διαθέτει ενσωματωμένες ρυθμίσεις, καθορισμένες από το Member Island ή από τον ίδιο τον τελικό χρήστη.

Το στοιχείο που μεσολαβεί στη ροή μιας κλήσης, και είναι πιθανότερο να επωμιστεί το έργο του διαχωρισμού ασφαλών κλήσεων, είναι το τείχος προστασίας (firewall), ή ο Session Border Controller.

Μία τυπική λίστα με τις ενσωματωμένες ρυθμίσεις ασφάλειας τις οποίες θα περιλαμβάνει ο μηχανισμός, ακολουθεί στη συνέχεια.

- Αναδίπλωση SAML μηνύματος (εάν η αξία του είναι “yes”, θα αναδιπλωθεί ο SAML κώδικας.)
- Απόρριψη της κλήσεως εάν η αξία του IdentityStength < n
- Απόρριψη της κλήσεως εάν η αξία του CostOfCall < n
- Απόρριψη της κλήσεως εάν η αξία του AuthenticationMethod < n
- Απόρριψη της κλήσεως εάν η αξία του IdentityAssertion < n
- Απόρριψη της κλήσεως εάν η αξία του ConnectionSecurity < n

· Απόρριψη της κλήσεως εάν η αξία του SPITSuspected > n

· Απόρριψη της κλήσεως εάν η αξία του Callcenter <> 0

· Απόρριψη της κλήσεως εάν η αξία του AssertionStrength < n

- **Header ασφάλειας**

Το υβριδικό μοντέλο το οποίο ισχύει για την ώρα, είναι πολύ πιθανό να συνεχίσει να εφαρμόζεται για αρκετό διάστημα ακόμη. Το μοντέλο αυτό περιλαμβάνει ένα τείχος προστασίας, το οποίο είναι σε θέση να αντιληφθεί τη γλώσσα SAML, ενώ ο Proxy ή το IP/PBX δεν μπορούν να αντιληφθούν και να μεταγλωττίσουν τον SAML κώδικα. Παρ' όλα αυτά, τα στοιχεία αυτά του VoIP δικτύου είναι, όπως άλλωστε επιβάλλεται, σε θέση να αποκλείσουν ή να δρομολογήσουν κλήσεις ανάλογα με την πιθανότητα αυτές να αποτελούν κλήσεις SPIT. Ο διαχωρισμός αυτός γίνεται με βάση ενσωματωμένων δικλείδων ασφάλειας, οι οποίες εμπεριέχονται στα στοιχεία αυτά.

Για να γίνει η μεταβλητή Ισχύς Δήλωσης (AssertionStrength) διαθέσιμη σε αυτά τα στοιχεία του δικτύου, θα πρέπει αυτή να εισαχθεί στον SIP header. Η επέκταση αυτή θα πρέπει να οριστεί. Προσθέτοντας αυτό το πλήθος πληροφοριών ως header, και έχοντας διαθέσιμες τις SAML δηλώσεις μέσω ενός υπέρ-συνδεδεμένου URL, επιτυγχάνουμε τη μείωση του μήκους του μηνύματος, και παράλληλα επιτρέπουμε την UDP[11] μετάδοση δεδομένων εντός του δικτύου, αν και κάτι τέτοιο δεν συνιστάται λόγω αναξιοπιστίας του πρωτόκολλου.

- **Κωδικός απόρριψης κλήσης**

Στην περίπτωση όπου το τείχος προστασίας (ή η αρχή ΤΑ όταν μιλάμε για την περίπτωση hosted SPIT φιλτραρίσματος) αποφασίζει για το πότε θα γίνει απόρριψη μίας κλήσεως, βασιζόμενο πάντα στις διαθέσιμες πληροφορίες ασφάλειας, θα πρέπει πάντα να επιστρέφει έναν κωδικό σφάλματος. Μέσω αυτού του κωδικού θα ενημερώνει τα υπόλοιπα στοιχεία ασφάλειας του δικτύου, αλλά και τον ίδιο τον συνδρομητή τελικά, για το ότι έχει γίνει κλήση SPIT προς αυτόν, και για το ότι τελικά έγινε απόρριψη της κλήσης. Ο κωδικός

[11] User Datagram Protocol (UDP)

αυτός είναι ο *438* με αιτιολογικό *"Rejected for Security Reasons"*, και μέσω αυτού μπορεί και ο διαχειριστής του δικτύου να ενημερωθεί για το τι έχει συμβεί στο δίκτυο, να ελέγξει την κατάσταση λειτουργίας του τείχους προστασίας, να εφαρμόσει επιπρόσθετες βελτιώσεις σ' αυτό, αλλά και να καταγράψει τις επιθέσεις για στατιστικούς λόγους.

- **Ασφάλιση του SAML header**

Σε αυτού του είδους την αρχιτεκτονική, υποθέτουμε ότι δημιουργείται ένα είδος ασφαλούς σύνδεσης μεταξύ της αρχής TA, και του τερματικού Member Island. Υπάρχουν ευρέως διαδεδομένες μέθοδοι ενσωμάτωσης κώδικα SAML σε ένα SIP μήνυμα. Παρ' όλα αυτά, θα πρέπει να δίνεται ιδιαίτερη προσοχή κατά τη διαδικασία αυτή, ώστε να αποφευχθεί η αλλοτρίωση του κώδικα SAML ή η άθελά μας εφαρμογή replay επιθέσεων.

Πιο συγκεκριμένα, η χρήση SIP-date στη hash function[12] δεν αποτελεί την πιο αξιόπιστη μέθοδο, καθώς γίνεται ανταλλαγή πληροφοριών της ανάλυσης της τιμής του Date, της διαφοράς της τιμής του Date μεταξύ των κόμβων του δικτύου, και της χρονικής παρέκκλισης η οποία δίδεται στις replay επιθέσεις. Με το να εφαρμόζουμε όμως αυστηρότερο συγχρονισμό των date μεταβλητών, οι θεμιτές κλήσεις είναι πολύ πιθανό να απορρίπτονται, καθώς τα ρολόγια θα πρέπει να είναι απόλυτα συγχρονισμένα, κάτι το οποίο είναι δύσκολο στην εφαρμογή του.

Η παραπάνω υλοποίηση προϋποθέτει την διάθεση πληροφοριών, οι οποίες σχετίζονται με τα επίπεδα ασφάλειας και την ταυτοποίηση κλήσης, σε μία έμπιστη κεντρική αρχή. Παράλληλα προϋποθέτει τη δυνατότητα πραγματοποίησης ανώνυμων κλήσεων μεταξύ των συνδρομητών του ίδιου δικτύου. Καθώς η IP τηλεφωνία εξελίσσεται, μας δίνεται η δυνατότητα πλέον, όπου δεν υπάρχει ανάγκη για ανωνυμία, να κάνουμε εισαγωγή πληροφοριών σχετικά με τον καλούντα, λίγο πριν την τελική συσκευή του συνδρομητή ο οποίος λαμβάνει την κλήση, ή στον proxy του Member Island. Κάτι τέτοιο αυξάνει κατά πολύ τα επίπεδα ασφάλειας, και καθιστά πολύ πιο δύσκολη την

[12] Συναρτήσεις κατατεμαχισμού. Συναρτήσεις που μετατρέπουν ένα κλειδί αναζήτησης σε διεύθυνση μνήμης.

υποκλοπή πληροφοριών σχετικά με την ταυτότητα και τα στοιχεία κάποιου συνδρομητή. Εάν δεν υπάρχουν πληροφορίες προς εισαγωγή, τότε μπορεί να εισαχθεί ένα κομμάτι κώδικα SAML. Σε αυτή την περίπτωση, το τερματικό member island είναι αυτό το οποίο θα πρέπει να αναγνωρίσει και να μεταγλωττίσει τον κώδικα SAML, να πάρει τις πληροφορίες που αυτός περιέχει, και να πραγματοποιήσει στη συνέχεια το σχετικό φιλτράρισμα κλήσεων.

Υπάρχουν περιπτώσεις, όπου η κεντρική αρχή ασφάλειας του VoIP τηλεφωνικού κέντρου εξακολουθεί να κατέχει σημαντικές πληροφορίες ασφάλειας, ακόμη και αν οι τελικοί χρήστες ή τα Member Islands, κάνουν οι ίδιοι παράλληλα δηλώσεις ασφάλειας. Σε αυτή την περίπτωση, η προτιμότερη λύση αποτελείται από ένα υβριδικό μοντέλο μίξης κώδικα SAML και προσθήκες ασφάλειας από την κεντρική αρχή του κέντρου.

Ο κώδικας SAML καθορίζει μεθόδους αίτησης πληροφοριών ασφάλειας οι οποίες μπορούν να διακινηθούν από την αρχή ασφάλειας σε συμπαγή μορφή, μέσω ασφαλούς διαδρομής, έτσι ώστε να διατηρηθούν μυστικές και ασφαλείς ακόμη και από τον συνδρομητή από τον οποίο προέρχονται. Κάτι τέτοιο μπορεί να πραγματοποιηθεί σε αρχιτεκτονικές όπου η κλήση δεν χρειάζεται να ακολουθήσει διαδρομή μέσω κεντρικών κομβικών σημείων ή όπου η πληροφορίες ασφάλειας βρίσκονται εκτός του δικτύου.

Είναι προφανές ότι την περαιτέρω αύξηση ασφάλειας και την αναγνώριση πιθανού SPIT, θα επέφερε η χρήση μηχανισμών όπως Firewalls ή Session Border Controllers, καθώς και η επιπλέον συνεργασία τους με την αρχής ασφάλειας και τα Member Islands.

13. Γενική αρχιτεκτονική μηχανισμών πρόληψης Spam στην διαδικτυακή τηλεφωνία

Ένας μηχανισμός πρόληψης SPIT θα πρέπει να πληροί κάποιες βασικές προϋποθέσεις, και να καλύπτει ορισμένες απαιτήσεις, έτσι ώστε να μπορεί να φανεί αποτελεσματικός. Οι προϋποθέσεις αυτές συνοψίζονται στις εξής:

- Θα πρέπει να ελαχιστοποιεί την πιθανότητα αποκλεισμού γνήσιων και νόμιμων κλήσεων.
- Θα πρέπει να μεγιστοποιεί την πιθανότητα αποκλεισμού κακόβουλων, spit κλήσεων.
- Η αναγκαιότητα παρέμβασης του καλούμενου, έτσι ώστε να προσδιορισθεί εάν η εκάστοτε κλήση αποτελεί κλήση spit ή όχι, θα πρέπει να μειωθεί στο ελάχιστο δυνατό.
- Όσο το δυνατό περισσότερο θα πρέπει να ελαχιστοποιηθεί η αναξιοπιστία η οποία προκαλείται στον καλούντα, καθώς αυτός προσπαθεί να πραγματοποιήσει μία νόμιμη κλήση.
- Οι εφαρμογές οι οποίες να βρίσκει ο μηχανισμός αυτός, δεν θα πρέπει να έχουν περιορισμούς όσον αφορά την τοποθεσία (γραφείο, σπίτι, δημόσιος χώρος, και λοιποί χωροταξικοί περιορισμοί), τις διαφορετικές κουλτούρες και συνήθειες των συνδρομητών, τη γλώσσα τους, το επίπεδο ασφάλειας το οποίο αυτοί απαιτούν, καθώς και άλλους τυχόν περιορισμούς.

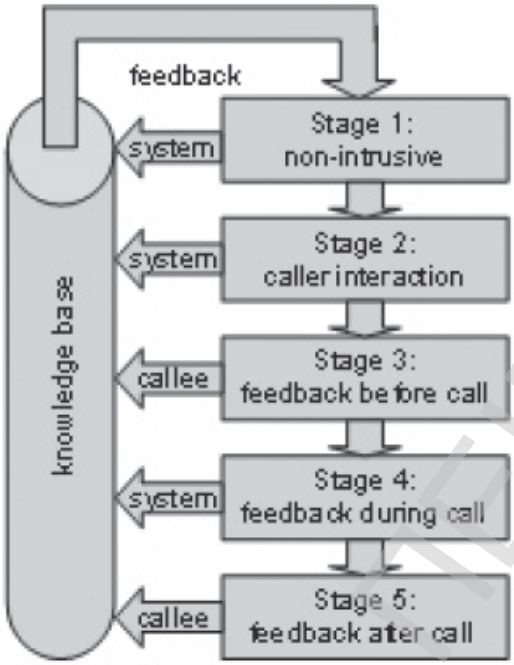
Αναφέροντας τα χαρακτηριστικά τα οποία θα πρέπει να διαθέτει ένας αξιόπιστος spit prevention μηχανισμός, θα πρέπει να αναφέρουμε επίσης ορισμένα χαρακτηριστικά τα οποία θα τον κάνουν πιο φιλικό και ευπροσάρμοστο στις εκάστοτε ανάγκες ενός οργανισμού. Τα χαρακτηριστικά αυτά αποτελούν κυρίως χαρακτηριστικά τα οποία θα πρέπει να λάβουν υπ ’όψιν τους οι σχεδιαστές ενός τέτοιου μηχανισμού.

Ορισμένα από αυτά είναι η δυνατότητα αναβάθμισής του, καθώς οι μέθοδοι spit εξελίσσονται διαρκώς καταφέρνοντας πολλές φορές να υπερνικούν σύγχρονες μεθόδους πρόληψής τους. Επιπρόσθετα, η ευκολία στην παραμετροποίηση και την σε βάθος χρόνου υποστήριξή του συστήματος, διότι ένας οργανισμός, καθώς και το τηλεφωνικό του κέντρο, μεταβάλλεται διαρκώς με ρυθμό τον οποίο θα πρέπει να ακολουθεί και το σύστημα ασφάλειάς του. Οι ενέργειες αυτές θα πρέπει να γίνονται με τη μεγαλύτερη δυνατή ευκολία από το εξειδικευμένο προσωπικού του οργανισμού ή του πάροχου διαδικτυακής τηλεφωνίας. Τελευταίος, αλλά σίγουρα από τους σημαντικότερους παράγοντες αποτελεί το κόστος του μηχανισμού, το οποίο λαμβάνεται σοβαρά υπ' όψιν, ιδίως όταν πρόκειται για μικρές επιχειρήσεις ή νεοσυσταθείς πάροχους τηλεφωνίας.

Υπάρχουν πολλοί μέθοδοι αντιμετώπισης spit κλήσεων, καθώς και πληθώρα μηχανισμών. Κανείς όμως από αυτούς δεν είναι σε θέση να καλύψει όλες τις προαναφερθείσες απαιτήσεις. Επιπρόσθετα, οι αποτελεσματικότερες μέθοδοι αντιμετώπισης spit απαιτούν αλληλεπίδραση με τον καλούντα, και συνεπώς χαρακτηρίζονται ως περισσότερο επιθετικογενείς, έτσι ώστε να αναγκάσουν τον καλούντα να τερματίσει ο ίδιος τη συνεδρία, με αποτέλεσμα ο καλούμενος να χάσει πιθανές σημαντικές κλήσεις.

Ακόμη χειρότερα, άλλες μέθοδοι απαιτούν για να λειτουργήσουν, και τη συνδρομή του καλούντα. Συνεπώς, ένα αποτελεσματικό σύστημα αντιμετώπισης spit κλήσεων θα πρέπει να συνδυάζει τις δυνατότητες και τα θετικά στοιχεία διαφορετικών μεθόδων, έτσι ώστε το σύστημα αυτό το οποίο προκύπτει να είναι τελικά σε θέση να αντιμετωπίσει αποτελεσματικά spit κλήσεις, απαιτώντας την ελάχιστη δυνατή συνδρομή του καλούντα και του καλούμενου.

Βασιζόμενοι στα παραπάνω, μπορούμε να προτείνουμε μία γενικευμένη αρχιτεκτονική συστήματος αντιμετώπισης spit κλήσεων, η οποία αποτελείται από πέντε αυξανόμενα επίπεδα εισβολής.



Σχήμα 28. Γενική αρχιτεκτονική συστήματος αντιμετώπισης κλήσεων spit.

Τα πέντε επίπεδα, από τα οποία αποτελείται το σύστημα αυτό, φροντίζουν ώστε παράλληλα με το διαχωρισμό μίας κακόβουλης κλήσης και απόρριψή της, να συνδράμουν παράλληλα στον εμπλουτισμό της γνωσιακής βάσης του συστήματος, το οποίο γίνεται ”εξυπνότερο” και είναι σε θέση στο μέλλον να αναγνωρίσει εξ’ αρχής μία πιθανή επίθεση.

Κατά το πρώτο επίπεδο, οι μέθοδοι πρόληψης δρουν “αόρατα”, απευθείας στον καλούντα και τον καλούμενο. Στο δεύτερο επίπεδο, η μέθοδος πρόληψης αλληλεπιδρά με τον καλούντα ή με την τερματική του συσκευή. Το τρίτο επίπεδο απαιτεί τη συνδρομή του καλούμενου προτού καν η κλήση πραγματοποιηθεί, ενώ κατά το τέταρτο επίπεδο ασφάλειας προσδιορίζονται οι μέθοδοι οι οποίες κρίνουν την επικινδυνότητα της κάθε κλήσης, ενώ αυτή είναι ενεργή. Εν τέλει, κατά το πέμπτο επίπεδο, απαιτείται η συνδρομή του καλούντα, μετά το πέρας της κλήσης, έτσι ώστε να ανιχνευθεί παρόμοια κλήση στο μέλλον και να μπλοκαριστεί.

Σε όλα τα επίπεδα, είτε οι αυτοματοποιημένοι μηχανισμοί, είτε ο καλούμενος, συμβάλουν στη λειτουργία του συστήματος, το οποίο απαιτεί τη γνωστοποίηση αρχικών πληροφοριών, έτσι ώστε να διαθέτουν κάποια τμήματά του αρχικές γνώσεις κατά το πρώτο επίπεδο λειτουργίας.

Παρ' όλα αυτά, μία εισερχόμενη κλήση δεν θα πρέπει να περάσει οπωσδήποτε και από τα πέντε επίπεδα. Για παράδειγμα, μία κλήση η οποία έχει ήδη αναγνωριστεί ως "νόμιμη" κατά το πρώτο επίπεδο του συστήματος, δεν χρειάζεται να ελεγχθεί περαιτέρω, οπότε μπορεί απευθείας να της επιτραπεί να πραγματοποιηθεί.
Σε γενικές γραμμές, η πραγματική πορεία την οποία θα ακολουθήσει μία κλήση, εξαρτάται από συγκεκριμένους παράγοντες, όπως ο βαθμός εισβολής ο οποίος επιτρέπεται από κάθε σύστημα.

Είναι αποδεδειγμένο στην πράξη πως μεγαλύτερη αποτελεσματικότητα επιτυγχάνεται μέσω μεθόδων υψηλότερων επιπέδων, οι οποίες είναι εκ κατασκευής περισσότερο επιθετικογενείς. Ένα αποτελεσματικό σύστημα αντιμετώπισης spit κλήσεων, θα πρέπει να συνθέτεται από πολλαπλές μεθόδους και να καλύπτει όλα τα επίπεδα, διατηρώντας μία ισορροπία μεταξύ του επιπέδου επιτρεπτής εισβολής και της αποτελεσματικότητας.

13.1 Χτίζοντας τα τμήματα ενός συστήματος πρόληψης spit κλήσεων

Πληθώρα πιθανών μεθόδων σχετικά με το τμηματικό χτίσιμο συστημάτων αντιμετώπισης spit, είναι υπό συζήτηση[13]. Θα παρουσιάσουμε μία γενική άποψη των γνωστότερων εξ' αυτών, κάνοντας αντιστοίχηση διαφόρων μεθόδων στα επίπεδα της γενικής αρχιτεκτονικής, τα οποία φαίνονται στο σχήμα 28.

[13] J. Rosenberg et al., "The Session Initiation Protocol (SIP) and Spam," draftietf-sipping-spam-01.txt, July 2005. Work in progress.

13.1.1 Επίπεδο 1. Καμία αλληλεπίδραση καλούντα και καλούμενου

Οι μέθοδοι αυτού του επιπέδου, δεν απαιτούν συνδρομή του καλούντα, καθώς αυτές είναι εντελώς αόρατες σε αυτόν.

- **Λίστες**

Η ταυτότητα του καλούντα συγκρίνεται με ένα πλήθος αποθηκευμένων ταυτοτήτων, έτσι ώστε να παρθεί απόφαση για το αν θα πρέπει να γίνει αποδοχή ή απόρριψη της κλήσης. Κατά τη διαδικασία αυτή λαμβάνονται υπ' όψη δύο είδη λιστών: Η "λευκή" και η "μαύρη" λίστα. Οι ταυτότητες οι οποίες είναι αποθηκευμένες στη λευκή λίστα, είναι αυτές οι οποίες τους επιτρέπεται να πραγματοποιούν κλήσεις, ενώ οι ταυτότητες της μαύρης λίστας θα απορριφθούν κατά την προσπάθειά τους να κάνουν κλήση. Μία τέτοια μεθοδολογία έχει τα πλεονεκτήματα της ευκολίας κατά την ενσωμάτωσή της σε ένα σύστημα, καθώς η τεχνολογία των βάσεων δεδομένων είναι αρκετά ανεπτυγμένη και ευέλικτη.

- **Αξιόπιστες ομάδες**

Αξιόπιστες ενδοδικτυακές συνδέσεις ελέγχονται προτού προωθηθεί κάποια κλήση στον τελικό συνδρομητή. Η λογική της συγκεκριμένη μεθόδου είναι το να γίνεται εντός κάθε domain εσωτερικός έλεγχος των συνδρομητών του, και να γίνει συμφωνία μεταξύ των διαφόρων domains έτσι ώστε να αποφεύγεται η μεταξύ τους αποστολή SPIT/SPAM. Η εφαρμογή μίας τέτοιας μεθοδολογίας είναι απλή, καθώς δεν απαιτείται υψηλού επιπέδου τεχνολογία, παρά μόνο απλές παραμετροποιήσεις.

- **Μοτίβο ανίχνευσης ανωμαλιών**

Κατά τη μέθοδο αυτή γίνεται προσπάθεια ανίχνευσης ύποπτων μοτίβων στη ροή της κίνησης, έτσι ώστε να ανιχνευθεί τυχόν spit. Ύποπτα μοτίβα μπορούν να ανιχνευθούν είτε μέσω συγκεκριμένων κανόνων αναγνώρισής των, ή με τη βοήθεια στατιστικών κανόνων.

Μία τέτοια μέθοδος δεν αντιμετωπίζει ιδιαίτερα προβλήματα κατά την ενσωμάτωσή της, καθώς η τεχνολογία την οποία απαιτεί είναι αρκετά

σύγχρονη, παρά το γεγονός ότι δεν έχει μέχρι στιγμής εφαρμοσθεί στο χώρο της διαδικτυακής τηλεφωνίας.

- **Γκρίζες λίστες**

Αποτελεί μία τεχνική η οποία συχνά αναφέρεται ως PMG (Progressive Multi Grey-leveling). Η μέθοδος αυτή παρακολουθεί διαρκώς τις κλήσεις, και αντιστοιχεί ένα επίπεδο του γκρίζου σε κάθε συνδρομητή. Εάν κάποιος χρήστης προσπαθεί επανειλημμένα να πραγματοποιήσει μία κλήση μέσα σε ορισμένο χρονικό διάστημα, το επίπεδο του γκρίζου του αυξάνεται σε πιο έντονο. Όταν ο χρήστης λήξει τις προσπάθειες κλήσης, το επίπεδο του γκρίζου του μειώνεται. Ευνόητο είναι πως όταν το επίπεδο του γκρίζου κάποιου χρήστη ξεπεράσει ένα προκαθορισμένο κατώφλι, αυτομάτως ο χρήστης θεωρείται ως υποψήφιος spammer. Η τεχνική αυτή, η υλοποίησή της οποίας χαρακτηρίζεται από μέτριου επιπέδου πολυπλοκότητα, έχει ήδη εφαρμοσθεί από ερευνητές[14].

13.1.2 Επίπεδο 2. Αλληλεπίδραση με τον καλούντα

Σε αυτό το επίπεδο οι μέθοδοι απαιτούν είτε τη συμμετοχή της τερματικής συσκευής του καλούντα (αποδεικτικά αποστολής), ή τη συμμετοχή του καλούμενου.

- **Υπολογιστικά Παζλ**

Η τεχνική αυτή αναθέτει μία πολυδάπανη σε πόρους διαδικασία στο τερματικό του καλούντα, προτού πραγματοποιηθεί η κλήση. Τα υπολογιστικά παζλς με τη συνύπαρξη του SIP πρωτοκόλλου έχουν πλέον καθιερωθεί από την IETF[15], καθώς η υλοποίησή της είναι μέτριας πολυπλοκότητας.

[14] D. Shin, and C. Shim, "Voice Spam Control with Gray Leveling," Proc. of 2nd VoIP Security Workshop, Washington DC, June 1-2 2005.
[15] Internet Engineering Task Force, an internet standards organization.

- **Αποδεικτικά Αποστολής**

Η φιλοσοφία της μεθόδου αυτής έχει να κάνει με το να επιβεβαιωθεί ότι ο καλλών είναι όντως ένας πραγματικός συνδρομητής, και το αποδεικτικό το οποίο στέλνει προέρχεται όντως από το domain του.

Μία τέτοια μεθοδολογία είναι δύσκολη στην υλοποίηση, ιδίως στις επικοινωνίες πραγματικού χρόνου και συνεπώς στην αντιμετώπιση φαινομένων SPIT, καθώς απαιτείται χρόνος κατά την αποστολή και έλεγχο των αποδεικτικών.

- **Turing Tests**

Τα τεστ αυτά, αποτελούν μία απλή μέθοδο αναγνώρισης εάν ο χρήστης είναι ένας ηλεκτρονικός υπολογιστής, ή μία ανθρώπινη οντότητα. Η μέθοδος αυτή απαιτεί έναν server ο οποίος ζητά από το χρήστη να απαντήσει σε απλά ερωτήματα τα οποία ο ίδιος ο server είναι σε θέση να παράγει και να αξιολογήσει.

Καθώς ένας υπολογιστής δεν είναι σε θέση να απαντήσει τέτοια ερωτήματα, θεωρείται ότι ο χρήστης που έδωσε σωστή απάντηση αποτελεί ανθρώπινη οντότητα.

Τέτοιου είδους τεστ συναντάμε συχνά σε σελίδες εισαγωγής στοιχείων μας στο διαδίκτυο, προς επιβεβαίωση ότι δεν είναι στο άλλο άκρο μία μηχανή spam.

Τα τεστ αυτά ονομάζονται CAPTCHAs (Completely Automated Public Turing Test to Tell Computers and Humans Apart).

Στην περίπτωση του SPIT prevention κάνουμε χρήση ηχητικών CAPTCHAs, παρά το γεγονός ότι κατά την εφαρμογή της μεθόδου αυτής υπάρχει μία ροπή προς τα σφάλματα λόγω των ηχητικών παραμορφώσεων.

13.1.3 Επίπεδο 3. Διακοπή καλούμενου από κλήση SPIT

Οι μέθοδοι αυτού του επιπέδου απαιτούν, τουλάχιστον τις περισσότερες φορές, ενέργειες από τον καλούμενο κατά τη λήψη μίας κλήσης SPIT.

- **Επικοινωνία βασισμένη σε έγκριση άδειας**

  Η λύση αυτή απαιτεί τον χρήστη Α να εξουσιοδοτήσει το χρήστη Β, κατά την πρώτη φορά όπου ο χρήστης Β θα προσπαθήσει να έρθει σε επαφή με τον Α.

  Ένα πλαίσιο εργασίας, το οποίο βασίζεται σε τέτοιου είδους μεθόδους συνδυασμένες με λίστες, υιοθετείται από τον οργανισμό IETF προς παραγωγή στάνταρντ για το πρωτόκολλο SIP.

13.1.4 Επίπεδο 4. Λήψη κλήσης από τον καλούμενο

Εδώ απαιτείται από τον καλούμενο να κάνει λήψη αρχικά της κλήσεως, και να πραγματοποιήσει τις όποιες ενέργειες κατά τη διάρκεια της κλήσης. Από τη μέχρι τώρα μεθοδολογία, σ' αυτή την κατηγορία ταιριάζει η μέθοδος του φιλτραρίσματος περιεχόμενου, η οποία δεν είναι από τι πλέον ενδεδειγμένες για την αντιμετώπιση SPIT. Παρ' όλα αυτά μπορούν ενδεχομένως να προταθούν άλλες μέθοδοι οι οποίες ταιριάζουν στην κατηγορία αυτή. Γι' αυτό το λόγο κρίνεται χρήσιμος ο προσδιορισμός της συγκεκριμένης αρχιτεκτονικής, έτσι ώστε να γίνει αντιστοίχηση μεθόδων οι οποίες ταιριάζουν σ' αυτή.

13.1.5 Επίπεδο 5. Ανάδραση από τον καλούμενο μετά την κλήση

Σ' αυτό το επίπεδο, ζητείται η συνδρομή του καλούμενου σχετικά με τις κλήσεις τις οποίες έχει λάβει.

- **Σύστημα βασισμένο στη φήμη**

  Ένα σύστημα βασισμένο στη φήμη, λειτουργεί βάση βαθμολογίας η οποία αναρτάται σε κάθε επαφή. Η βαθμολογία αυτή εξαρτάται από το εάν η επαφή έχει στο παρελθόν επιδείξει καλή ή άσχημη "συμπεριφορά".

Περισσότερο αποδοτική θα είναι αυτή βαθμολογία, εάν βασιστεί στην αξιολόγηση άλλων χρηστών, αλλά θα μπορούσε επίσης να σχηματιστεί χωρίς τη μεσολάβηση κάποιου χρήστη, βάση κριτηρίων τα οποία εξαρτώνται από άλλες μεθόδους αντιμετώπισης SPIT.

Μία τέτοια μεθοδολογία δεν είναι καθόλου δύσκολη στην εφαρμογή και ενσωμάτωσή της, με μόνο σημείο στο οποίο θα πρέπει να δοθεί σημασία, η δημιουργία κάποιων στάνταρντ όσων αφορά το πλαίσιο εργασίας.

- **Διευθύνσεις μειωμένης χρήσης**

Ένας μηχανισμός ο οποίος ακολουθεί την τεχνική αυτή, προσπαθεί να αντιμετωπίσει τα φαινόμενα SPIT, ανιχνεύοντας τη διεύθυνση στην οποία θα εμφανιστεί το πρώτο spam μήνυμα, και αλλάζοντάς την άμεσα.

Η ενσωμάτωση της μεθοδολογίας αυτής είναι σχετικά εύκολη, καθώς δεν απαιτεί τεχνολογία υψηλού επιπέδου, αρκετά όμως δύσκολη είναι η εφαρμογή της, καθώς η απόκριση του μηχανισμού πρέπει να είναι άμεση, η αλλαγή διεύθυνσης να γίνεται ταχύτατα, καθώς και να υπάρχει απόθεμα διευθύνσεων.

- **Πληρωμή Ρίσκου**

Ο μηχανισμός αυτός λειτουργεί χρεώνοντας προκαταβολικά ένα πάγιο τέλος τους συνδρομητές για την πρώτη κλήση που θα επιχειρήσουν να κάνουν. Το τέλος αυτό επιστρέφεται όταν διαπιστωθεί ότι η κλήση αυτή δεν αποτελούσε κλήση SPIT, και παράλληλα ο συνδρομητής προστίθεται στις λευκές λίστες.

Η τεχνική αυτή απαιτεί έναν μηχανισμό αναγνώρισης κλήσεων SPIT και ένα εξελιγμένο σύστημα χρέωσης το οποίο θα πρέπει να συνεργάζεται με το κέντρο ξεχωριστά από το βασικό σύστημα χρέωσης. Οι απαιτήσεις αυτές, καθώς και το γεγονός ότι μία τέτοιου είδους χρέωση προς τους συνδρομητές θα ήταν αντιδεοντολογική, καθιστούν την τεχνική αυτή όχι τόσο ρεαλιστική, καθώς και πολύ δύσκολη στην εφαρμογή της.

- **Νόμιμες Ενέργειες**

Η μέθοδος αυτή βασίζεται στην προώθηση νομοθετικών ρυθμίσεων προς όλα τα κράτη, έτσι ώστε να γίνει ποινικοποίηση του spam στη διαδικτυακή τηλεφωνία.

Παρά το γεγονός ότι κάτι τέτοιο στη υλοποίησή του φαίνεται σχετικά απλό, στην πράξη είναι εντελών μη ρεαλιστικό, καθώς υπάρχει έλλειψη ενός διεθνούς νομοθετικού πλαισίου εργασίας, όσων αφορά τις επικοινωνίες. Παράλληλα, θα ήταν πολύ δύσκολη η συμφωνία όλων των κρατών σε ένα τέτοιο νομοθετικό πλαίσιο, καθώς ο ρυθμός ανάπτυξης της διαδικτυακής τηλεφωνίας από κράτος σε κράτος, διαφέρει δραματικά.

- **Ανάδραση μετά την πρώτη επαφή**

Ένας μηχανισμός σε αυτή την περίπτωση φροντίζει έτσι ώστε η ανάδραση να γίνεται από τον καλούμενο ακριβώς μετά την πρώτη επαφή με κάθε συνδρομητή.

Η βασική ιδέα είναι να επιτρέπεται η κλήση από οποιονδήποτε ανώνυμο συνδρομητή μόνο μία φορά. Μετά το πέρας αυτής της πρώτης κλήσης, ο καλούμενος θα πρέπει να κάνει αξιολόγηση της κλήσης την οποία δέχτηκε. Εάν η κλήση αυτή αποτελεί μία SPIT κλήση, ο καλούμενος δηλώνοντάς την, αποτρέπει την επανάληψή της στο μέλλον. Και σε αυτή την περίπτωση κάνουμε χρήση λιστών ασφαλών και μη συνδρομητών.

Η μέθοδος αυτή μειονεκτεί λόγω του ότι υπάρχει πιθανότητα ένας συνδρομητής να δεχτεί αρκετές SPIT κλήσεις, προτού δημιουργήσει πλούσια λίστα με απαγορευμένους καλούντες. Παρουσιάζει αρκετά κοινά στοιχεία με τη μέθοδο αντιμετώπισης spam emails.

13.2 Το επόμενο επίπεδο ενός συστήματος πρόληψης spit κλήσεων

Σε αυτό το κομμάτι θα γίνει περιγραφή ενός θεωρητικού συστήματος πρόληψης SPIT, η οποία θα βασίζεται σε ανάλυση ενός μοτίβου ανθρώπινης

επικοινωνίας. Ο σχεδιασμός και η ενσωμάτωση του συστήματος αυτού βασίζονται σε μεθόδους και αρχές τις οποίες περιγράψαμε προηγουμένως κατά την ανάλυση της βασικής αρχιτεκτονικής ενός τέτοιου συστήματος.

Ο βασικός σκοπός ενός συστήματος πρόληψης SPIT είναι η προστασία του καλούμενου από το να τον διαταράξει μία κλήση SPIT, εξασφαλίζοντας παράλληλα ότι ο ίδιος δεν θα χάσει καμία μη SPIT κλήση. Σε μία ιδανική περίπτωση, αυτό θα πρέπει να επιτευχθεί με τρόπο τέτοιον ώστε να είναι απολύτως φιλικός προς τον καλούμενο. Παρ' όλα αυτά, η εφαρμογή της μεθόδου του πρώτου επιπέδου, η οποία λειτουργεί όντας αόρατη στον καλούντα και τον καλούμενο, δεν είναι αρκετά αποτελεσματική. Γι' αυτό το λόγο θα πρέπει να λαμβάνουμε σοβαρά υπ όψη ένα σταθερό επίπεδο εισβολής.

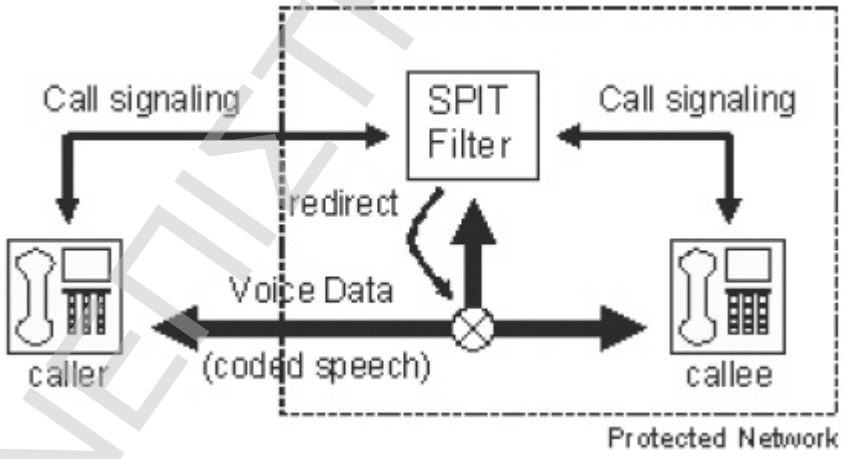
Για να καταφέρουμε να αποφύγουμε οποιαδήποτε διαταραχή του καλούμενου από κλήση SPIT, θα εστιάσουμε τη θεωρητική μελέτης μας σε ένα καινοτομικό Turing Test (CAPTHCA), για πρόληψη SPIT. Κατά το δεύτερο επίπεδο, το σύστημα πρόληψης SPIT δέχεται μία εισερχόμενη κλήση εκ μέρους του καλούμενου και πραγματοποιεί έναν έλεγχο. Βάση του αποτελέσματος, η κλήση είτε προωθείται στον καλούμενο ή απορρίπτεται, όπως φαίνεται και στο σχήμα 29.

Υποθέτοντας ότι ως επί το πλείστον οι κλήσεις SPIT πραγματοποιούνται από υπολογιστικά προγράμματα και όχι από ανθρώπινες οντότητες, θα περιγράψουμε μία ισχυρή μέθοδο η οποία πραγματοποιεί διαχωρισμό μεταξύ των συνδρομητών με φυσική υπόσταση, και των μηχανών. Ένα τέτοιου είδους Turing Test θα πρέπει να καλύπτει τις παρακάτω απαιτήσεις:

- Να διαθέτει ένα επίπεδο τυπικότητας και ευγένειας έτσι ώστε να μην προσβάλλει τον καλούντα.
- Να είναι αρκετά σύντομο, έτσι ώστε να μην απαιτεί μεγάλο επίπεδο υπομονής από τον καλούντα.
- Να είναι κατανοητό και εύχρηστο από συνδρομητές οι οποίοι κυμαίνονται σε διάφορα επίπεδα μόρφωσης και τηλεπικοινωνιακού ιστορικού.

- Θα πρέπει να είναι σε θέση να λειτουργήσει απρόσκοπτα με συνδρομητές οι οποίοι έχουν ιδιαίτερη προφορά.
- Απαιτείται να είναι αρκετά ενημερωμένο και εμπλουτισμένο, έτσι ώστε να είναι σε θέση να αντιληφθεί διαφορετικές διαλέκτους τις οποίες μπορεί να χρησιμοποιούν οι συνδρομητές.
- Η πολυπλοκότητά του θα πρέπει να είναι όσο το δυνατό χαμηλή, έτσι ώστε να είναι σε θέση να ενσωματωθεί σε όλων των ειδών τις συσκευές των συνδρομητών, καθώς και αυτές οι οποίες είναι χαμηλότερης αξίας.
- Θα πρέπει να είναι αρκετά εντατικό και περίπλοκο έτσι ώστε να απορρίψει οποιαδήποτε προσπάθεια μηχανής η οποία προσπαθεί να μιμηθεί ανθρώπινη οντότητα.

Περιγράψαμε ένα Turing Test το οποίο βασίζεται στον έλεγχο ανθρώπινων επικοινωνιακών προτύπων, είναι όσο το δυνατό φιλικότερο προς το χρήστη, παρέχει μεγάλο επίπεδο προστασίας του καλούμενου, ενώ ταυτόχρονα προκαλεί την ελάχιστη δυνατή ενόχληση στον καλούντα.

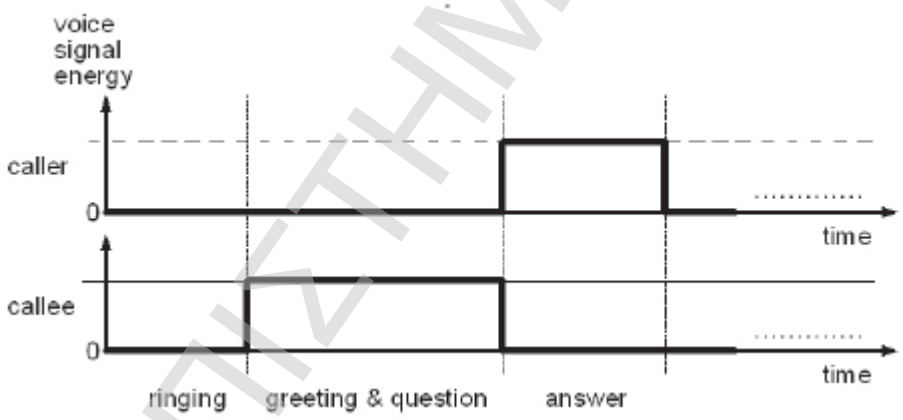


Σχήμα 29. Φιλτράρισμα κλήσης κατά το δεύτερο επίπεδο ενός συστήματος πρόληψης SPIT (Turing Tests).

Το Turing Test το οποίο περιγράψαμε, βασίζεται στην υπόθεση ότι η ανθρώπινη συζήτηση ακολουθεί συγκεκριμένα πρότυπα δραστικότητας.

Υπάρχουν διαθέσιμες μελέτες οι οποίες επιδεικνύουν το πως αυτά τα επικοινωνιακά πρότυπα είναι αναγνωρίσιμα. Ένα παράδειγμα είναι αποτελεί μία κλήση μίας ανθρώπινης οντότητας σε άλλη, όπου υπάρχουν συγκεκριμένες κατεστημένες συνήθειες τις οποίες και οι δύο ακολουθούν. Παραδείγματος χάρης, εφόσον ο καλούμενος αποδεχτεί την κλήση, είναι αυτός και ο οποίος είθισται να μιλήσει πρώτος. Κατά τη διάρκεια της κλήσης, συνηθίζεται το ένα μέλος να διατηρεί σιωπή καθώς το άλλο μιλάει. Το προτεινόμενο Turing Test διενεργεί έλεγχο για το εάν ο καλούντας ακολουθεί τις συνήθειες αυτές.

Το σχήμα 30 απεικονίζει ένα παράδειγμα ενός επικοινωνιακού προτύπου, στο οποίο επιδεικνύονται τα επίπεδα των φωνών των δύο μελών μίας κλήσης. Του καλούντος (πάνω), και του καλούμενου (κάτω). Όταν πραγματοποιηθεί η κλήση και προτού ο καλούμενος απαντήσει, το επίπεδο και των δύο μελών, όσον αφορά τη φωνή, είναι μηδενικό ή πολύ χαμηλό.



Σχήμα 30. Σχέδιο παλμών φωνής καλούντα και καλούμενου κατά την εκκίνηση μίας κλήσης.

Το πρότυπο αυτό αφορά αποκλειστικά το επίπεδο του σήματος φωνής. Είναι εντελώς ανεξάρτητο από το περιεχόμενου του φωνητικού σήματος και γι' αυτό το λόγο μπορεί εύκολα να υλοποιηθεί με πολύ μικρές απαιτήσεις σε πόρους.

Η διαδικασία αντιμετώπισης SPIT του συγκεκριμένου συστήματος είναι σχετικά απλή. Καθώς το σύστημα SPIT prevention κάνει αποδοχή της κλήσης,

στέλνει αυτόματα ένα προεγγεγραμμένο ηχητικό μήνυμα χαιρετισμού στον καλούντα, το οποίο μπορεί να προσαρμοστεί έτσι, ώστε να είναι αποδεκτό από το σύστημα και να μην απορρίπτεται. Σε περίπτωση όπου ο καλούντας διακόψει το μήνυμα χαιρετισμού, είτε αποτελεί περίπτωση αγενούς συνομιλητή, ο οποίος δεν ακολουθεί τους συνήθεις κανόνες τηλεφωνικής επικοινωνίας, ή πρόκειται για μία μηχανή η οποία ξεκινά απευθείας την αναπαραγωγή SPIT μηνύματος. Και στις δύο περιπτώσεις, το σύστημα αποφυγής SPIT θα πρέπει να καταχωρεί την κλήση ως μία κλήση SPIT, και να την τερματίζει. Σε ιδανική περίπτωση θα προηγείται του τερματισμού της κλήσης ηχογραφημένο μήνυμα το οποίο θα εξηγεί το λόγο για τον οποίο η κλήση θα λάβει τέλος.

Το επίπεδο ανεπιθύμητης πρόσβασης του επιτιθέμενου κατά τη μέθοδο αυτή, μπορεί να ελαχιστοποιηθεί με την αποστολή από το σύστημα αντιμετώπισης SPIT ενός ηχητικού τόνου, αντί του ηχογραφημένου μηνύματος. Σε περίπτωση όπου η κλήση έχει γίνει από φυσικό πρόσωπο, αυτό θα υποθέτει ακούγοντας τον τόνο, ότι ακόμη δεν έχει απαντηθεί η κλήση του. Εάν όμως την κλήση έχει εκκινήσει μηχανή, αυτή δεν είναι σε θέση να αντιληφθεί και να επεξεργαστεί τον τόνο, οπότε και θα πραγματοποιήσει άμεσα τη μετάδοση της κλήσης SPIT, καθώς αντιλήφθηκε ότι η κλήση έχει απαντηθεί από το άλλο άκρο. Έτσι το σύστημα θα απορρίψει άμεσα την κλήση ως κλήση SPIT.

Με αυξημένο επίπεδο διείσδυσης, αλλά παράλληλα αποδεκτό, μπορεί να γίνει αναπαραγωγή ενός μηνύματος το οποίο θα ενημερώνει τον καλούντα για το ότι η κλήση του προωθείται και θα πραγματοποιηθεί σύντομα. Για ακόμη μεγαλύτερο έλεγχο και ασφάλεια, το ηχητικό μήνυμα χαιρετισμού θα μπορούσε να ακολουθήσει μία απλή ερώτηση, όπως για παράδειγμα το όνομα του ατόμου το οποίο καλεί. Σε μία τέτοια ερώτηση δεν αναμένεται συγκεκριμένη απάντηση από το σύστημα, αλλά μία μικρής διάρκειας, κοφτή απάντηση, η οποία λογικά θα αποτελεί και το όνομα του καλούντα. Το σύστημα, χωρίς να έχει ανάγκη από λογισμικό αναγνώρισης φωνής, ελέγχει απλά για το αν η απάντηση που θα πάρει είναι σύντομη, και ο καλών θα πρέπει λογικά αμέσως μετά την απάντησή του να διατηρεί ησυχία για ένα

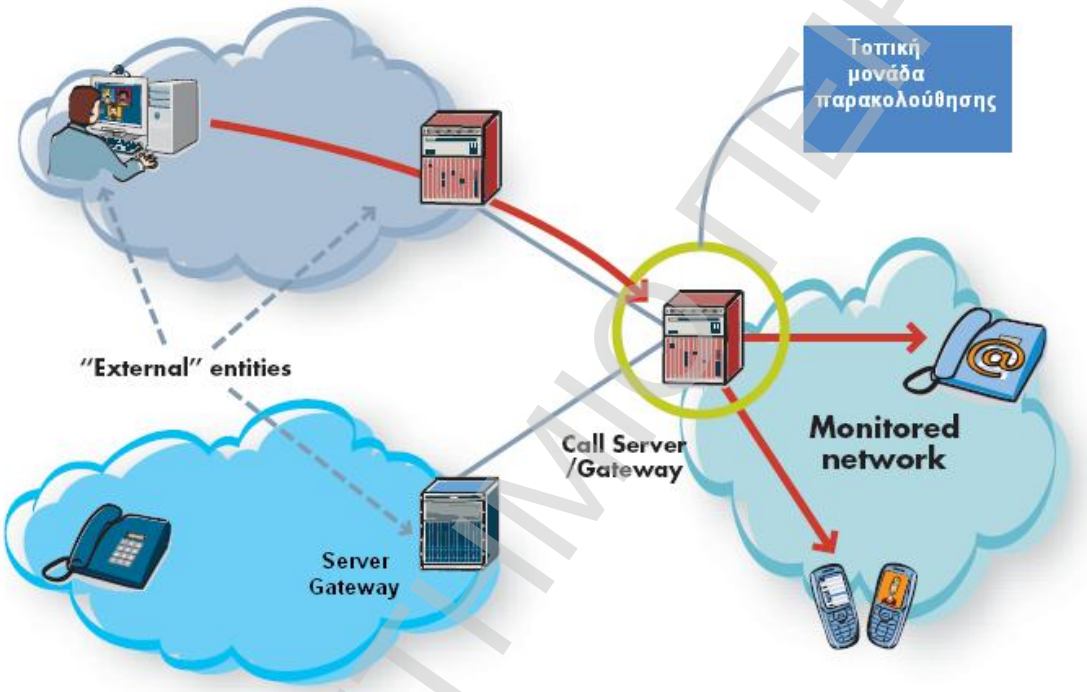
πολύ μικρό διάστημα. Έτσι, η μέθοδος αναγνώρισης έντασης φωνής από το επίπεδο ”low” στο επίπεδο ”high” και πάλι στο ”low”, είναι επαρκής για την περίπτωσή μας.

Η μεθοδολογία αυτή, καλύπτει και τις επτά απαιτήσεις ενός συστήματος αντιμετώπισης SPIT, τις οποίες προαναφέραμε. Είναι ικανοποιητικά ανθρωποκεντρική και με άμεση απόκριση, δεν επηρεάζεται από το γνωστικό υπόβαθρο του καλούντα ή την προφορά του, και είναι σε θέση να προσαρμοσθεί σε οποιαδήποτε γλώσσα αυτός επιθυμεί. Το σύστημα αναγνώρισης έντασης φωνής είναι, όσον αφορά το τμήμα του λογισμικού, απλό, και απαιτείται υψηλό επίπεδο τεχνολογίας για να παρακαμφθεί. Επιπρόσθετα, το επίπεδο διείσδυσης μπορεί να ρυθμιστεί ανάλογα με τις προτιμήσεις του καλούμενου. Επιπλέον ρυθμίσεις οι οποίες απαιτούνται, αφορούν το επίπεδο του κατωφλίου κατά τη διαδικασία αναγνώρισης έντασης φωνής. Υπάρχει δυσκολία κατά την αναγνώριση της απόλυτης ησυχίας, και της σχετικής ησυχίας. Αυτό συνήθως συμβαίνει όταν ο καλών βρίσκεται σε περιβάλλον θορυβώδες, οπότε και θα πρέπει να γίνουν οι απαραίτητες ρυθμίσεις στο κατώφλι της έντασης ”low”.

Ένα τέτοιο σύστημα πρόληψης κλήσεων SPIT θα πρέπει παράλληλα να κάνει χρήση και των μεθόδων το επιπέδου 1. Ιδιαιτέρως, θα πρέπει να ενσωματωθεί η τεχνική χρήσεων λευκών και μαύρων λιστών. Εξαιρετικά βολική φαντάζει η χρήση λευκών λιστών, καθώς με αυτό τον τρόπο αποφεύγεται ο άσκοπος επαναλαμβανόμενος έλεγχος έμπιστων χρηστών. Έτσι μειώνεται κατά πολύ ο χρόνος απόκρισης του συστήματος. Τα αποτελέσματα δε, ενός turing test μπορεί να αποτελέσουν ανατροφοδότηση για μία μαύρη ή λευκή λίστα.

Η θεωρητική παρουσίαση του συστήματος αντιμετώπισης SPIT, την οποία κάναμε, βασίζεται σε τυπικά επικοινωνιακά μοτίβα. Για την ενσωμάτωσή του με άλλες μεθόδους αντιμετώπισης SPIT προτείνεται ένα σύστημα γενικής αρχιτεκτονικής το οποίο επιτρέπει ελαστικότητα στην ενσωμάτωση διαφορετικών μεθόδων αντιμετώπισης SPIT.

Εξίσου σημαντική θεωρητική προσέγγιση ενός συστήματος αντιμετώπισης SPIT, είναι αυτή η οποία τοποθετεί το σύστημα ακριβώς ένα επίπεδο έξω από το δίκτυό μας. Έτσι παίρνουμε το ρίσκο της υπόθεσης πως δεν υπάρχει κακόβουλος χρήστης εντός του δικτύου, αλλά όλοι οι συνδρομητές του αποτελούν έμπιστους χρήστες. Η ιδέα έχει να κάνει με την παρακολούθηση κίνησης της VoIP σηματοδοσίας στον access domain call server του καλούμενου, όπως φαίνεται και στο σχήμα 31.



Σχήμα 31. Αντιμετώπιση SPIT κλήσεων ένα επίπεδο πριν το domain.

Με αυτό τον τρόπο γίνεται εστίαση μόνο στους εξωτερικούς spammers, υποθέτοντας ότι το δίκτυό μας, απαρτίζεται μόνο από έμπιστους χρήστες. Η διαδικασία ελέγχου των εξερχόμενων SPIT κλήσεων από το δίκτυό μας, αποτελεί μία εντελώς ξεχωριστή διαδικασία.

Πραγματοποιήσαμε λεπτομερή ανάλυση των απαιτήσεων ενός προτεινόμενου συστήματος, και περιγράψαμε το σχεδιασμό του. Ένα πρωτοποριακό στοιχείου ενός τέτοιου συστήματος, αποτελούν τα turing tests, τα οποία συναντούν και καλύπτουν όλες τις προαναφερθείσες απαιτήσεις, δεν έχουν εφαρμοσθεί ακόμη σε υλοποιημένα συστήματα αντιμετώπισης SPIT, και

προβλέπεται να αποτελούν μία αρκετά αποτελεσματική λύση κατά το διαχωρισμό φυσικών προσώπων, από μηχανές παραγωγής κλήσεων SPIT. Τα τεστ αυτά ανιχνεύουν την αντίδραση του καλούντα μετά από την αναπαραγωγή ενός ηχογραφημένου μηνύματος, και πραγματοποιούν σύγκριση μεταξύ συνηθισμένων επικοινωνιακών μοτίβων. Η μέθοδος αυτή ελαχιστοποιεί την εμπλοκή του χρήστη μέσω μίας παραμετροποιήσιμης μεθόδου και για την εφαρμογή της απαιτείται ελάχιστη υπολογιστική ισχύς.

Μελλοντικές μελέτες βασισμένες στον κώδικα SAML

Πολλές μελέτες σχετικά με τη μελλοντική VoIP ασφάλεια περιλαμβάνουν ως προϋπόθεση την ύπαρξη κεντρικών αρχών ασφάλειας εντός του δικτύου. Έτσι, οποιαδήποτε πληροφορία σχετική με το επίπεδο ασφάλειας, και την πιστοποίηση ταυτότητας, είναι διαθέσιμο στην αρχή αυτή. Με τη συνεχόμενη ανάπτυξη της από IP σε IP επικοινωνίας, και με την απουσία της ανάγκης για ανωνυμία εντός του δικτύου, οι οποιεσδήποτε πληροφορίες σχετικά με τον καλούντα, μπορούν να εισαχθούν στην τελική συσκευή του χρήστη, ή στον διακομιστή του Member Island. Εάν δεν υπάρχει επιπλέον πληροφορία για να προστεθεί στην βάση πληροφοριών της αρχής ασφαλείας, τότε μπορεί να παραχθεί κώδικας SAML στον τελικό χρήστη ή στο Member Island. Στην περίπτωση αυτή, το τελικό Member Island, το οποίο και θα περιέχει τον κώδικα με τους περιορισμούς, θα είναι σε θέση μέσω του κώδικα να φιλτράρει καταλλήλως τις κλήσεις.

Παρ' όλα αυτά, ίσως υπάρξουν περιπτώσεις όπου η κεντρική ασχή ασφάλειας θα συνεχίσει να διατηρεί σημαντικές πληροφορίες ασφάλειας, ακόμη και αν ο τελικός χρήστης ή το Member Island κάνουν τις δικές τους δηλώσεις ασφάλειας. Στην περίπτωση αυτή, προτιμάται ένα υβριδικό μοντέλο καθαρού end to end SAML κώδικα, το οποίο μαζί με τις προσθήκες της κεντρικής αρχής ασφάλειας, θεωρείται ως η καλύτερη λύση.

Ο κώδικας SAML καθορίζει μεθόδους αίτησης πληροφοριών ασφάλειας από και προς την αρχή ασφάλειας, οι οποίες επιτρέπουν τη μεταφορά αυτών των πληροφοριών με τρόπο ενσωματωμένο και ασφαλή, έτσι ώστε να

διατηρούνται μυστικές και ασφαλείς ακόμη και από τον χρήστη από τον οποίο έχουν προέλθει, ή από το Member Island. Οι μέθοδοι αυτοί μπορούν να ενσωματωθούν σε αρχιτεκτονικές όπου η κλήση δεν χρειάζεται να διατρέχει κεντρικά κομβικά σημεία στο δίκτυο, ή σε δίκτυα όπου οι πληροφορίες ασφάλειας είναι τοποθετημένες εκτός οργανισμού.

14. Ισχύουσα κατάσταση αντιμετώπισης κλήσεων SPIT

Όπως εκτενώς περιγράψαμε, οι ανεπιθύμητες SPIT κλήσεις, μπορούν να είναι πολλών ειδών. Από ένα απλό ερώτημα σφυγμομέτρησης ή μία καμπάνια προώθησης προϊόντων και υπηρεσιών, έως κακόβουλες κλήσεις παράνομης συλλογής χρημάτων.
Η VoIP τεχνολογία έχει προσφέρει νέα εργαλεία προώθησης προϊόντων, και έχει συμβάλει αισθητά στην ασφάλεια των επικοινωνιών καθώς και στην ανάπτυξη νέων υπηρεσιών πάντα στη διάθεση των συνδρομητών. Με την τάχιστη όμως ανάπτυξη της διαδικτυακής τηλεφωνίας, προκύπτει παράλληλα η διεύρυνση του προβλήματος SPIT, το οποίο τείνει να πάρει διαστάσεις email spam.

Πέραν τον προβλημάτων τα οποία έχουμε αναφέρει στη συγκεκριμένη μελέτη, αντιμετωπίζουμε πληθώρα άλλων προβλημάτων όσων αφορά το SPIT.
Παραδείγματος χάριν, η ανάλυση του περιεχομένου δεδομένων είναι μη εφαρμόσιμη, καθώς και σε πολλές περιπτώσεις παράνομη. Η απόφαση τρόπου χειρισμού της κλήσης πρέπει να παίρνεται σε πραγματικό χρόνο, προτού ξεκινήσει η συνεδρία.

Καθώς οι VoIP spammers ενδιαφέρονται σπάνια στη διακοπή υπηρεσιών, το SPIT δεν αποτελεί συνήθως μία Denial of Service (DoS) επίθεση, γι' αυτό και οι τεχνικές οι οποίες χρησιμοποιούνται για την ανίχνευση Denial of Service επιθέσεων, είναι ουσιαστικά ανεφάρμοστες, καθώς δεν υπάρχουν παραποιημένα πακέτα, ημιτελείς παραμετροποιήσεις κλήσεων, και λοιπά στοιχεία DoS.

Οι τρέχουσες λύσεις αντιμετώπισης SPIT εστιάζουν σε συγκεκριμένες προσεγγίσεις.

- Στην ταυτότητα και την υπεγγυότητα του καλούντα κατά την πρόσβασή του στο δίκτυο, καθώς και την αξιόπιστη αυθεντικοποίηση του domain. Η μεθόδευση αυτή είναι λειτουργική μόνο εάν όλοι οι χρήστες

αποδεχτούν τις συγκεκριμένες πολιτικές και πληρούν τα ίδια σφαιρικά στάνταρ.

Η ισχυρή αυθεντικοποίηση είναι απαραίτητη για την ορθή και αποτελεσματική λειτουργία των λευκών και μαύρων λιστών, των συστημάτων τα οποία είναι βασισμένα στην φήμη των χρηστών, καθώς και τους κύκλους εμπιστοσύνης.

- IP διευθύνσεις περιορισμένης χρήσης. Οι χρήστες μπορούν να εγγράφονται στο δίκτυό τους με αναλώσιμες IP URIs (Uniform Resource Identifiers), οι οποίες υπάρχουν κυρίως για να αναθέτονται σε νέους, μη έμπιστους ακόμη, συνδρομητές. Στην περίπτωση όπου μία IP δεσμεύεται από κάποιον κακόβουλο εισβολέα, ο φυσικός ιδιοκτήτης της απλά την αποσύρει.
- Νομοθετικοί περιορισμοί. Περιορισμοί σε εθνικό επίπεδο, οι οποίοι όμως συχνά δεν γίνονται σεβαστοί από εταιρίες και χρήστες εκτός συνόρων. Δι' αυτό το λόγο κρίνεται και επιτακτική η ίδρυση παγκόσμιων περιορισμών και σταθερών στον τομέα της διαδικτυακής τηλεφωνίας σε διεθνές επίπεδο.

15. Κανονισμοί και νομικοί περιορισμοί

Με την ανάπτυξη της διαδικτυακής επικοινωνίας, και την εγκαθίδρυσή της ως τον πλέον προηγμένο τρόπο επικοινωνίας της εποχής μας, είναι επιτακτική η ανάγκη ίδρυσης κάποιων κανονισμών και όρων για την εύρυθμη λειτουργία και την ομοιογένεια των δικτύων. Οι κανονισμοί αυτοί για να έχουν την αρμόζουσα ισχύ και βαρύτητα, θα πρέπει να ελέγχονται αυστηρά από έναν αρμόδιο οργανισμό, καθώς και να ασκούνται κυρώσεις με τη μη συμμόρφωση σε αυτούς τους κανονισμούς.

Δυστυχώς η ασύμμετρη ανάπτυξη της διαδικτυακής τηλεφωνίας μεταξύ των κρατών, δεν έχει ενεργοποιήσει όλα τα κράτη στην ίδρυση τέτοιων οργανισμών, και την ενεργοποίηση σχετικών κανονισμών και περιορισμών. Οι Ηνωμένες Πολιτείες Αμερικής, είναι το πρώτο κράτος το οποίο έχει αναπτύξει σχέδιο νομικών περιορισμών και κανονισμών σχετικά με την ασφάλεια στη διαδικτυακή τηλεφωνία.

Οι εταιρίες τηλεπωλήσεων λειτουργούν υπό κανονισμούς της εταιρίας Τηλεφωνικής Προστασίας Καταναλωτή[16], η οποία ενστερνίστηκε καταχωρήσεις του τμήματος προστασίας τηλεφωνικών συνδρομητών της διεθνούς επιτροπής εμπορίου[17].

Επιπλέον περιορισμοί έχουν να κάνουν με:

- Κλήσεις οι οποίες περιέχουν ηχογραφημένα μηνύματα προς κατοικίες, χωρίς την προηγούμενη συγκατάθεση του καλούμενου, εκτός από περιπτώσεις εξαιρετικής ανάγκης, ή θέματα ασφάλειας.
- Αυτοματοποιημένη κλήση ή ηχογραφημένο μήνυμα προς συνδρομητή, ο οποίος χρεώνεται για την τρέχουσα τηλεφωνική συνεδρία. (όπως για παράδειγμα κλήση προς κινητό τηλέφωνο σε λειτουργία roaming)
- Αυτόκλητες διαφημίσεις, οι οποίες στέλνονται προς πανομοιότυπες συσκευές.

[16] Telephone Consumer Protection Act (TCPA).
[17] The Federal Trade Commission, the National Do Not Call Registry.

Των περιορισμών αυτών απαλλάσσονται:

- Χρήστες οι οποίοι έχουν συνάψει επαγγελματικές σχέσεις με τον εκάστοτε συνδρομητή.
- Κλήσεις, μη κερδοσκοπικού περιεχομένου. (για παράδειγμα σφυγμομετρήσεις, προεκλογικά δημοψηφίσματα, θρησκευτικά θέματα, ενημέρωση κεφαλαίου)

Οι περιορισμοί αυτοί, καθώς και οι εξαιρέσεις, βρίσκονται ακόμη υπό μελέτη.

Το ευρωπαϊκό κοινοβούλιο, έχει υιοθετήσει την οδηγία 2002/58/EC[18] ως κατευθυντήρια οδηγία για τη διεθνή νομοθεσία. Απαγορεύει τη χρήση αυτόματων μηχανών κλήσεως και φαξ, για απευθείας διαφήμιση άνευ της προηγούμενης συγκατάθεσης του εκάστοτε συνδρομητή. Έτσι δίνονται δύο επιλογές. Είτε η προεπιλεγμένη απαγόρευση τηλεπωλητών, εκτός αν δοθεί η συγκατάθεση του συνδρομητή, ή η ελεύθερη επικοινωνία των τηλεπωλητών με τους συνδρομητές εώς ότου οι δεύτεροι δηλώσουν μη επιθυμία περαιτέρω επικοινωνίας μαζί τους. Το Ηνωμένο Βασίλειο, έχοντας ασχοληθεί με το θέμα νομοθεσίας στις διαδικτυακές τηλεφωνικές επικοινωνίες, έχει επιλέξει τη δεύτερη επιλογή.

[18] Οδηγία περί ιδιωτικότητας και ηλεκτρονικών επικοινωνιών του Ευρωπαϊκού κοινοβουλίου, και του συμβουλίου της 12ης Ιουλίου 2002.

16. Σχόλια – Διαπιστώσεις - Συμπεράσματα

Στη διατριβή αυτή, μελετήθηκε η χρήση του διαδικτύου για VoIP σηματοδοσία, πως μας δίνεται πλέον η δυνατότητα να περάσουμε στο επόμενο επίπεδο την επικοινωνία μέσω τηλεφωνίας, αλλά και οι κίνδυνοι οι οποίοι ελλοχεύουν με τη έλευση της νέας αυτής τεχνολογίας.
Αναλύθηκαν τα στάδια μέσω των οποίων γίνεται η μετάβαση από την PSTN αρχιτεκτονική στη VoIP τηλεφωνία. Η τεχνογνωσία η οποία απαιτείται για τη μετάβαση αυτή, η πλήρης εκμετάλλευση της νέας μορφής τηλεφωνικής επικοινωνίας, καθώς και το πώς οι μέχρι τώρα τεχνικές ασφάλειας, μπορούν να εφαρμοστούν στη διαδικτυακή τηλεφωνία. Εξετάσθηκαν οι κίνδυνοι στη διαδικτυακή τηλεφωνία, και οι επιπτώσεις κάθε μίας κατηγορίας αυτών. Προτάθηκαν νέες μέθοδοι αντιμετώπισης κακόβουλων επιθέσεων, οι οποίες μπορούν να αποτελέσουν το έναυσμα για νέες μελέτες προς ανάπτυξη καινοτόμων λύσεων ασφάλειας.
Συμπερασματικά, αντιλαμβανόμαστε ότι οι κίνδυνοι, καθώς και οι μέχρι τώρα γνωστοί τύποι επιθέσεων, αποτελούν μόνο την κορυφή του παγόβουνου, όσων αφορά την ασφάλεια στη διαδικτυακή τηλεφωνία.
Πέραν των απλών ενοχλητικών επιθέσεων κατά τη διάρκεια μίας κλήσης, αντιλαμβανόμαστε ότι τους σημαντικότερους κινδύνους αποτελούν επιθέσεις οι οποίες αποσκοπούν σε οικονομικά οφέλη υπέρ του επιτιθέμενου. Οι μηχανισμοί ασφάλειας οι οποίοι αναλύθηκαν, βρίσκουν εφαρμογή χωρίς όμως να αποτελούν πανάκεια, καθώς απαιτείται διαρκής αναβάθμισή τους, και προσαρμογή στις νέες υπηρεσίες οι οποίες πλέον μας παρέχονται, καθώς και στους νέους τύπους hardware.
Η ενσωμάτωσή τους, σε πολλές περιπτώσεις αποτελεί μία σύνθετη διαδικασία, χωρίς όμως να καθίσταται ακατόρθωτη.

Συμπερασματικά, μπορούμε να πούμε ότι ζυγίζοντας τα οφέλη, αλλά και τους κινδύνους στη διαδικτυακή τηλεφωνία, η ζυγαριά γέρνει προς την πρώτη πλευρά. Οι δυνατότητες οι οποίες μας προσφέρονται πλέον είναι απεριόριστες, πολλές εκ των οποίων είναι ακόμη υπό ανάπτυξη. Μέσω της

μελέτης αυτής, παραθέτονται και γνωστοποιούνται πιθανές απειλές, προτεινόμενοι τρόποι αντιμετώπισής τους, καθώς και μελλοντικά προβλήματα τα οποία μπορεί να προκύψουν με τη χρήση και την περαιτέρω ανάπτυξη της διαδικτυακής τηλεφωνίας. Γίνεται προφανείς η ανάγκη διερεύνησης νέων αρχιτεκτονικών ασφάλισης των τηλεφωνικών κέντρων, και νέων διαδικασιών αυθεντικοποίησης και θωράκισης. Μελανό σημείο κατά την ανάπτυξη της διαδικτυακής τηλεφωνίας, αποτελεί η μη παράλληλη εξέλιξη της σε όλα τα κράτη. Οι διαφορές αυτές στο ρυθμό εξάπλωσης και ανάπτυξής της, αποτελεί τροχοπέδη στην εξέλιξη μεθόδων αντιμετώπισης πιθανών επιθέσεων καθώς και στην ανάπτυξη νέων δυνατοτήτων.

Βιβλιογραφία

D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis and S. Gritzalis. SIP Security Mechanisms: A State-of-the-art Review. In *the Proceedings of the Fifth International Network Conference (INC 2005)*, pages 147–155, July 2005, Samos, Greece

J. Arkko, V. Torvinen, G. Camarillo, A. Niemi and T. Haukka. Security Mechanism Agreement for the Session Initiation Protocol (SIP). *RFC 3329, IETF*, January 2003.

M. Baugher,D. McGrew, M. Naslund, E. Carrara and K. Norrman. The Secure Real-time Transport Protocol (SRTP). *RFC 3711, IETF*, March 2004.

T. Dierks and C. Allen. The TLS Protocol. *RFC2246, IETF*, January 1999

S. Niccolini, E. Chen. VoIP Security Threats relevant to SPEERMINT. http://tools.ietf.org/html/draft-niccolini-speermintvoipthreats- March 2007.

J. Rosenberg. The Real Time Transport Protocol (RTP) Denial of Service (Dos) Attack and its Prevention. http://www-rn.informatik.unibremen. de/ietf/mmusic/id/draft-rosenbergmmusic- rtp-denialofservice-00.txt. June 2003.

H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia. Fast Detection of Denial of Service Attacks on IP Telephony. In *Proceedings of the 14th IEEE International Workshop on Quality of Service (IWQoS 2006)*, June 2006.

J. Rosenberg, H. Schulzrinne et al., “SIP: session initiation protocol”, RFC 3261, 2002

S. Niccolini, “SPIT and SPIM”, http://www.iptel.org/voipsecurity/workshop/program_1stjune2006.php, 3rd VoIP Sec. Workshop, June 2006, Berlin, Germany

J. Seedorf, “Using Cryptographically Generated SIP-URIs to Protect the Integrity of Content in P2P-SIP”, Third Annual VoIP Security Workshop, June 2006, Berlin, Germany, to appear in ACM Digital Library

Center for Democracy & Technology: Spam 2005: Technology, Law and Policy, Washington D.C., March 2005, http://www.cdt.org/speech/spam/spam2005/

Commission of the European Union: Commission Staff Working Document: The treatment of Voice over Internet Protocol (VoIP) under the EU Regulatory Framework, 14 June 2004, http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/commiss_serv_doc/406_14_voip_consult_paper_v2_1.pdf
R. Pierce Reid: Voice Spam Spam, Spamity Spam – White Paper, July 2004, http://www.qovia.com/resources/pdfs/white%20papers/qovia_spit_wpaper.doc

Jonathan Rosenberg, Cullen Jennings, Jon Peterson: Identity Privacy in the Session Initiation Protocol (SIP), draft-rosenberg-sip-identity-privacy-00, SIP Internet- Draft,11 July 2005, http://www.ietf.org/internet-drafts/draft-rosenberg-sipidentity- privacy-00.txt

Rosenberg, J., Jennings, C., Peterson, J., “SIP and Spam”, draft-ietf-sipping-spam-00

Jennings, C., Peterson, J., Watson, m., “Private Extensions to SIP for Asserted
Identity within Trusted Networks”, IETF RFC 3325

Secure SIP or SIPS – see section 19.1 of RFC 3261

D. Shin, and C. Shim, "Voice Spam Control with Gray Leveling," Proc. Of 2nd VoIP Security Workshop, Washington DC, June 1-2 2005.

R. Pierce Reid: Voice Spam Spam, Spamity Spam – White Paper, July 2004, http://www.qovia.com/resources/pdfs/white%20papers/qovia_spit_wpaper.doc

Bundesnetzagentur: Anhφrung zu Voice over IP (VoIP) – Themenweise Auswertung der Anhφrung zu Voice over IP, October 2005, http://www.bundesnetzagentur.de/media/archive/3173.pdf